

ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA

ART 2025/4916

BETWEEN

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

AFFIDAVIT

I, **Fraser Tweedale** of 29 Cape Street, Holland Park 4121, affirm:

1. I hold a Bachelor of Engineering (Computer Systems Engineering) from the University of Queensland, and have worked as a software engineer since 2008. I am currently employed as a Principal Software Engineer at Red Hat, LLC, working on authentication and identity management solutions, a role I have held since 2014. I am involved in open source software development, both in my work and in a personal capacity.
2. Unless otherwise stated, the facts set out in this affidavit are within my own knowledge.

Background

3. I have applied to the Administrative Review Tribunal (**Tribunal**) under s 57A of the *Freedom of Information Act 1982* (Cth) (**FOI Act**) for review of a decision of Services Australia to refuse my request under the FOI Act for access to the source code of the Android version of the *myGov Code Generator* application (**App**).
4. The App generates a six-digit, time-based one-time password (**TOTP code**) which users enter alongside their username and password when logging into their myGov account. A TOTP code is valid for 30 seconds and serves as a single-use authentication code. TOTP codes are derived from a secret, randomly generated seed value (the '**TOTP shared secret**'), which is possessed by the App (after the App has been enrolled) and by the myGov Service (where the unique shared secrets are associated with corresponding myGov user accounts).
5. The respondent in the proceeding, the CEO of Services Australia, relies upon the 'open' and 'confidential' affidavits of Mr Garrett McDonald, the Chief Information Security Officer of Services Australia.
6. I make this affidavit in support of my application for review of Services Australia's decision to refuse my FOI application in the ART.

Lodged on behalf of the Applicant

Applicant contact: Jason Bosland

Prepared by: Jason Bosland

Wise Law
141A Como Parade East
Parkdale Vic 3195

Telephone: 0421 193 711

Email: JB@wiselaw.com.au

What is 'source code'?

7. Source code is the human-readable text that defines a computer program or part of a computer program. It is written in a 'programming language', of which there are many. The source code for a program may span multiple or many files, and may contain source code written in a variety of programming languages. Computer programmers write or modify the source code. Tools called 'compilers' or 'interpreters' transform the human readable source code into machine readable instructions ('machine code') and data that can be executed by a computer. The machine code and data in the executable program are typically not human readable or modifiable without the help of specialised tools.
8. Source code is typically stored in a 'version control system' that tracks changes to the source code over time. Version control systems allow retrieval or reconstruction of the source code as it existed at a specified point in time. The term 'repository' refers to the source code of an application or software project as stored by a version control system, including historical versioning data.
9. When referring to the source code of a particular program or application (**app**), the term 'source code' would ordinarily be taken to include:
 - 9.1. The source code, written in one or more programming languages;
 - 9.2. Source code written in specialised languages used to define the user interface of the application (if any), which are not necessarily programming languages;
 - 9.3. Graphics, audio, or video assets that form part of the application - for example, graphical icons or 'notification' sounds;
 - 9.4. Instructions for compiling and/or executing the program, which could be written using programming languages or other specialised languages or data formats;
 - 9.5. Programs for testing the software, which could be defined using programming languages or other specialised languages or data formats, and test data used by the testing programs;
 - 9.6. Any human-readable documentation stored alongside the source code in the repository;
 - 9.7. The source code of any dependencies that has been included in the repository alongside the source code of the program or application itself (a practice referred to as "vendoring" or "bundling"), whether modified or unmodified;
 - 9.8. Any other information which is stored in the repository and which is necessary for, or relevant to, the development, compilation, execution, testing, distribution, deployment, or maintenance of the application or software project.
10. All of the information described in the definition of 'source code' in the preceding paragraph is typically stored together in the repository for the software project. A request for the 'source code' of an application at a particular time should be taken to refer to the 'snapshot' of all of the information in the repository as it existed at the specified time, excluding files that do not meet this definition of 'source code'.

Open source software

11. 'Open source' software is software distributed under a software licence (an 'Open Source licence') that grants access to the source code, permitting it to be studied and modified, and permitting redistribution of the software with or without modifications. 'Free software', 'Free/libre software' and 'Free/libre open source software' (FLOSS) are related terms with similar definitions; most 'open source' software is 'free software' and vice-versa. 'Free' refers to freedom, not to cost; publishers may charge money for access to software that is provided under an Open Source licence.
12. Software may have its source code disclosed to the public (allowing study) without necessarily being open source i.e. not released under an Open Source licence that allows unrestricted use and modification. 'Source available' and 'disclosed source' are terms of art for such software.
13. My FOI request is for the source code of the App to be publicly disclosed. It is not a request for Services Australia to release the code under an Open Source licence that grants rights to modify the App or distributed modified versions.
14. Open Source software is widely used in industry. This includes software components that are dependencies of larger software solutions used within or delivered by an organisation, and 'stand-alone' software solutions that are provided under an Open Source licence and used 'as is' within an organisation.

Open Source software and Red Hat

15. Red Hat, LLC is a leading provider of enterprise software infrastructure whose products include operating systems, cloud computing infrastructure, and automation solutions. Annual revenue exceeds USD 7 billion. Red Hat's Australian subsidiary is Red Hat Asia Pacific Pty Ltd.
16. Almost all of Red Hat's software products, including software delivered to customers, and software services operated by Red Hat for or on behalf of customers, are Open Source software. That is, the source code is available to customers under Open Source licences. Practically speaking, the source code is also available to the public at large because Red Hat composes its software products from public repositories of Open Source software.
17. Services Australia, the Respondent, uses Red Hat software. A contract between Services Australia and Red Hat Asia Pacific Pty Ltd (Contract Notice CN4023201) for 'Software Subscriptions and Services' was executed on 29 June 2023 for an original value of AUD 27,147,639.88 and subsequently extended and varied to the current contract value of AUD 104,070,605.71.

Annexed hereto and marked '**FT-1**' is a screenshot of the details of Contract Notice CN4023201 from the AusTender website, accessed on 28 July 2026.

Australian Government open source policy

18. The Digital Transformation Agency (DTA) is an Australian Government agency driving government digital transformation strategy and policy to deliver benefits to all Australians. Prior to October 2016 it was called the Digital Transformation Office (DTO).

19. The DTA publishes the **Digital Service Standard (DSS)** which sets the requirements for designing and delivering high-quality digital government services and applies to all public facing government digital services. DSS version 2 is the current version, having come into effect for new services on 1 July 2024 and for existing services on 1 July 2025, and is available at: <https://www.digital.gov.au/policy/digital-experience/digital-service-standard>.
20. The previous version of the DSS, version 1.0, was in effect from 6 May 2016 until version 2 came into effect. It applied to all government agencies delivering public facing digital services with respect to those services. The myGov Service is one such public facing digital service. Services Australia was and is subject to the DSS with respect to the myGov Service.
21. Criterion 8 of DSS version 1.0 required agencies to 'Make all new source code open by default' (**Criterion 8 v.1**). One of the stated reasons why agencies must do this is that '[o]pen source helps to...increase transparency'.

Annexed hereto and marked '**FT-2**' are screenshots of the Digital Service Standard (DSS) version 1.0 published by the Digital Transformation Agency (DTA), as archived by the Internet Archive Wayback Machine on 26 February 2024 and accessed on 27 July 2026.

22. Two articles published by the DTA provide further context about open source code and advice to agencies regarding the implementation of Criterion 8. These articles are no longer published on the DTA website but are available in an archive of the old version of the website, and via the Internet Archive Wayback Machine. The articles have also been released under the FOI Act following a request by me.

23. On or about 14 August 2015, the DTA published an article entitled 'Open and secure'.

Annexed hereto and marked '**FT-3**' are screenshots of the article 'Open and secure' published on the DTA website on or about 14 August 2024, as archived by Internet Archive Wayback Machine on 25 June 2022 and accessed on 27 July 2026.

24. The article 'Open and secure' explains the DTA's approach to releasing their own source code and their position that security and trust are enhanced, not harmed, by disclosing source code. It states (FT-3):

We've all seen that security through obscurity doesn't work. It leaves us in the dark on how our data is stored, protected and used.

You shouldn't have to take our word that our systems are secure, or that we fix our vulnerabilities - you should be able to see it in our designs, our code, our build and our operations. Being open invites trust - you should be able to trust us not because we tell you that you should, or because we're the only supplier, but because we've earned it.

...

We think the good guys outweigh the bad

A question you might be asking is: Why all this openness? Doesn't it give the bad guys an advantage? We think it gives the good guys a bigger one. Any user, or indeed any organisation, can look over the code for weaknesses. For example, we're looking at using the codebase from GOV.UK as part of the basis for one of the DTO's

work programs. We can look over the code, and if we find a bug, we can either report it or even fix it directly. If GOV.UK was closed, we'd pay to use the codebase and they may not ever find certain vulnerabilities (which doesn't mean the bad guys haven't found them), or never fix them if they do.

25. On or about 20 February 2017, the DTA published an article entitled 'Making source code open'.

Annexed hereto and marked '**FT-4**' are screenshots of the article 'Making source code open' published on the DTA website on or about 20 February 2017, as archived by Internet Archive Wayback Machine on 17 March 2022 and accessed on 27 July 2026.

26. The article 'Making source code open' (FT-4) makes several important points, including that: disclosing source code is not the same as exposing user data; that source code should be separate from any secrets required for the operation of the application or service; and that disclosure of source code promotes reuse and financial accountability:

Making your code open source is not giving away user data.

[Criterion 8](#) of the [Digital Service Standard](#) tells teams to be open by default, but this can be difficult for some teams. First timers can be unsure about what extra work going 'open source' will mean. Others feel that their code shouldn't be open source because nobody else would want it. I've also heard that code can not be open sourced because of security reasons. These are all important considerations for teams.

If you have secrets littered through your closed source code, someone will eventually find them. Anyone who views your site has access to your HTML and javascript at the click of a button. It's not as simple for mobile and desktop apps, but still very achievable. [Industry best practice](#) tells us to separate our code from the secrets it uses. If you haven't done this, it's unlikely you'll meet criterion 5 of the Digital Service Standard: [Make it secure](#).

Why would I?

Government code should be available to others unless there is a compelling reason. Everyone in the public service benefits from being able to reuse code that others have developed. We all work for the taxpayer and they should be able to see and use what they've paid for.

The article then emphasise that except for secrets like passwords and keys, source code can be shared and reused, and that brand protection concerns are not relevant to code developed by government:

Once teams understand more about what open source is, and isn't, they find they don't usually have any reason not to be open. However, it is common for teams to be concerned about security.

Security is a very valid reason, but you shouldn't use it as an excuse to close everything. Keeping passwords and keys private helps to keep our user's data private and secure. Not only is it good practice, it's part of the obligation we have in serving the public. Code that doesn't contain these secrets can be shared and reused by others.

There are lots of examples of world class security products that are open source. Talk with your department's [ITSA](#) (Information Technology Security Advisor) for specific advice.

Many private sector organisations close their code to maintain control of their brand and their user experience, in government, we don't have those issues.

27. DSS version 2 removed the explicit Criterion 8 v.1. There is no evidence that security concerns were a factor in its removal. Through a series of FOI requests to the DTA, I sought access to internal and inter-agency information about the development of DSS v2 and, in particular, the removal of Criterion 8 v.1. There were no access refusal decisions and my requests turned up a variety of research, registers of consultation, feedback about draft versions, and similar. There were references to Criterion 8 v.1 in two of the documents I received.
28. The first document is a DTA Report entitled 'Digital Service Standards and Measures', 9 June 2023, which presents research into what good digital service delivery looks like.

Annexed hereto and marked '**FT-5**' are pages 1-3 and 14-15 of the DTA Report, 'Digital Service Standards and Measures', dated 9 June 2023.

29. The DTA Report states (FT-5, pages 14 and 15):

Research also identified 4 principles currently included in the Australian Government's DSS which may be less relevant in 2023 or may not be resonating with all stakeholders. These include:

...

Make the source code open: Some agencies have found this principle hard to achieve in practice, as it may not always be possible or appropriate to publish source code in the public domain.

30. The second document is entitled 'Digital Service Standard — Feedback and Actions Register'. It contains two records of feedback related to the removal of the 'Make source code open' criterion, with associated comments.

Annexed hereto and marked '**FT-6**' is the DTA document 'Digital Service Standard — Feedback and Actions Register', (date unknown).

31. Page 4 records the following feedback (FT-6, page 4):

(Via comment on slide 11) - Are we actively dropping the making 'source code open by default' principle? Is there a reason that we aren't [sic] encouraging the share-back approach?

The associated comment is (FT-6, page 4):

Chris has highlighted a preference to move away from open source to open standards. It would be good to understand the two sides of this argument a bit further – we will schedule some time with you to discuss.

Page 19 records the following feedback (FT-6, page 19):

(Via email) The rationale behind open-source vs open standards would be good to share. There is a very [sic] that the DTA has historically been a champion for use of open-source technologies.

The associated comment is (FT-6, page 19):

The CEO has highlighted a preference to move away from open source to open standards. It would be good to understand the two sides of this argument a bit further – we will schedule some time with you to discuss.

32. Chris Fechner is CEO of the DTA, currently and throughout the development of DSS v2. On 9 July 2026, I contacted Mr Fechner by email to ask for further information about the removal of the 'Make source code open' criterion. He sent a response email to me on 17 July 2026.

Annexed hereto and marked '**FT-7**' is email correspondence between me and Mr Chris Fechner, CEO of the Digital Transformation Agency, dated 9 July 2026 (my email) and 17 July 2026 (Mr Fechner's response).

33. According to Mr Fechner, the driving factor behind the omission of Criterion 8 v.1 from the DSS v2 was to emphasise 'open standards' rather than 'open source' for digital services interoperability across government. He states in his email (FT-7):

The removal of the specific criterion 'Make source code open' from the Digital Service Standard was not intended to signal opposition to open-source software. During the development of DSS v2, there was a deliberate effort to make the Standard more principles-based and applicable across a wider range of digital services and agency contexts.

My view has always been that the Australian Government operates in a mixed technology environment, comprising both open-source and proprietary solutions. I do not oppose open source and recognise the significant value it can provide. However, I continue to be particularly conscious of the importance of interoperability across government, and of the role that open standards play in enabling that interoperability regardless of the underlying technology choices made by agencies.

The references to open standards in the feedback register reflected this focus. Standards such as those developed by W3C, along with JSON, OData, OAuth, SAML and WCAG, help ensure systems can exchange information, integrate effectively and remain accessible and portable over time. The change was not a move away from open source, but rather an emphasis on the standards that allow diverse systems and technologies to work together across the Australian Government.

Where government entities choose to use or develop open-source software, we continue to support open and transparent development practices, within appropriate security, privacy and other legislative requirements.

The ACSC / ASD 'Shifting the Balance' report

34. A report entitled 'Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software' (the **Shifting the Balance Report**) was published in October 2023 by the Australian Cyber Security Centre (ACSC) - a department of the Australian Signals Directorate (ASD) - jointly with the apex cyber security agencies of USA, Canada, UK, Germany, Netherlands, Norway, New Zealand, Korea, Israel, Japan, Singapore, Czech Republic, and the Organization of American States (OAS).

Annexed hereto and marked '**FT-8**' is a copy of the Shifting the Balance Report.

35. The 'Software Product Security Principles' section of the Report lays out 'three core principles to guide software manufacturers in building software security into their design...' (FT-8, page 10). Principle 2 is 'Embrace radical transparency and accountability'. The explanation of this principle on (FT-8, page 20) of the report begins:

Software manufacturers should pride themselves in delivering safe and secure products, as well as differentiating themselves from the rest of the manufacturer community based on their ability to do so.

Let's address a common concern about transparency. When practitioners discuss radical transparency, there is a tendency for the conversation to get bogged down in a concern that they are providing a 'roadmap for attackers'. However, the overwhelming evidence is that attackers are doing just fine without such roadmaps, and such concerns should take a back seat to transparency that benefits direct customers, indirect customers, supply chains, and the entire software industry.

The COVIDSafe app

36. A well-known example of an agency following Criterion 8 v.1 is the disclosure of the source code of the **COVIDSafe** contact tracing app (both the Android and Apple iOS variants). In 2020, the DTA was tasked with developing and delivering a contact tracing app in response to the COVID-19 pandemic. COVIDSafe was the result. It was released in April 2020. On 8 May 2020, the DTA publicly released the source code on the GitHub public code hosting and collaborative development platform.

Annexed hereto and marked '**FT-9**' are screenshots of the DTA's post announcing the public release of the source code, entitled 'DTA publicly releases COVIDSafe application source code', published on 8 May 2020, as archived by Internet Archive Wayback Machine on 26 October 2026 and accessed on 27 July 2026.

37. The announcement draws a distinction between the app source code, which was released, and the back-end service operated by the DTA (the 'COVIDSafe National Information Storage System'), which was not released:

Protecting the privacy of Australians downloading and using COVIDSafe is paramount. Prior to launching the application, the source code was reviewed by government security agencies, academics and industry specialists. We are releasing the app code, but to ensure the privacy of individuals and integrity of the overall system, the code that relates to the COVIDSafe National Information Storage System will not be released.

38. A DTA blog post published on or about 7 September 2020 entitled 'Key COVIDSafe improvements enhance and protect your privacy' announced an update to the COVIDSafe app and other news and updates.

Annexed hereto and marked '**FT-10**' are screenshots of the DTA's post entitled 'Key COVIDSafe improvements enhance and protect your privacy', published on or around 7 September 2020, as archived by Internet Archive Wayback Machine on 17 June 2021 and accessed on 27 July 2026.

The post also announced the public release of the full COVIDSafe Cryptography Specification:

On 8 May 2020, we released the app's source code to our GitHub repository (<https://covidsafe.gov.au/app-code-terms-and-conditions.html>). As part of our commitment to transparency, today we're releasing the COVIDSafe Cryptography Specification ([link](#)). We have worked with government experts, academia, industry specialists and the tech community to make sure the best security and privacy protections possible for all COVIDSafe app users.

The post also contains commentary on the improvement of the security of the COVIDSafe app and system since the initial release.

Working with subject matter experts in industry and academia, we have improved the COVIDSafe code and design. We have enhanced privacy by adding an additional layer of encryption to the Bluetooth exchange.

We also continue to work closely with government, industry, academia and members of the community – including software developers and researchers – to improve the security, privacy and usability of COVIDSafe. We would like to thank everyone for their feedback and recommendations, which continue to inform the development of the app.

39. The official website for COVIDSafe was hosted at <https://covidsafe.gov.au/>. This website is no longer available but archives of its content are available on the Internet Archive 'Wayback Machine'. A page on this site entitled 'Background to COVIDSafe' gave a comprehensive overview of the system, its purpose and implementation.

Annexed hereto and marked '**FT-11**' are screenshots of the 'Background to COVIDSafe' website as archived by the Internet Archive Wayback Machine on 22 December 2022, which is the most recent capture prior to the site becoming unavailable, accessed on 27 July 2026.

40. The 'Background to COVIDSafe' website section 'Australian Cyber Security Centre Assessment' explains that the ACSC, a division of the Australian Signals Directorate (ASD), conducted security testing assessments and (FT-11):

The ACSC has provided technical cyber security advice and assistance to the Digital Transformation Agency in relation to the security of COVIDSafe and its supporting infrastructure. This advice has been directed at ensuring that COVIDSafe is informed by best practice cyber security principles.

The final paragraph in this section says, in relation to the publicly available source code (FT-11):

A number of independent app developers and cyber security experts have provided assurance in relation to the security of COVIDSafe through review of the publicly available mobile application source code. This feedback was provided to the Digital Transformation Agency to inform later releases.

From this it can be inferred that the ACSC advice in relation to the cyber security of the COVIDSafe system either encouraged, or else was not at odds with, the disclosure of the source code of the COVIDSafe Android and iOS applications.

41. The COVIDSafe system deals with personal information of users including phone number, age range, postcode, and name (or pseudonym). This information is stored in the COVIDSafe National Information Storage System backend when a user registers their device. Registered devices perform 'digital handshakes' when in proximity, i.e. they exchange unique identifiers over the Bluetooth wireless interface. The network communication and protocol between the COVIDSafe app (on a user device) and the COVIDSafe National Information Storage Systems includes the registration procedure, and uploading recent 'digital handshakes' when the user has tested positive.
42. The COVIDSafe mobile app and the COVIDSafe system are similar to the myGov Code Generator app and myGov system in the following ways:
 - 42.1. The COVIDSafe app deals with sensitive, personally identifying information.
 - 42.2. The COVIDSafe app involves a registration procedure, and other interactions, that convey sensitive information to servers operated by a Government agency.
 - 42.3. The COVIDSafe app source code necessarily includes details about the network interactions and the locations of the servers, and details about the cryptographic and security mechanisms employed.
 - 42.4. The servers and backend systems operated by the agency store sensitive personal information and would be attractive targets for cyber threat actors, either to obtain access to the information stored on those systems, or to obtain access to those systems themselves, or to disrupt the operation of the system, or for other nefarious purposes.

Open source policy and regulation in other jurisdictions

43. Besides the Australian Government, many other governments have official policies or legislative instruments encouraging or mandating their agencies to disclose the source code of software applications they develop.
44. The Digital Service Standards and Measures report (FT-5) includes a review of 16 'comparable jurisdictions' digital service standards. These included 9 national governments, 5 Australian state governments, the Government of Ontario, and the Digital Standards policy of the United Nations Development Programme. Jurisdictions were selected based on having 'implemented digital service standards' and being 'considered leaders in online service delivery'. The table of jurisdictions and standards reviewed, and the selection criteria, are on pp 7-8 of the report (FT-5, pages 7-8).

45. Nine of the 16 jurisdictions reviewed had a criterion similar or equivalent to Criterion 8 v.1 (FT-5, Figure 5, page 11). These jurisdictions were: the USA, UK, Finland, New Zealand, the UN, and the states of New South Wales, Queensland, Western Australia and South Australia (FT-5, Figure 20, page 56).

The UK Technology Code of Practice

46. The United Kingdom's Technology Code of Practice (**UK-TCoP**) is the UK's government-wide standard for all technology projects or programmes. The standard is developed by the Government Digital Service (GDS) and Central Digital and Data Office (CDDO). It is mandatory for agencies to consider all points of the UK-TCoP as part of the 'Cabinet Office spend control process' for project funding.

Annexed hereto and marked '**FT-12**' are screenshots of the UK-TCoP on the official website at <https://www.gov.uk/guidance/the-technology-code-of-practice>, accessed on 27 July 2026.

47. UK-TCoP point 3 is (FT-12):

3. Be open and use open source

Publish your code and use open source software to improve transparency, flexibility and accountability.

48. The GDS and CDDO have published a collection of guidance documents that explain why this point is important, how to comply with it, and what kinds of source code should or should not be open to the public.

Annexed hereto and marked '**FT-13**' are screenshots of the 'Making source code open and reusable' guidance document accessed on 27 July 2026 at

<https://www.gov.uk/service-manual/technology/making-source-code-open-and-reusable>.

49. The GDS/CDDO guidance document 'Making source code open and reusable' explains that there are very few reasons not to publish source code, and cites code that relates to unannounced policy and code that protects against fraud as legitimate examples of source code that should not be disclosed:

When it's acceptable for code to be closed source

There are very few examples of code that must not be published in the open.

The main reason for code to be closed source is when it relates to policy that has not yet been announced. In this case, you must make the code open as soon as possible after the policy is published.

You may also need to keep some code closed for security reasons, for example code that protects against fraud. Follow the guidance on [code you should keep closed](#) and [security considerations for open code](#).

The same document distinguishes 'code with a security-enforcing function' from the fraud detection example and states that such 'security-enforcing code' does not need to be kept secret:

Making code with a security-enforcing function open

Code that contributes to your service's security does not need to be kept closed.

Many security-enforcing functions, such as cryptographic algorithms, are better when openly examined and understood while the keys are kept private.

Most cryptographic standards are developed in the open by standards authorities. UK public sector services use cryptographic security that's aligned with open, internationally recognised [standards and guidance from the National Cyber Security Centre](#).

50. Another GDS/CDDO guidance document entitled 'When code should be open or closed' affirms the distinction between 'security-enforcing code' and 'fraud detection algorithms'. It says that agencies 'should' keep algorithms used to detect fraud 'closed' (secret), and that:

You should open all other code. This includes:

- configuration code
- database schema
- security-enforcing code

Annexed hereto and marked '**FT-14**' are screenshots of the 'When code should be open or closed' guidance document accessed on 27 July 2026 at <https://www.gov.uk/government/publications/open-source-guidance/when-code-should-be-open-or-closed>.

51. Another GDS/CDDO guidance document entitled 'Security considerations when coding in the open' explains that 'security through obscurity' is not a valid approach to software security, and that 'Open code can be just as secure or more secure than closed code.':

Don't rely on closed code as your only security measure

You should use multiple countermeasures to keep your system secure, known as the '[defence in depth](#)' approach. You should not rely on keeping code closed to keep it secure. This is known as [security through obscurity](#), which is considered insufficient by security experts.

Attackers can still learn many details about your code when it is closed. By keeping your code closed, you can also introduce other risks and complications including:

- deprioritisation of code review
- additional costs and complexity of access controls

The technology team at the Ministry of Justice has [explained how it has considered the risks of keeping code closed and why it works in the open](#).

Open code can be just as secure or more secure than closed code. For example, cryptographic algorithms are open and prove their robustness through peer review. You should consider [which code should be opened](#).

Annexed hereto and marked '**FT-15**' are screenshots of the 'Security considerations when coding in the open' guidance document accessed on 27 July 2026 at <https://www.gov.uk/government/publications/open-source-guidance/security-considerations-when-coding-in-the-open>.

52. The 'Security considerations when coding in the open' guidance document (FT-15) references the UK Ministry of Justice (MoJ-UK) article 'Why we code in the open'. That article details the MoJ-UK's view on the benefits of publishing their source code and the security consequences.

Annexed hereto and marked '**FT-16**' are screenshots of the UK Ministry of Justice 'Why we code in the open' article accessed on 27 July 2026 at <https://mojdigital.blog.gov.uk/2017/02/21/why-we-code-in-the-open/>.

53. Among the benefits claimed by the MoJ-UK (FT-16) are reduced costs:

Building technology and making it secure costs money. Whether it's simply the time people spend discussing it, or in the security features or components used.

Keeping code confidential can be complex, leading to additional cost and leaving less money available to use securing the data the service handles.

The agency also refers to how source code transparency builds trust in government:

Transparency and freedom of information are important priorities at the Ministry of Justice. So being more open about our code, and the processes which lead to coding decisions, are vital parts of building trust in government.

54. The MoJ-UK believes that access to source code gives 'only a negligible advantage' to cyber threat actors (FT-16):

Doesn't it give attackers an advantage?

Although there's a common concern that coding in the open could give an advantage to an attacker, we believe that only a negligible advantage exists.

In fact there is no evidence to suggest that being open source makes software more susceptible to exploitation.

For example, publishing code in the open, especially when using good security discipline, is no riskier than closed source software where the binaries (the executable version of the source code) are public.

Lots of closed source software such as components, libraries and operating systems can be disassembled to reveal a similar level of detail to source code.

If you look at all the bugs in closed source products, the people that find the bugs don't have the source, they have [disassembly tools], it's out there and it's going to work on open and closed source binaries — get over it.

—Dr. Ian Levy, Technical Director, [NCSC](#), in [an interview with ZDNet](#) in 2013

The NCSC is the National Cyber Security Centre (NCSC-UK), the UK's apex cyber security agency which sits within the Government Communications Headquarters (GCHQ-UK) organisation.

European Digital Identity Wallet

55. Some jurisdictions have legislated that software developed by the government must be open source. The European Union Regulation (EU) **910/2014**, and Regulation (EU) **2024/1183** which amends 910/2014, are particularly relevant to the present matter.

Annexed hereto and marked '**FT-17**' and '**FT-18**' are the official English language versions of Regulation (EU) 910/2014 and Regulation (EU) 2024/1183, respectively.

56. Regulation (EU) 910/2014 is a legislative instrument of the European Parliament and the Council of the European Union, binding upon Member States, that seeks to (FT-17 at (2), page 257/73):

This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

In other words, it seeks to establish a digital identity framework for use throughout the EU.

57. Regulation (EU) 2024/1183 substantially amends 910/2014 to more precisely define the technical requirements of the digital identity framework and operational requirements for how member states participate in and deliver particular elements of the solution. The 'European Digital Identity Wallet' is the central element in the updated regulation. The preamble to 2024/1183 explains the role and purpose of the European Digital Identity Wallet (FT-18 at (7), page 2/56):

A more harmonised approach to electronic identification should reduce the risks and costs of the current fragmentation due to the use of divergent national solutions or, in some Member States, the absence of such electronic identification solutions. Such an approach should strengthen the internal market by allowing Union citizens, residents in the Union, as defined by national law, and businesses to identify themselves and to provide authentication of their identity online and offline in a safe, trustworthy, user-friendly, convenient, accessible and harmonised way, across the Union. The **European Digital Identity Wallet** should provide natural and legal persons across the Union with a harmonised electronic identification means enabling authentication and the sharing of data linked to their identity. Everyone should be able to access public and private services securely, relying on an improved ecosystem for trust services and on verified proofs of identity and electronic attestations of attributes, such as academic qualifications, including university degrees, or other educational or professional entitlements. The European Digital Identity Framework is intended to achieve a shift from the reliance on national digital identity solutions only, to the provision of electronic attestations of attributes valid and legally recognised across the Union. Providers of electronic attestations of attributes should benefit from a clear and uniform set of rules, while public administrations should be able to rely on electronic documents in a given format.

58. The European Digital Identity Wallet technical requirements include authentication of persons, verifiable electronic signatures by persons, and verifiable attestation of attributes of persons including, but not limited to: legal name; pseudonyms; address; age; gender; civil status; family composition; nationality or citizenship; educational and professional qualifications titles and licences; power and mandates to represent particular persons; public permits and licences; and for legal persons, financial and company data (FT-18 at ANNEX V, page 54/56; and ANNEX VI, page 55/56).

59. EU Member States are required to provide European Digital Identity Wallets implementations. 2024/1183 inserts Article 5a(1) into 910/2014 which states (FT-18 at Article 1(5), page 18/56):

For the purpose of ensuring that all natural and legal persons in the Union have secure, trusted and seamless cross-border access to public and private services, while having full control over their data, each Member State shall provide at least one European Digital Identity Wallet within 24 months of the date of entry into force of the implementing acts referred to in paragraph 23 of this Article and in Article 5c(6).

60. Member States are required to disclose the source code of their European Digital Identity Wallet implementations. 2024/1183, inserts Article 5a(3) into 910/2014 which states (FT-18 at Article 1(5), page 19/56):

The source code of the application software components of European Digital Identity Wallets shall be open-source licensed. Member States may provide that, for duly justified reasons, the source code of specific components other than those installed on user devices shall not be disclosed.

The preamble of 2024/1183 explains the motivation for this requirement (FT-18 at (33), page 7/56):

The transparency of European Digital Identity Wallets and the accountability of their providers are key elements to creating social trust and trigger acceptance of the framework. The functioning of European Digital Identity Wallets should therefore be transparent and, in particular, allow for verifiable processing of personal data. To achieve this, Member States should disclose the source code of the user application software components of European Digital Identity Wallets, including those that are related to processing of personal data and data of legal persons. The publication of this source code under an open-source licence should enable society, including users and developers, to understand its operation, audit and review the code. This would increase users' trust in the ecosystem and contribute to the security of European Digital Identity Wallets by enabling anyone to report vulnerabilities and errors in the code. Overall, this should provide suppliers with an incentive to deliver and maintain a highly secure product. However, in certain cases, the disclosure of the source code for the libraries used, communication channel or other elements that are not hosted on the user device, could be limited by Member States, for duly justified reasons, especially for the purpose of public security.

61. Regulation (EU) 2024/1183 and Regulation (EU) 910/2014, as amended and currently in force, draw a distinction between components installed on user devices (the source code of which 'shall be open-source licenced') and components not installed on user devices (the source code which the Member State 'may' withhold if 'duly justified'). It is apparent from the preamble and articles of 2024/1183 that the European Parliament and Council have paid careful attention to the security needs of the digital identity framework established by this

legislation and decided that, with respect to components installed on user devices, the security of the system is not compromised and the public interest is best served by mandating that the source code of those components be publicly disclosed under Open Source licences.

62. Fully open source reference implementations of the European Digital Identity Wallet system, including mobile applications for the Android and Apple iOS platforms, have been published by the European Commission at <https://github.com/eu-digital-identity-wallet>.

Artificial Intelligence (AI)

63. On 22 June 2026 the Australian Cyber Security Centre (ACSC), a department of the Australian Signals Directorate (ASD) published jointly with the apex cyber security agencies of Canada, New Zealand, UK, and USA a statement entitled 'Five Eyes cyber security agencies statement - The AI shift in cyber risk: why leaders must act now' (the **Five Eyes statement**). The opening paragraph declares the context and purpose of the statement:

As the leaders of the Five Eyes cyber security agencies, we are united in our call to action: the evolving landscape of artificial intelligence (AI) is rapidly transforming cyber risk, and we must act swiftly to remain ahead.

Annexed hereto and marked '**FT-19**' is the Five Eyes statement published on 22 June 2026.

64. The Five Eyes statement clearly conveys that AI is a powerful tool for both attackers and defenders (FT-19, page 2):

Use AI to strengthen defence

Adversaries are already using AI to move faster and more effectively. Defenders must do the same.

Organizations that integrate AI tools into their security operations can detect vulnerabilities earlier, improve software quality, monitor unusual behaviour, and respond faster to incidents – reducing both the cost and impact of incidents.

Success will not come from having the most tools. It will come from getting the basics right, acting quickly, and integrating cyber security into core business strategy.

65. On 21 July 2026 OpenAI, a leading AI company, disclosed a security incident involving an OpenAI autonomous AI system (the AI system). During an internal test to evaluate the performance of the system, it discovered and exploited vulnerabilities in OpenAI's test environment, escaping it. It then discovered and exploited vulnerabilities in the production services of another company, Hugging Face, Inc. The AI system included both recent publicly available AI models, and not-yet-released AI models.

Annexed hereto and marked '**FT-20**' are screenshots of the 20 July 2026 OpenAI announcement entitled 'OpenAI and Hugging Face partner to address security incident during model evaluation'.

66. The OpenAI article emphasises that the AI system discovered and exploited the vulnerabilities without access to source code of the systems involved (FT-20):

The incident also makes clear that advanced models can discover and exploit novel attack paths in real-world systems without source-code access. It highlights that advanced cyber capabilities must be developed alongside stronger safeguards and defensive tools.

Information about the App that is in the public domain

GitHub

67. There are two separate entries on the public platform, GitHub, which describe and/or replicate some details of the myGov Code Generator app (the App).
68. **GitHub** is a public source code hosting and collaboration service, currently owned and operated by Microsoft. Millions of developers and companies around the world use GitHub to host and collaborate on source code. Many projects and code ‘repositories’ are public (open source).
69. GitHub is based on the ‘Git’ version control system and tracks changes to code repositories over time. GitHub includes an ‘issues’ feature, which allows users to report problems or request features in a repository, and a ‘pull requests’ feature that enables GitHub users to propose changes to the code in a repository (which can subsequently be merged or rejected by a repository maintainer). Both of the ‘issues’ and ‘pull requests’ features support discussions, where users can comment on the content of the issue or pull request.
70. **GitHub Gist** is a service operated by GitHub for publishing ‘gists’, which are typically source code snippets, experiments, how-to guides, and proof-of-concept code. GitHub Gist web pages allow other Github users to leave comments on Gists.
71. I have been an active GitHub user since 2012.

mygov-totp-enroll repository

72. On 11 April 2019, GitHub user, ‘abrasive’ (James Wah), published on GitHub the ‘mygov-totp-enroll’ repository (**mygov-totp-enroll repository**).
- Annexed hereto and marked ‘**FT-21**’ are screenshots of the landing page of the Github repository posted by user, ‘abrasive’, as at 1 July 2026:
<https://github.com/abrasive/mygov-totp-enroll>.
73. The mygov-totp-enroll repository contained an alternative implementation of the myGov Code Generator enrollment workflow, serving as a functional substitute of the official App. In this workflow, a user performs an initial authentication to the official myGov Service using their account username and password, and the application requests a TOTP shared secret, and activates the TOTP two-factor authentication method for the user’s myGov account. The behaviour of the mygov-totp-enroll application which is contained in the GitHub repository diverges from the behaviour of the official App in what it does with the TOTP shared secret after retrieval. The official App stores it securely on the user’s mobile device on which the App is running. In contrast, the mygov-totp-enroll application presents the TOTP shared secret in a form that enables the user to enroll the TOTP shared secret in their preferred TOTP authenticator app (for example, Google Authenticator).

74. The source code contained in the 'mygov-totp-enroll' repository includes:

- 74.1. Approximately 90 lines of HyperText Markup Language (HTML) code across two files, defining the user interface;

Annexed hereto and marked '**FT-22**' are screenshots of the two files containing the HTML code, as at 1 July 2026:

<https://github.com/abrasive/mygov-totp-enroll/blob/master/instructions.html> and <https://github.com/abrasive/mygov-totp-enroll/blob/master/ui.html>.

- 74.2. Approximately 200 lines of application code written in the JavaScript programming language, in 1 file. Of this, approximately 90 lines implement the interactions with the myGov services, approximately 15 lines implement the presentation of the TOTP secret as a QR code, and the remainder deals with initialisation of the application and user interface and other 'boilerplate';

Annexed hereto and marked '**FT-23**' are screenshots of the code written in JavaScript programming language, as at 1 July 2026:

<https://github.com/abrasive/mygov-totp-enroll/blob/master/main.js>.

- 74.3. Invocations of behaviour provided by third party software packages related to network requests, data encoding and decoding, and QR code generation.

75. Following the publication of the mygov-totp-enroll repository, a series of improvements and bug fixes were made to the repository by various contributors including the original author.

76. GitHub users also filed problem reports or discussed proposed changes to this repository using the 'issues' and 'pull request' functions. It is evident from the issues and pull requests on the mygov-totp-enroll repository, and the associated discussions, that numerous people had success using the mygov-totp-enroll program to enable TOTP authentication on their myGov account. It follows that the implementation of the mygov-totp-enroll program, in respect of the TOTP enrollment protocol, its use of myGov Service Application Programming Interfaces (APIs), and its implementation and parameter selection for the TOTP algorithm, was correct such that it served as a functional substitute for the official *myGov Code Generator* mobile application.

Annexed hereto and marked '**FT-24**' are screenshots of the 'issues' and 'pull request' entries in which users discuss how to use the mygov-totp-enroll repository to enable TOTP authentication for their myGov account, as at 1 July 2026.

77. Based on the information reproduced in FT-21, FT-22, FT-23 and FT-24, it can be concluded that the source code in the mygov-totp-enroll repository published on GitHub contains identical or functionally equivalent information about the myGov service domain names, authentication protocol, API 'endpoints', and payload formats that would be present in the source code of the official App. Therefore, this information about the App and its interaction with the myGov Service is in the public domain.

mygov_totp_storage Gist

78. On 27 April 2021, GitHub user, 'hacker1024' (Joshua Leivenzon), published on GitHub Gist a 'gist' entitled 'Information about TOTP token storage in the App, as well as token extraction instructions' (**hacker1024 gist**).

Annexed hereto and marked '**FT-25**' are screenshots of the GitHub gist posted by hacker1024, including comments from other users as at 1 July 2026:

<https://gist.github.com/hacker1024/5d0845863e2dced27fd5eebc4ac95a39>

79. For the purposes of this affidavit, the term 'hacker' should be understood as someone with deep expertise in computer systems and who applies their skills enthusiastically to solve problems. The GitHub account name 'hacker1024' should therefore not be associated with malicious intent or nefarious activities.
80. The hacker1024 gist contained instructions for extracting the TOTP shared secret from the App's internal storage directory. These instructions include the following information about the App:
- 80.1. Where and how the encrypted TOTP shared secret and associated encryption key are stored within the App's internal storage directory;
 - 80.2. The encryption algorithms and parameters that the App uses to encrypt the TOTP shared secret;
 - 80.3. A 'hard-coded' (static) password which is used to decrypt the secondary encryption key, which in turn decrypts the TOTP shared secret;
 - 80.4. The TOTP algorithm parameters, particularly digest algorithm, number of digits, and time duration;
 - 80.5. The steps a user can follow to decrypt and decode the TOTP shared secret, and prepare it for use with other TOTP authenticator applications.
81. As evident from the screenshot reproduced in FT-25, several users wrote comments indicating that, by following the instructions, they successfully extracted the TOTP seed secret from the App's internal data storage. The publisher account, hacker1024, also posted a follow-up comment providing additional information about device requirements to successfully execute the instructions (FT-25).
82. As a result of the hacker1024 gist and associated comments from users reproduced in FT-25, accurate information about the App and its implementation, in particular how the App stores the TOTP shared secret, is in the public domain.

Reddit discussion

83. A Reddit discussion initiated by Reddit user 'j_l-w' in the r/australia forum on April 12, 2019, entitled 'for all the myGov fake 2FA haters', discusses myGov's two-factor authentication system (**j_l-w discussion**). The initial post in the discussion includes a link to the 'mygov-totp-enroll' GitHub repository owned by the GitHub user 'abrasive' (James Wah). It is apparent from the text of the initial post, and the correspondence of the name 'j_l-w' to 'James Wah', that Reddit user 'j_l-w' and GitHub user 'abrasive' are one and the same person.

Annexed hereto and marked '**FT-26**' is the Reddit post by user 'j_l-w' in the r/Australia forum as at 1 July 2026:

https://www.reddit.com/r/australia/comments/bc6gmv/for_all_the_mygov_fake_2fa_haters/

84. A Reddit user, 'Thingface', published two comments in the j_l-w discussion explaining how to intercept the network communications of the official App to read the TOTP shared secret, and an analysis of the protocol and intercepted message payloads (**Thingface comments**).

Annexed hereto and marked '**FT-27**' are screenshots of the two comments made by user, 'Thingface', on the Reddit post as at 1 July 2026:

https://www.reddit.com/r/australia/comments/bc6gmv/for_all_the_mygov_fake_2fa_haters/

85. Reddit user 'j_l-w' posted a follow-up message in response to the Thingface comments that includes a statement that he took a similar approach to analysing the behaviour of the official App.

Annexed hereto and marked '**FT-28**' is a screenshot of the follow-up message by Reddit user 'j_l-w' as at 1 July 2026:

https://www.reddit.com/r/australia/comments/bc6gmv/for_all_the_mygov_fake_2fa_haters/

86. The information about the protocol and messages published on Reddit by user 'Thingface' as captured in annexure FT-27 is in the public domain.

Affirmed by the deponent	)	
Fraser Tweedale at Brisbane	)	
on 29 July 2026	)	
before me:	)	Signature of deponent

.....
Signature of witness

Daniel Davison
Solicitor

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-1

The following is the annexure marked **FT-1** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains a screenshot of the details of Contract Notice CN4023201 from the AusTender website, accessed on 28 July 2026 at:

<https://www.tenders.gov.au/Cn/Show/2d04ff5e-c6cf-4299-82c6-c42965118aaa>

.....
Daniel Davison
Solicitor

Contract Notice View - CN4023201-A4 ▶ Contract Notice View - CN4253078 ▶ Contract Notice List ▶ Contract Notice View - CN4023201

Contract Notice View - CN4023201

AusTender holds Contract and Standing Offer Notices for the 07/08 financial year forward. For information related to previous years, please refer to <https://data.gov.au/data/en/dataset/historical-australian-government-contract-data>.

Subcontractors: For Commonwealth contracts that started on or after 1 December 2008, agencies are required to provide the names of any associated subcontractors on request. Information on subcontractors can be sought directly from the relevant agency through the Agency Contact listed in each Contract Notice.

Software Subscriptions and Services

Agency Details

Contact Name:
PURCHASING HELPDESK

Phone:
18 0090 6144

Email Address:

Office Postcode:
2900

CN ID: CN4023201

Agency: Services Australia

Publish Date: 14-Dec-2023

Category: Components for information technology or broadcasting or telecommunications

Execution Date: 29-Jun-2023

Contract Period: 1-Jul-2023 to 30-Nov-2026

Extension Options: 2

Max End Date: 30-Nov-2026

Contract Value (AUD): \$104,070,605.71
Original: \$27,147,639.88

Description: Software Subscriptions and Services

- Amendments:**
- [CN4023201-A4](#) - Execution of option, extension, renewal, or other mechanism outlined when the contract was initially awarded (8-Jul-2026)
 - [CN4023201-A3](#) - Variation to contract value (25-Feb-2026)
 - [CN4023201-A2](#) - Execution of option, extension, renewal, or other mechanism outlined when the contract was initially awarded (10-Jul-2025)
 - [CN4023201-A1](#) - Value increase and end date extension (5-Jul-2024)

Procurement Method: Open tender

ATM ID: SLS/001 and DTA-ICT-

SON ID: [SON3490955](#)

Suppliers Invited: 1

Confidentiality - Contract: No

Confidentiality - Outputs: No

Consultancy: No

Agency Reference ID: D341036849

Supplier Details

Name: Red Hat Asia Pacific Pty Ltd

Town/City: Brisbane

Postcode: 4000

State/Territory: QLD

Country: AUSTRALIA

ABN: 35 090 438 485

[Return to top](#) 

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-2

The following is the annexure marked **FT-2** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains the Digital Service Standard (DSS) version 1.0 published by the Digital Transformation Agency (DTA), as archived by the Internet Archive Wayback Machine on 26 February 2024 and accessed on 27 July 2026 at:

<https://web.archive.org/web/20240226185631/https://architecture.digital.gov.au/digital-service-standard-v1-full-text>

.....
Daniel Davison
Solicitor

Australian Government Architecture

Menu

Digital Service Standard v1.0

Notice

The [Digital Service Standard v2.0](#) was released on 4 December 2023. For the 2024-25 Budget process, agencies going through the DCAP Assessment will be required to meet the [Digital Service Standard v1.0](#).

This page outlines the Digital Service Standard v1.0. [Click here](#) for guides and tools on how to meet the Standard.

1. Understand user needs

Research to develop a deep knowledge of the users and their context for using the service.

Why it's in the Standard

You need to understand the people who use your service (your users) and what they want to do (their user needs) in order to build a service that works for them. You need to understand users and their needs from their point of view and not solely through the lens of the project you have been tasked with.

To do this, you will need to really understand what users are trying to do when they encounter your part of the service and you need to design services that address that context. This will often involve understanding things that are not 'in scope' or part of your responsibility so that you can design better services.

You will need to understand all aspects (end to end and across channels) of your users' current experience. You should include as users everyone who is involved in the service delivery: end users, public servants delivering the service and other intermediaries who support end users to access the service.

Your user research needs to cover a wide range of users and show that you understand how different user scenarios may impact service design and delivery. You must include from the earliest stages users who may need assistance to interact digitally, or are unable to interact digitally at all.

2. Have a multidisciplinary team

Establish a sustainable multidisciplinary team to design, build, operate and iterate the service, led by an experienced product manager with decision-making responsibility.

Why it's in the Standard

Good government services are built quickly and iteratively, based on user needs. Your [digital delivery team](#) must be set up in the right way to do this.

They need:

- ▶ a broad mix of skills and roles from the start
- ▶ quick decision-making processes and the ability to change and adapt as the service evolves
- ▶ to be adequately resourced and empowered to deliver the product or service

3. Agile and user-centred process

Design and build the service using the service design and delivery process, taking an agile and user-centred approach.

Why it's in the Standard

Designing services in a user-centred way means that the services you deliver will be easy to use and convenient for the people who need to use them, helping them to stay in the digital channel.

Designing using agile methods allows you to be more proactive and respond easily to change, both in technology and government policy. Services should be improved frequently; they will be cheaper and more accountable to users.

4. Understand tools and systems

Understand the tools and systems required to build, host, operate and measure the service and how to adopt, adapt or procure them.

Why it's in the Standard

The technology you choose to build your service must help you respond quickly and regularly to the needs and expectations of users. This criteria makes sure you:

- ▶ consider all the risks and constraints associated with the technology you choose
- ▶ avoid contracts that lock you into particular solutions and limit your ability to make decisions to improve the service
- ▶ build a sustainable system that can be easily managed once live
- ▶ identify the required infrastructure to successfully and continuously deliver the digital service
- ▶ have a procurement approach that will not restrict, inhibit or limit ongoing and future service delivery
- ▶ consider existing tools and systems and avoid unnecessary fragmentation and/or costs
- ▶ consider appropriate tools and systems already in use in government
- ▶ embed measurement tools at the start of development

5. Make it secure

Identify the data and information the service will use or create. Put appropriate legal, privacy and security measures in place.

Why it's in the Standard

People who use government services must have confidence that:

- ▶ any information they provide is confidential and stored appropriately
- ▶ the system they're using is safe and secure
- ▶ they know how their information will be used by government
- ▶ they can easily retrieve information they provide

If a service cannot guarantee confidentiality, integrity and availability of the system, people will not use it.

6. Consistent and responsive design

Build the service with responsive design methods using common design patterns and the style guide for digital content.

Why it's in the Standard

Using responsive design, following common design patterns and style guidance for digital content, and making sure the service is accessible means it will be user-friendly,

inclusive, adaptable, and measurable. It will also be available on the platforms and devices that users choose.

Consistent design that is responsive to different devices helps you to save time and money by re-using something that already exists that follows better practice, and is based on data and user research. This means you can concentrate on the unique things your service needs to do.

Responsive design ensures that users can interact with your service regardless of their device size or type, and browser or device processing power. The service should follow mobile-first design principles, consider users on slow internet connections or

with limited download data, work well for both mouse and touch devices, and use front-end technology that works well regardless of device processing power.

Writing and designing content so it is consistent, plain and in the language of your users helps people gain trust and confidence in using different services. By providing information they can easily understand they may be less likely to use alternative websites that could be misleading.

7. Use open standards and common platforms

Build using open standards and common government platforms where appropriate.

Why it's in the Standard

Using open standards and common government platforms helps you to:

- ▶ meet the needs of your users by building with proven solutions
- ▶ make users' experience of government more consistent, which generates trust
- ▶ save time and money by reusing things that are already available
- ▶ be more efficient by sharing data appropriately
- ▶ move between different technologies when you need to, avoiding vendor lock-in

8. Make source code open

Make all new source code open by default.

Why it's in the Standard

It's important to share your source code so others with a similar need can reuse it.

Open source helps to:

- ▶ reduce costs for your project and others'

- ▶ avoid lock-in
- ▶ stop duplication
- ▶ increase transparency
- ▶ add benefits, from improvements by other developers

9. Make it accessible

Ensure the service is accessible and inclusive of all users regardless of their ability and environment.

Why it's in the Standard

You need to make sure everyone who needs your service can use it. This includes people with disability and older people, and people who can't use, or struggle with, digital services.

Your service must be accessible to users regardless of their digital confidence and access to a digital environment. This includes users in remote areas and users with different devices.

You also have a legal requirement to ensure your service is usable and accessible to people with disabilities (see the [Disability Discrimination Act 1992](#)). Australian Government agencies are required to meet the Web Content Accessibility Guidelines ([WCAG](#)) [Level 2.1](#)

10. Test the service

Test the service from end to end, in an environment that replicates the live version.

Why it's in the Standard

All government services should be user-friendly and easy to use, regardless of the technology your users use, their expertise with the subject matter, or their level of digital skill.

You cannot wait until the service is live to discover problems that stop people from using the service. You need to rigorously and comprehensively test every part of the service during development.

11. Measure performance

Measure the performance of your service and understand what outcomes it is delivering. Report results to your stakeholders openly and regularly to encourage continuous improvement.

Why it's in the Standard

Every service should aim for continuous improvement. Metrics are an important starting point for discussions about a service's strengths and weaknesses. By measuring performance, you can help answer questions that people care about.

- ▶ what is and isn't working?
- ▶ what value or benefit does this service provide to users?
- ▶ where can a service be improved? (time, cost, ease of use)
- ▶ have we achieved what we set out to achieve?

There are a few common problems to avoid in performance measurement for government services:

- ▶ the achievement of targets or outputs becomes more important than meeting user needs
- ▶ reliance on what is easy to count, rather than what should be counted
- ▶ failure to adjust to social, demographic, and economic factors that impact performance data
- ▶ measuring after something has changed, without getting a baseline to compare to first.

What is a performance indicator?

A performance indicator is a signal used to monitor a service or system. These signals can include:

- ▶ inputs/outputs – such as money, headcount, physical resources, human resources, time
- ▶ activities – such as calls responded to, units delivered, reports completed
- ▶ outcomes – the result a person experienced because they used a service.

Input and activity data provide only part of the picture of how a service is performing. This is where user research can help you learn more about why something is performing the way it is.

By using a combination of qualitative and quantitative indicators, you will be better placed to understand what is happening for your service and why.

Key performance indicators

Identifying and capturing the right indicators can ensure all your decisions for new or existing services are evidence-driven. The following key performance indicators are a strong start to monitoring your service:

- ▶ outcome – what outcome happened for a person because they interacted with the service?

- ▶ value add – what are the user benefits of this service? What is the return on investment?
- ▶ completion rate and time – how easy or fast is it for a person to move through your service? How many people drop out and do not complete, and why?
- ▶ cost per transaction – how cost efficient is your service for the user and for government?

There are other metrics your service can use to understand how it is performing, such as:

- ▶ error rates
- ▶ uptime – including cloud service performance
- ▶ response/load times – use global standards to compare your results (current best practice is 2 seconds or less)
- ▶ content metrics – such as readability level, scroll depth, and search bar use
- ▶ audience – is your service reaching the expected demographics? Why or why not?
- ▶ repeatability – is the service provided in a consistent and dependable manner?
- ▶ digital take up – this shows how your digital service is being used compared to alternate channels. It can be helpful to understand which channels are more popular or accessible, and why. Remember that not all services and not all people are able to use a digital option
- ▶ user satisfaction – where and how you ask for this feedback matters. Consider face-to-face and anonymous avenues for feedback to support people in providing honest responses.

If your service is compliance based, ways to measure user satisfaction could include:

- ▶ communication and expectations – people know what to do and how long it will take up front, and what they are told is what happens
- ▶ fairness – people may not be happy with the result, but feel they were treated fairly and with respect throughout the service
- ▶ behavioral changes – for example, people demonstrate changes in actions or decisions
- ▶ self-identified results – people provide feedback on how a service made a difference in their life or helped them meet a need.

Be wary of commercial methods of measuring user satisfaction such as Net Promoter Score. These types of measurement do not always translate well in the public arena because they assume people using a service can take their business elsewhere or are interacting with the service by choice.

Share your results

No service can be monitored in a vacuum. Share results with your team to identify areas of improvement. This keeps the team human-focused and makes it easier to explore and prioritise enhancements.

Share results with your stakeholders to tell the story of how the service is currently

working, and to raise any issues that may impact service delivery early. Think beyond reports, such as showcases, blogs, short videos and inter-agency meet-ups. Find interactive ways to help communicate more broadly the results your service is experiencing.

Share key metrics with the public and the people who access your service. This builds trust and can encourage people to give you feedback, because it demonstrates you listen and use it to make the service better for themselves and others.

Always consider the audience you share your performance results with, and ensure you are meeting [Australian privacy principles and laws](#).

12. Don't forget the non-digital experience

Ensure that people who use the digital service can also use the other available channels if needed, without repetition or confusion.

Why it's in the Standard

People often start using a service and have to come back to it later, or switch to a non-digital channel to complete the transaction. We need to make sure users' transitions between non-digital and digital channels (when they need to happen) are as smooth as possible.

13. Encourage everyone to use the digital service

Encourage users to choose the digital service and consolidate or phase out existing alternative channels where appropriate.

Why it's in the Standard

As we build user-friendly, inclusive, adaptable, and measurable, government services, the digital channel will become more convenient for users than non-digital channels like post, phone and shopfronts. Increased digital take-up will mean users can spend less time interacting with government. This will result in greater cost efficiencies for government.

We still need to help users who are unable to use digital channels and provide support to those who need it. But we want to ensure digital channels are used whenever possible and to scale back, or phase out, alternative channels when we can.

Was this information helpful?

☐ Yes

☐ No



An Initiative of the Digital
Transformation Agency

[Contact us](#)

Social media



LinkedIn



Twitter



RSS

[Privacy](#) | [Disclaimer and copyright](#) | [Accessibility](#)

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-3

The following is the annexure marked **FT-3** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains screenshots of the DTA blog post 'Open and secure' published on or about 14 August 2015, as archived by Internet Archive Wayback Machine on 25 June 2022 and accessed on 27 July 2026 from:

<https://web.archive.org/web/20220625075027/https://www.dta.gov.au/blogs/open-and-secure>

.....
Daniel Davison
Solicitor



[Home](#) > Open and secure

Open and secure

Mark McKenzie – 14 August 2015

Tags: [Open source](#) [Security](#) [Collaboration](#)

Yes, you really can. We've all seen that security through obscurity doesn't work. It leaves us in the dark on how our data is stored, protected and used.

You shouldn't have to take our word that our systems are secure, or that we fix our vulnerabilities - you should be able to see it in our designs, our code, our build and our operations. Being open invites trust - you should be able to trust us not because we tell you that you should, or because we're the only supplier, but because we've earned it.

Our mantra is 'simpler, clearer, faster and more humane public services', and that means considering the needs of our users above all else. Our approach to security is no different. By being open and transparent our users can see what our systems are doing, which is a key part of treating our users humanely.

To showcase the security of our designs, our code, and our operations, we've implemented a few practices.

Open code

Our code, where possible, will be published in public Github repositories and can be downloaded by anyone. The only exception is when we're prevented by contract or law, and we'll generally try to avoid those situations if we can. Our designs will be published under the same principle. Where we go to the trouble of certifying or security testing our software or systems, we'll publish the reports in as much detail as possible.

RSS feeds

[Our feeds](#)

Sign-up for DTA updates

If you would like to receive email notification when we publish news and blogs, please fill in the form.

* indicates required

Email address *

First name

Last name

State or territory

[Subscribe](#)

We think the good guys outweigh the bad

A question you might be asking is: Why all this openness? Doesn't it give the bad guys an advantage? We think it gives the good guys a bigger one. Any user, or indeed any organisation, can look over the code for weaknesses. For example, we're looking at using the codebase from GOV.UK as part of the basis for one of the DTO's work programs. We can look over the code, and if we find a bug, we can either report it or even fix it directly. If GOV.UK was closed, we'd pay to use the codebase and they may not ever find certain vulnerabilities (which doesn't mean the bad guys haven't found them), or never fix them if they do.

Collaboration

We know we've got some really smart people here, but we also know that we don't have a monopoly on them. So we'd love you to take our code and look at it, use it, analyse it, fork it, or even contribute to it. If you find an issue like a bug or something you'd like changed, let us know by lodging a ticket against the code in Github. Then we can prioritise, find and fix it - quickly.

We're building confidence and trust in our systems by being as open and honest with our users as possible. You'll be able to see that we're implementing security right through our designs and code, you'll be able to understand why we get gold certification stamps for security from our certification partners, and you'll appreciate that your data is looked after by us because we operate our systems with the same transparency principles.

We have smart people developing for us, but you're smart too, so we'd love you to join us in making Australian services great. We also want other Australian Government organisations to be as open as us - you're more than welcome to contribute to our software, or host your own in Github inside our organisation.



[Contact us](#) [Join our team](#) [Accessibility](#) [Cookies](#) [Privacy](#)
[Disclaimer and copyright](#)

© Commonwealth of Australia. With the exception of the Commonwealth Coat of Arms and where otherwise noted, this work is licensed under the CC BY 4.0 license.

Social media

 [Twitter](#)
 [Facebook](#)
 [LinkedIn](#)

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-4

The following is the annexure marked **FT-4** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains screenshots of the article 'Making source code open' published on the DTA website on or about 20 February 2017, as archived by Internet Archive Wayback Machine on 17 March 2022 and accessed on 27 July 2026.

.....
Daniel Davison
Solicitor



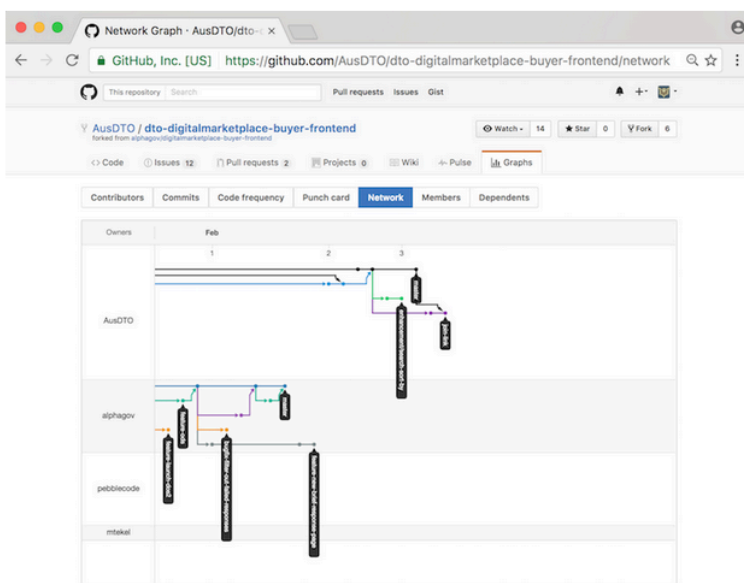
[Home](#) > Making source code open

Making source code open

Alastair Parker – 20 February 2017

Tags: [Open source](#)

Deciding whether or not something should be made open source can be a tricky decision. Firstly, knowing what you're trying to achieve, and then understanding how you can get there, will make the decision a little easier. Here are three options to consider: collaborative open source, open source and closed source.



Caption: This image shows contributions to the DTA's open source Digital Marketplace from the UK's Government Digital Service and people in the community.

RSS feeds

Our feeds

Sign-up for DTA updates

If you would like to receive email notification when we publish news and blogs, please fill in the form.

* indicates required

Email address *

First name

Last name

State or territory

Subscribe

Collaborative open source code

What is it?

Equal parts product, community and collaboration. It might have started off as only your project but it's much more than that now. The community might now be dependent on this code.

Why would I?

You have made something that solves your problems, and you know it will solve other people's as well. There are features you want implemented but you don't have the time.

How do I?

It can be a lot of work, but it will pay off when you start getting features implemented for free by others. Before anyone else starts helping out, you'll have to make it easy for them.

There aren't any hard and fast rules, but there is a good chance you'll want to have:

- **great developer documentation:** remember that people will be contributing because they want to not because they have to. Write the kind of documentation you would want to read.
- **automated tests:** nobody likes integrating with code that doesn't work. Unless you want to spend all your time debugging, you will want people to write tests for their own code.
- **clear and simple structure:** your project should be well laid out with well named packages and classes. Your code should be easy to read and clear about what it is doing and why. Nobody cares how clever you are and how much you can achieve with a single line of code. Aim for 10 lines per method.
- **well structured code:** your code should be in standalone parts that are reusable on their own. Make it easy for people to reuse the bits they want without having to pull apart everything you've done.
- **contribution guidelines:** tell your contributors how you want things done and what can they do to maximise the chances of you accepting their new code. There are guidelines out there that can help you. [Here is an example from GitHub.](#)

Anything else?

You will need to dedicate some time to growing and nurturing your community. Questions will need answering, issues will need filing, releases will need releasing. Always keep in mind that this is now bigger than you and your team, and you might not always have total control of what happens. We're all in this together. Anything we can do to reuse code and minimise costs to the community is worth any extra effort.

Let us know if you take this direction. We would love to see what you've done. We might even contribute.

Open source

What is it?

Code that is available to others, but you aren't helping them use or improve it. It isn't bad code, but you haven't gone the extra mile to make it collaborative.

Maybe you've started something that others will be able to expand upon and reuse? Maybe it will inspire others about new ways they can solve their own problems? You never know, someone might have been struggling with exactly the same thing!

Making your code open source is not giving away user data.

[Criterion 8](#) of the [Digital Service Standard](#) tells teams to be open by default, but this can be difficult for some teams. First timers can be unsure about what extra work going 'open source' will mean. Others feel that their code shouldn't be open source because nobody else would want it. I've also heard that code can not be open sourced because of security reasons. These are all important considerations for teams.

If you have secrets littered through your closed source code, someone will eventually find them. Anyone who views your site has access to your HTML and javascript at the click of a button. It's not as simple for mobile and desktop apps, but still very achievable. [Industry best practice](#) tells us to separate our code from the secrets it uses. If you haven't done this, it's unlikely you'll meet criterion 5 of the Digital Service Standard: [Make it secure](#).

Why would I?

Government code should be available to others unless there is a compelling reason. Everyone in the public service benefits from being able to reuse code that others have developed. We all work for the taxpayer and they should be able to see and use what they've paid for.

How do I?

Start today! Sign your department up to an online open source community and add your product. We use [GitHub](#) but you can use whatever works for you and your department.

We have a [guide about sharing code](#) that will give you more information about how to make your code open.

At some point in your journey you will need to pick an open source license for your code. The [Choose a License website](#) is a good resource to get you started on the different types of licences available. They can be a little hard to read, so seek legal advice on the licenses if you're unsure.

If you're struggling to get started, let us know! We're happy to give you a hand.

Anything else?

Try to find some time to make your work easier for others to reuse and contribute to. If nothing else, it will help the people who take over maintaining what you're working on.

Closed source

What is it?

Pretty much exactly what it sounds like. The source code is only available to the authors and a select few within their agency.

Why would I?

Once teams understand more about what open source is, and isn't, they find they don't usually have any reason not to be open. However, it is common for teams to be concerned about security.

Security is a very valid reason, but you shouldn't use it as an excuse to close everything. Keeping passwords and keys private helps to keep our user's data private and secure. Not only is it good practice, it's part of the obligation we have in serving the public. Code that doesn't contain these secrets can be shared and reused by others.

There are lots of examples of world class security products that are open source. Talk with your department's [ITSA](#) (Information Technology Security Advisor) for specific advice.

Many private sector organisations close their code to maintain control of their brand and their user experience, in government, we don't have those issues.

How do I?

Simple. Keep doing what you are already doing. **But remember:** having closed source code doesn't mean you can get lazy. People will still need to read and update your code, it could be around for a long, long time. Take pride in your work and code like the world is watching.

Anything else?

Have a careful think if there are any parts of your code that might be useful to others. The code doesn't have to come from your primary product. Tools and utilities you've written might be useful for others in similar circumstances.

If you can't find any code to make available to others, see if you can offer products as open services instead. At least that way government won't have to reinvent the wheel.

If you'd like some help or just to get in touch, leave us a comment below.

Alastair Parker is an architect at the Digital Transformation Agency.



[Contact us](#) [Join our team](#) [Accessibility](#) [Cookies](#) [Privacy](#)
[Disclaimer and copyright](#)

Social media

Twitter
 Facebook
 LinkedIn
 YouTube

© Commonwealth of Australia. With the exception of the Commonwealth Coat of Arms and where otherwise noted, this work is licensed under the CC BY 4.0 license.

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-5

The following is the annexure marked **FT-5** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains the DTA Report, 'Digital Service Standards and Measures', dated 9 June 2023.

.....
Daniel Davison
Solicitor



Australian Government
Digital Transformation Agency



Digital Service Standards and Measures

Analysis of approaches for international and domestic digital service standards and measuring digital service delivery performance

9 June 2023

Digital Transformation Agency



© Commonwealth of Australia (Digital Transformation Agency) 2019

With the exception of the Commonwealth Coat of Arms and where otherwise noted, this product is provided under a Creative Commons Attribution 4.0 International Licence.

<http://creativecommons.org/licenses/by/4.0/legalcode>

The Digital Transformation Agency has tried to make the information in this product as accurate as possible. However, it does not guarantee that the information is totally accurate or complete. Therefore, you should not solely rely on this information when making a commercial decision.

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties with accessing this document, please email communications@dtg.gov.au.

Version: 1801

Contents

Executive Summary	4
1. Introduction	6
<i>Digital Service Standards</i>	<i>7</i>
<i>Common Characteristics</i>	<i>9</i>
<i>Value Drivers</i>	<i>10</i>
<i>Focus Areas</i>	<i>10</i>
2. Principles	11
<i>Principles Included</i>	<i>11</i>
<i>Emphasis on outcomes vs. inputs</i>	<i>15</i>
<i>Structure of standards</i>	<i>17</i>
<i>Lessons learned</i>	<i>18</i>
3. Services Covered	19
<i>Common criteria</i>	<i>19</i>
<i>Lessons Learned</i>	<i>21</i>
4. Compliance and Adoption	22
<i>Compliance archetypes</i>	<i>22</i>
<i>Common challenges</i>	<i>29</i>
<i>Assessments across project lifecycle</i>	<i>30</i>
<i>Driving compliance without mandates</i>	<i>30</i>
<i>Lessons Learned</i>	<i>31</i>
5. Supporting Components	32
<i>Guides, design systems and tools</i>	<i>32</i>
<i>Enablement and awareness</i>	<i>36</i>
<i>What others are finding most useful</i>	<i>38</i>
<i>Lessons Learned</i>	<i>39</i>
6. Measuring Performance	40
<i>Recommended metrics</i>	<i>40</i>
<i>Mandated metrics</i>	<i>42</i>
<i>Measuring WofG performance</i>	<i>43</i>
<i>Additional Guidance and Tools</i>	<i>45</i>
<i>Lessons Learned</i>	<i>46</i>
7. Maintaining the Standard	47
<i>Refreshing the standard</i>	<i>47</i>
<i>Measuring effectiveness</i>	<i>51</i>
<i>Lessons Learned</i>	<i>52</i>
8. Conclusion	53
9. List of abbreviations	55
Appendix A: Principles	56
Appendix B: Structure	71

Executive Summary

The Australian Government is considered a leader in digital service standards and was one of the first jurisdictions globally to establish one. The DTA's Digital Service Standard (DSS) was published in 2016. Reviews of the DSS were completed in 2017 and 2021, and in 2021 some work was completed towards a refresh but was not progressed past Beta. Assessments against the DSS are no longer consistently completed.

Since 2016, much has changed in the landscape of digital government service delivery, and there is an opportunity to refresh the standard. Rapid advancements in technology have unlocked new opportunities to improve services and customers' expectations for service delivery have risen exponentially. The government landscape has also evolved, as the Australian Government continues to target an ambitious forward-looking vision for customer centric service delivery. There has also been significant increase in overall digital maturity and familiarity with modern digital ways of working, meaning some principles may no longer resonate or be aligned to strategic objectives.

Ensuring the DSS aligns to modern best practices will be important to achieving whole-of-government (WofG) strategic objectives. It is a key part of the Australian Government Architecture (AGA) and sets expectations for what good service delivery looks like across WofG. It will help to achieve the Australian Government's ambition for world class digital service delivery, as articulated in the 2023 Digital and Data Strategy, myGov User Audit and APS Review recommendations.

In May 2023, The Boston Consulting Group (BCG) was engaged by the Australian Digital Transformation Agency (DTA) to conduct research into international and domestic digital service standards and how to measure what good service delivery looks like. This included desktop research into 17 comparable jurisdictions' digital service standards and measurement approaches. It also included interviews with 14 representatives from government digital service standards teams across 8 jurisdictions, and over 10+ subject matter experts in design across the public and private sectors to gain firsthand insights into lessons learned.

This document contains findings on lessons learned across 6 focus areas: principles, services covered, compliance and adoption, supporting components, measuring performance and maintaining the standard.

Research across the focus areas revealed several key findings which can be used to inform future updates to the DSS.

Governments globally are designing their digital service standards and principles to signal change and target areas of lower digital maturity. Most standards set expectations for both ways of working and service delivery outcomes to cater for variability in WofG digital maturity. Research provides insight on potential ideas to consider adding or de-emphasising, to account for new areas of interest and areas which may no longer be resonating.

Most digital service standards are applied to new or renewed public-facing informational and transactional services, although 40 per cent of jurisdictions researched have expanded scope to include internal employee-facing services as well.

To drive adoption and compliance of standards, many jurisdictions have implemented mandates, however not all are strongly enforced. Where standards are not mandated, they are published only as guidance to set a north star for service delivery. The degree of mandate and enforcement of standards is dependent on a jurisdiction's culture, level of centralisation, political trade-offs, availability of resources and presence of powers to enforce consequences (e.g., funding controls, domain controls). Both approaches of enforcing mandates and publishing standards as guidance have potential to drive positive outcomes, but key success factors must be considered for each.

Regardless of approach to compliance, leading governments drive adoption by making the standards useful through supporting manuals, playbooks, guides, reusable tools and design systems. They have also invested significantly in enabling teams through training, trusted advisory services, and communities of practice (CoPs). As digital maturity increases over time, governments must move from early-stage educator to mature advisor, to ensure the highest quality and consistency of services.

Most jurisdictions encourage the measurement of service delivery performance through their digital service standards. Many governments include measurement principles, recommend metrics for measurement, provide detailed guidance to support teams in the selection of additional metrics, and advise teams in the use of data collected to improve services over time. Some governments have also endeavored to understand performance at a WofG level using these measurements or WofG analytics platforms.

Lessons learned indicate that standards should be refreshed regularly and maintained centrally, while supporting components (guides, tools, design systems) should be continually updated with input from the broader government community to ensure they remain effective, useful and relevant. While many jurisdictions are not formally measuring the effectiveness of their standards, some governments rely on formal and informal feedback and other basic indicators (e.g. page downloads, number of assessments completed) to measure use and effectiveness of the standard.

1. Introduction

The Australian Government is considered a leader in digital service standards and was one of the first jurisdictions globally to establish one.

The DTA's Digital Service Standard (DSS) was published in 2016. Reviews of the DSS were completed in 2017 and 2021, and in 2021 some work was completed towards a refresh but was not progressed past Beta. Assessments against the DSS are no longer consistently completed.

Since 2016, much has changed in the landscape of digital government service delivery. Rapid advancements in technology have unlocked new opportunities to improve services, and customers' expectations for service delivery have risen exponentially. Boston Consulting Group (BCG) research shows that 93 per cent of Australians expect digital government services to be as good as those provided by public and private sector leaders¹ and approximately 90 per cent say digital customer experience impacts trust and confidence in government².

The government landscape for digital service delivery has also evolved. The Australian Government continues to have an ambitious forward-looking vision for customer centric service delivery, and there has been significant increase in overall digital maturity and familiarity with modern digital ways of working. For example, the Australian Government [Digital Review](#) identified that between 2018 and 2021, WofG digital maturity increased significantly, and most agencies are now considered advanced. As a result, some principles may no longer resonate.

Ensuring the DSS remains current and aligns to modern best practices will be important to achieving WofG strategic objectives. It is a key part of the [Australian Government Architecture](#) (AGA) and sets expectations for what good service delivery looks like across WofG. It will also support the vision for customer centric service delivery as articulated in the Australian Government's [Data and Digital Government Strategy](#), the [myGov User Audit](#) and [APS Review](#). The DSS will play a key role in improving accessibility and inclusion and enabling the delivery of simple and seamless digital services that foster trust.

¹ BCG Citizen Satisfaction Survey 2022

² BCG and Salesforce Trust Imperative 2021

Digital Service Standards

In May 2023, BCG was engaged by the Australian Digital Transformation Agency (DTA) to conduct research into global digital service standards and service delivery performance measures. The resulting findings will be used to inform a refresh of the Australian Government's DSS, identify opportunities to promote compliance and adoption across agencies and provide considerations for the measurement of service delivery performance across WofG.

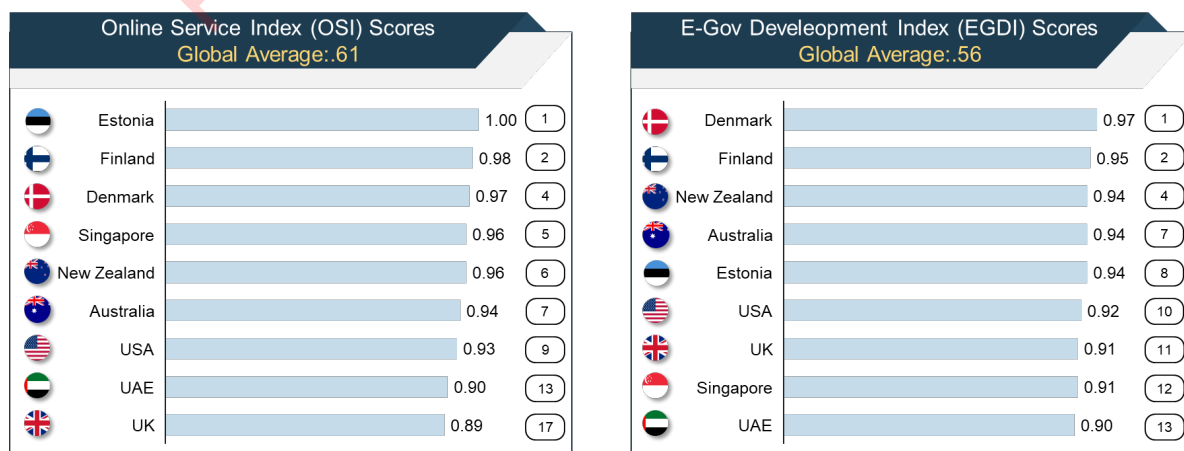
Research included review of 17 comparable jurisdictions' digital service standards and measurement approaches. It also included interviews with 14 representatives from government digital service standards teams across 8 jurisdictions and over 10+ subject matter experts in design across the public and private sectors.

Figure 1: 17 jurisdictions selected for deep dive analysis

Government	Standard
 Australian Govt	DTA Digital Service Standard
 US Federal Govt	USDS Digital Services Playbook
 UK Govt	GOV.UK Service Manual
 Finnish Govt	Principles of Digitalisation
 Danish Govt	Development Guide for Public Digital Services
 UAE Federal Govt	Digital Customer & Digital Government Service Policy
 Singapore Govt	GovTech Digital Service Standards
 New Zealand Govt	Digital Service Design Standards
 Federal Govt of Germany	Service Standard
 Estonian Govt	Digital Service Principles
Organisation	Standard
 UNDP	UNDP Digital Standards
Government	Standard
 Govt of Ontario	Digital Service Standards
 Western Australian Govt	Digital Service Design Principles
 South Australian Govt	Digital Services Standards Policy
 Queensland Govt	Digital Service Standards
 New South Wales Govt	Digital Service Toolkit
 Victorian Govt	Digital Design Principles

Jurisdictions were shortlisted for this research based on two criteria; they have implemented digital service standards or comparable policies, and they are considered leaders in online service delivery. For example, they rank highly on both the UN E-Government Online Service Index and E-Government Development Index (if included in this index).

Figure 2: UN E-Government Survey (2022) rankings



(n) Overall ranking in full list of countries surveyed

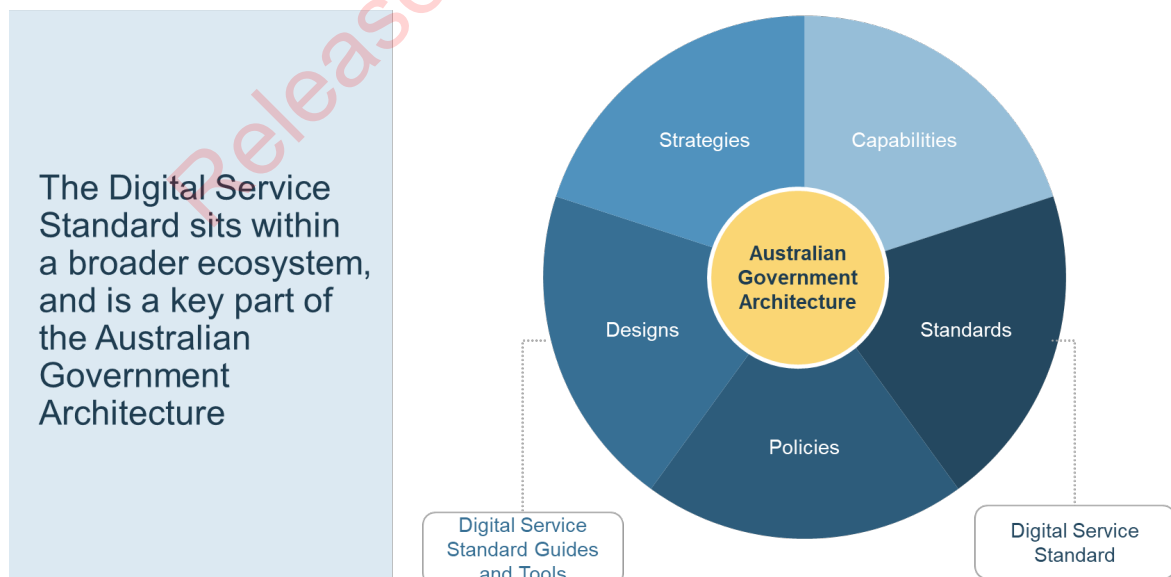
Common Characteristics

Digital service standards are usually part of a broader digital government ecosystem. While the composition of this ecosystem varies by jurisdiction, they share some common characteristics or features. Almost universally, at the centre of digital service standards are principles aligned to broader digital service delivery strategy. These principles are supported by common components which vary by jurisdiction, but can include design manuals/playbooks/guides, design standards/requirements, design systems and communities of practice (CoPs).

On a broader scale, these standards work alongside wider government policies and strategies (e.g. accessibility, privacy and security standards), core and common platforms (e.g. digital identity, payments, notifications, central WofG service delivery platforms), broader government reform agendas, and digital capability uplift and enablement programs.

In Australia, the DSS forms a key part of the Australian Government Architecture (AGA); a decision-making and policy framework that helps agencies develop scalable, secure and resilient digital capabilities. Guides and Tools (e.g. requirements for Australian Government websites) related to the DSS also form part of this architecture.

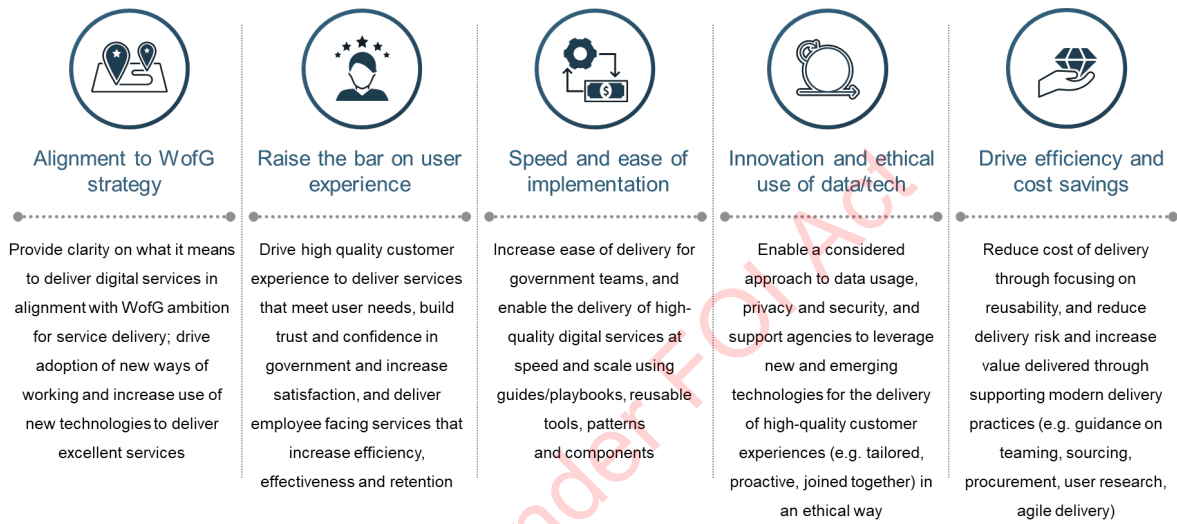
Figure 3: DSS within the Australian Government Architecture



Value Drivers

Digital service standards set expectations for what good digital service delivery looks like across WofG. In doing so, they can be designed to maximise value across 5 key areas: aligning to WofG strategic objectives, improving customer and employee experience, increasing speed and ease of delivery of digital services, encouraging innovation and ethical use of technology, and driving efficiency and cost savings.

Figure 4: 5 ways digital service standards deliver value for customers and government



It is important to consider target objectives when designing or refreshing digital service standards. This is because the principles and supporting components required to achieve each objective will vary. For example, principles and tools can be designed to encourage the use of new and innovative technology, or design systems can be created to increase ease and speed of delivery.

Focus Areas

This document contains findings on approaches taken by other jurisdictions and lessons learned across 6 focus areas:

1. Principles
2. Services covered
3. Compliance and adoption
4. Supporting components
5. Measuring performance
6. Maintaining the standard

Findings from research have been organised to align to these six focus areas, as presented in the sections of this report to follow.

2. Principles

Principles Included

Benchmarking of 16 governments' digital service standard principles reveals strong commonality between the Australian Government's existing 13 principles and those adopted across other jurisdictions. Figure 5 below presents these existing 13 principles and the number of jurisdictions which have adopted the same, or similar, principles.

Figure 5: DTA Digital Service Standard principles compared to 16 other jurisdictions

 AUS Current State: Existing DSS Principles		# Jurisdictions with similar principle
1	Understand user needs	15/16
2	Have a Multidisciplinary team	9/16
3	Agile and user centred process	10/16
4	Understand tools and systems	7/16
5	Make it secure	12/16
6	Consistent and responsive design	10/16
7	Use open standards and common platforms	15/16
8	Make source code open	10/16
9	Make it accessible	13/16
10	Test the service	10/16
11	Measure performance	10/16
12	Don't forget the non digital experience	8/16
13	Encourage everyone to use the digital service	6/16

This comparison reveals two main points of difference:

1. **Principle 13: Encourage everyone to use the digital service.** 6 out of 16 jurisdictions included the same, or a very similar principle. The United Kingdom (UK) Government originally included this principle but removed it in 2019, reflecting a shift in focus towards designing services that people want to use rather than encouraging people to use the service. Some governments, including the Victorian State Government, have also included principles which focus on ease of use to make digital the first choice for customers.
2. **Principle 4: Understand tools and systems.** 7 out of 16 jurisdictions included a similar principle. Across these jurisdictions, there was significant variance in specificity relating to technology requirements. For example, some jurisdictions' principles specify requirements for modern, flexible, composable and scalable architectures, whereas others focus on understanding technology and how it will be procured and managed.

To identify additional ideas to consider for future iterations of the DSS, a mapping of principles included by other jurisdictions but not reflected in Australia's current DSS was completed. This mapping identified 9 additional principles commonly adopted by other jurisdictions.

Figure 6: Nine principles commonly adopted across jurisdictions

Category	Principles	Jurisdictions with this principle	# of jurisdictions
User Experience	1 Simple, easy and intuitive services	UK US DEN SIN ONT WA VIC	7/16
	2 Design end-to-end user experience	US UK SIN ONT VIC	5/16
	3 Relevant services (aware of user)	DEN SIN GER VIC	4/16
Trust and Data	4 Be good data stewards	US FIN DEN UAE NZ UN ONT NSW	8/16
	5 Use data/research to drive decisions	US DEN GER WA NSW	5/16
Tech Reliability	6 Operate reliable, resilient services	UK FIN UAE VIC	4/16
Delivery and Planning	7 Plan and resource for lifetime of the service	UAE SIN NZ UN ONT NSW	6/16
	8 Assign leadership and accountability	US FIN NZ UN NSW	5/16
Reusability	9 Use and contribute to common platforms, components, and patterns	UK FIN DEN SIN GER WA NSW VIC	8/16

It should be noted that the frequency by which principles appeared across standards indicates what other jurisdictions have identified as relevant for their contexts but does not provide an indication of whether principles are effective at delivering outcomes.

To identify principles for consideration in the Australian Government context, individual jurisdictions' unique principles were also analysed.

Table 1 below provides an overview of additional principles adopted across jurisdictions.

Table 1: Additional principles adopted across jurisdictions

Jurisdiction	Additional principles adopted
US Federal Government	• Structure budgets and contracts to support delivery • Choose a modern technology stack • Deploy in a flexible hosting environment • Automate testing and deployments
UK Government	• Provide a joined-up experience across all channels
Finnish Government	• We will cut unnecessary red tape • We will produce benefits for our customers quickly • We will ask for new information only once
Danish Government	• Simple clear language • Conventions for flow and functionality • Field validation • Personalisation • Compliance with agreed architectural standards • Solutions that must be on borger.dk and must comply with the portals' common design systems and integration process
UAE Federal Government	• Design easy and proactive government services • Government agencies should provide all their digital services through the unified digital platform • Government entities should request for information one-time and follow laws on data sharing
German Government	• Making things easy is hard work – challenge the status quo
Singapore Government	• Review services at least once every 3 years • Only build apps if necessary • Only display content govt content • A single website with.gov.sg domain
New Zealand Government	• Be inclusive, and provide ethical and equitable services • Be clear about what you are trying to change and why • Design for our unique constitutional and cultural environment • Use digital technologies to enhance service delivery
United Nations Development Programme	• Do no harm • (Perhaps) don't build it
Government of Ontario	• Ensure users succeed the first time • Continually improve, even after launch

Jurisdiction	Additional principles adopted
	• Support those who need it • Only include elements that have a purpose
Western Australian Government	• Start with user needs, not government needs • Do less • Understand context • Build digital services not websites • Take a one-government approach
New South Wales Government	• Deliver outcomes for customers, before solutions for government • Measure and improve, don't spin up and drop
Victorian Government	• Designed for mobile or tablet first • Fast: Quick to submit and provide efficient E2E service • Aware of history • Aware of user • Solve the right problem • Progress over perfection • Innovate with purpose

Leveraging input from these additional principles and insight from expert interviews, additional ideas — beyond the 9 commonly adopted principles — were identified to consider for future iterations of the DSS. For example:

- Ask for data only once
- Collaborate widely
- Have a modern technology stack
- Build transparency, accountability and trust
- Leverage data and technology ethically
- Harness new technologies to deliver excellent services (e.g. AI)
- Deliver joined-up services
- Solve the right problem/clarity of objectives

Research also identified 4 principles currently included in the Australian Government's DSS which may be less relevant in 2023 or may not be resonating with all stakeholders. These include:

- **Multidisciplinary teaming:** Potential that some departments/agencies with higher digital maturity may have already adopted the multi-disciplinary teaming approach. However, some agencies with lower digital maturity may still be working towards fully integrating new ways of working.
- **User centred and agile processes:** Some agencies have historically found this principle harder to achieve, as traditional government funding and governance processes bias towards waterfall delivery approaches and up-front solutioning.

- **Make the source code open:** Some agencies have found this principle hard to achieve in practice, as it may not always be possible or appropriate to publish source code in the public domain.
- **Encourage people to use the service:** Research identified a broader trend of shifting from a “Digital by Default” approach whereby customers are encouraged to use digital channels, towards designing digital services which customers want to use and are their first choice.

Detailed mapping of principles across jurisdictions are include in Attachment A for reference.

Emphasis on outcomes vs. inputs

Digital service standard principles can be designed to define expectations for what good service delivery looks like from an or inputs/process, outputs or outcomes perspective:

- **Input/process-focused:** Principles which are input/process-focused define expectations for processes and ways of working which drive better digital service delivery outputs and outcomes. Examples include understanding user needs, testing the service, or adopting agile/multidisciplinary teaming approaches.
- **Output-focused:** Principles which are output-focused define expectations for tangible characteristics of digital services. Examples include using a standard domain, asking for data only once, using digital identity or hosting on a common platform.
- **Outcome-focused:** Principles which are outcome-focused define the benefits that good services are expected to deliver for customers, users and government. Examples include meeting user needs, delivering secure services, operating reliable services, or making services accessible, simple and easy to use.

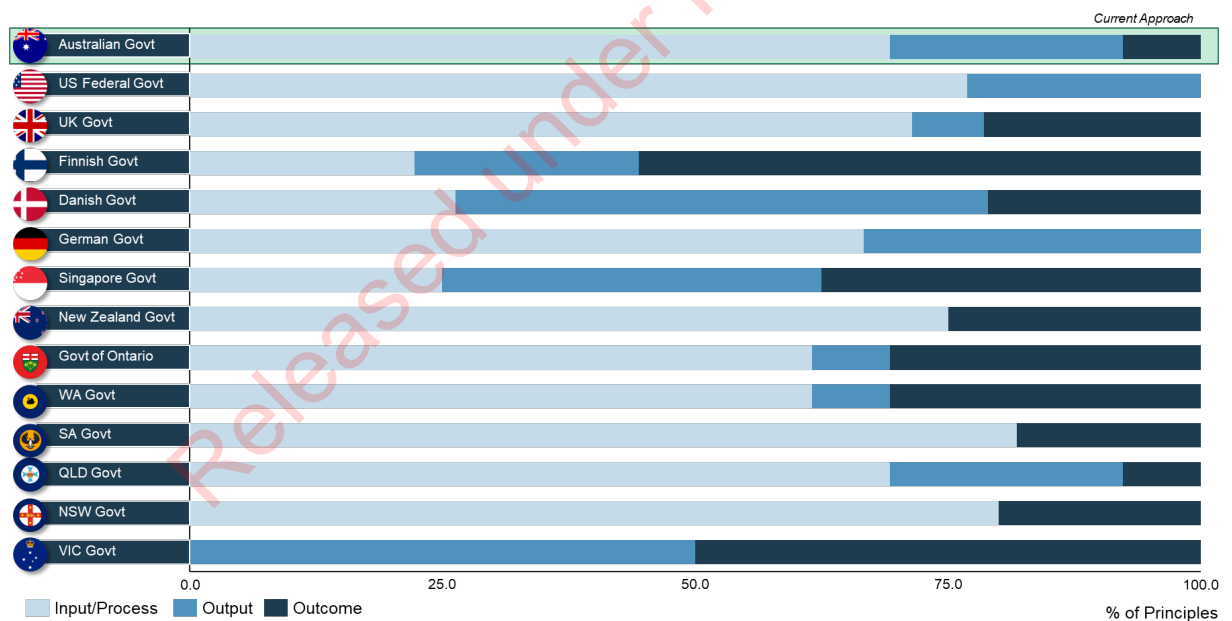
Each approach delivers different benefits and may be appropriate for different scenarios:

- ***Input/process-focused principles*** are effective when there is variable digital maturity across WofG and are intended to provide teams guidance on how to get to good service delivery outcomes. A key benefit is providing design teams with the authority to challenge the status quo and drive change by setting the expectation for ways of working.

- **Output-focused principles** are effective when there is a desire to drive high levels of consistency, and there is sufficient digital maturity across WofG to drive towards target output. Output-focused principles have the added benefit of being objective and easy to assess and provide flexibility on day-to-day delivery activities and approaches.
- **Outcome-focused principles** are effective when there is high digital maturity across WofG. They increase focus on value delivery rather than process or meeting specific requirements and allow for maximum creativity and innovation by providing flexibility in how outcomes are delivered. They also allow for context to be applied where single output-focused requirements might not fit all scenarios.

All jurisdictions included a mix of input/process, output and outcome-focused principles, with varying degree of emphasis. The main driver for this blended approach is to accommodate variability in digital maturity across WofG.

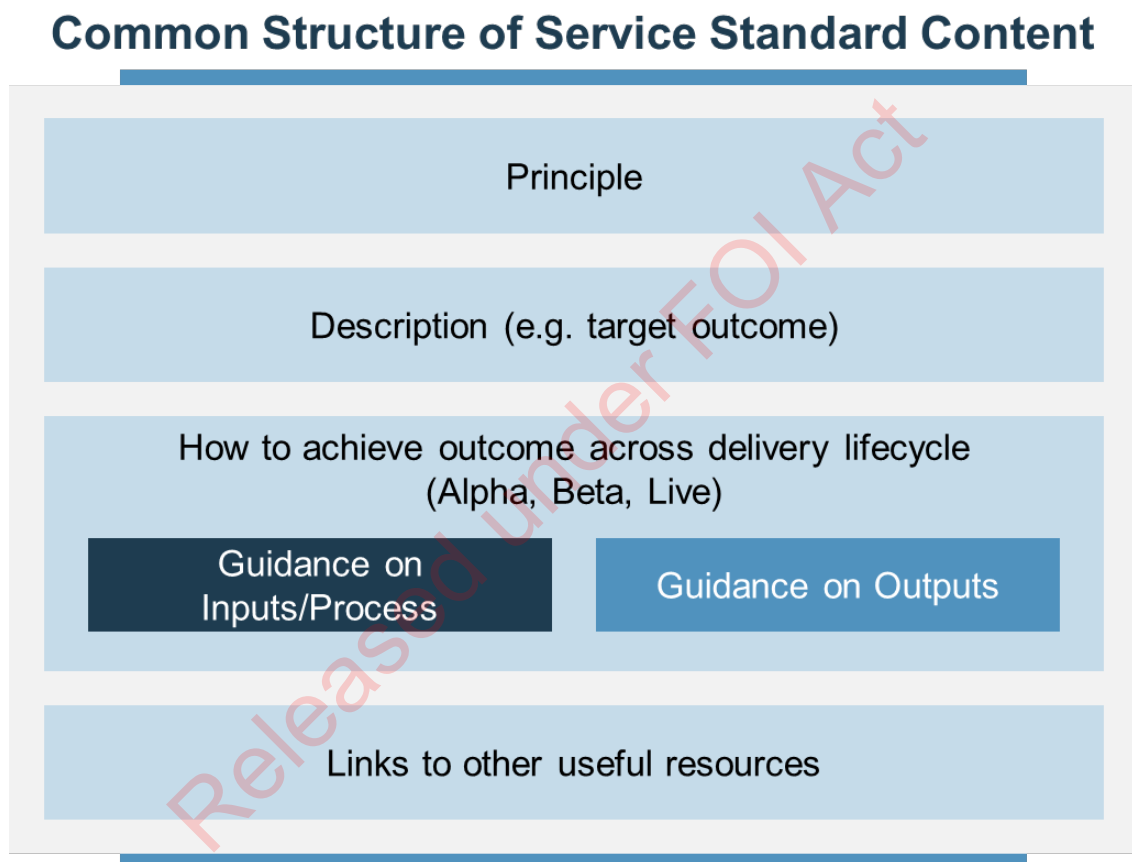
Figure 7: Percentage of principles which are input/process, output and outcome-focused



Structure of standards

Even for outcome-focused principles, most jurisdictions provide guidance on inputs/processes in the supporting detail. While some jurisdictions house this information in guides (e.g. Victoria), others present it alongside principles (e.g. UK, Australia, Singapore, New South Wales). For example, a common structure adopted is presented in Figure 8.

Figure 8: Common structure of standards³



Case studies which provide an overview of how individual jurisdictions have structured their standards are included as Appendix B for reference.

³ Illustration does not reflect variability in where content is housed across jurisdictions (e.g. whether guides are separate or directly linked to and presented alongside principles)

Lessons learned

Keep it short and simple: List of principles should be short, and principles themselves should be simple, clear and understandable. They should reflect concepts design teams are passionate about, inspire them to deliver great services, and be easy to use and navigate. For example, the Estonian Government strived to have no more than 10 principles, and the UK Government reduced their list of principles in 2015 (from 25 to 18) and 2019 (from 18 to 14).

Move the needle: The purpose of digital service standards is to raise the bar on digital service delivery. Principles should be designed to target areas across government which require capability uplift and not areas where capabilities have already been mastered.

Balance aspiration with achievability: Whilst being aspirational, principles should also reflect the constraints teams are working within and be realistically achievable for design teams. For example, traditional government funding models tend to bias towards waterfall delivery, and publishing source code may not always be feasible.

Include both outcome and process/input-focused principles: Principles should be designed to bring everyone up to standard. In environments where there is variable digital maturity, include principles which set expectations for ways of working (processes/inputs) which will lead to target outcomes.

Avoid introducing barriers to delivery: Avoid principles which introduce unnecessary red tape or administrative burden e.g. Ontario found a principle which requires teams to test services with a minister and obtain sign off before go-live to be restrictive.

Reflect broader strategic objectives: Best practice principles reflect overarching strategic objectives and provide clarity on how they support those objectives. This will be important to drive adoption across WofG.

Accompany principles with guidance and support: Designers across government want to deliver good services in alignment with the standards. Provide support to teams so that they can achieve aspirations; supplement principles with guidance and capability uplift, which will empower teams to meet the requirements and deliver excellent services.

Develop principles using a consultative approach: Generate buy-in by consulting widely to gain alignment on principles, target outcomes and ways of working. To do this, ground all standards refreshes in feedback from the WofG community and industry experts as appropriate.

3. Services Covered

Common criteria

Research indicates that when jurisdictions apply thresholds or criteria to define the scope of services covered by digital service standards, they tend to do so across 5 dimensions:

Table 2: Common criteria used to define scope of services covered

Dimension	Description
User Base	Customer facing services or internal services
Purpose	Informational or transactional services
Service Owner	Services delivered by government or outsourced services
Service Age	New/refreshed services or high priority existing services
Other	High transaction volume, high cost or high impact (e.g. interdepartmental) services

Approach taken varies by jurisdiction. Areas of greatest variance in approach across jurisdictions include user base and service age.

- **User Base:** All jurisdictions apply digital service standards to customer facing services. Increasingly, jurisdictions are moving to expand scope to also include internal, government employee-facing services. 40 per cent of jurisdictions have already done this, and one additional jurisdiction interviewed identified this as a consideration for the future. The New Zealand Government includes both user bases, but limits scope of internal services to those which are interagency.
- **Purpose:** All but one jurisdiction (UK Government) apply digital service standards to both informational and transactional services.
- **Service Owner:** All jurisdictions apply digital service standards to services delivered by or under the direct control of government. One jurisdiction (New Zealand Government) also includes services outsourced to delivery partners.
- **Service Age:** All jurisdictions apply digital service standards to new or refreshed services. Some jurisdictions also apply these standards to existing services (Australian Commonwealth Government, Finnish Government, Danish Government, UAE Federal Government, and Singapore Government). This criterion is sometimes qualified by additional thresholds such as services delivered after a specific date or existing high transaction volume services.

- **Other:** Some jurisdictions limit application of digital service standards to high transaction volume services, high-cost services or services included in specific WofG strategies (e.g. Denmark's "Digital by Default" mandate). These criteria are most useful for defining which services will be subject to compliance activities for enforcement of standard.

Approaches adopted across jurisdictions, including current approach adopted by the Australian Government, are depicted in Figure 9. Key trends identified include the expansion of scope to include internal services and a focus on new and renewed services.

Figure 9: Comparison of services covered by digital service standards

User Base	Customer facing services   NZ WA SA QLD	Customer facing and internal services   US UK UAE ONT NSW VIC	
Purpose	Transactional Services  UK	Transactional and informational services   AUS US FIN DEN UAE SIN NZ ONT WA SA QLD NSW VIC	
Service Owner	Services delivered by government   AUS US UK FIN DEN UAE SIN ONT WA SA QLD NSW VIC	Outsourced services  NZ	
Service Age	New or renewed services   UK ONT WA SA QLD	New or renewed, and existing services   AUS FIN DEN UAE SIN	Criteria not applied   US NZ NSW VIC
Other	No other qualifiers applied   US FIN DEN UAE SIN NZ WA SA NSW VIC	Other qualifiers (e.g. transaction volume or cost)   AUS UK ONT QLD	

It should be noted that while many governments indicate that the digital service standards are applicable across a wide scope of services, application of these standards is not necessarily always mandated, assured or enforced.

More specifically, the scope of applicability and scope of compliance activities are not always linked. For example, the US Government, New Zealand Government and Finnish Government set criteria to define which digital services their standards cover but publish them as guidance only (refer to section 4 of this report for additional information on compliance approaches).

Lessons Learned

Focus on new or refreshed services: Requiring services already delivered be brought up to standard can impose significant burden on agencies to upgrade services. Existing services will likely require additional funding to bring services in line with the standards.

Include both transactional and informational services: Governments across all jurisdictions are designing digital service standards to set expectations for both informational and transactional service delivery.

Apply it to everyone equally: Most jurisdictions apply digital service standards to all parties involved in delivering services delivered by or under the direct control of government. This includes 3rd parties designing and delivering digital services for government (i.e. system integrators, or services where ongoing management of technology solution is outsourced, but service delivery responsibility is under the direct control of government).

Uplift experience for customers and internal users: Set expectations for good service delivery, regardless of user base and target uplift in customer and employee experience. Improving internal services which sit behind customer facing service delivery will equip customer service employees to better meet customer needs and increase efficiency and effectiveness whilst also improving employee engagement and retention.

Focus on impact: While digital service standards may be written to be applicable to all types of new and refreshed services, thresholds can be applied for compliance activities to focus on highest impact areas; for example, services that are customer facing, high volume, cost or impact, or internal services that are interagency, support customer facing processes or have high user bases.

4. Compliance and Adoption

Compliance archetypes

Governments leverage a variety of mechanisms to drive compliance and adoption of their digital service standards. Broadly speaking, these can be categorised into three main archetypes, reflecting the degree to which digital service standards are mandated and enforced. The three models for compliance include:

1. **Centrally mandated and enforced:** Compliance to standards is mandatory, assessments are completed to check compliance, and levers are applied to enforce compliance.
2. **Centrally mandated, but not enforced:** Compliance to standards is mandatory, but execution of formal assurance processes and enforcement activities are limited or not conducted.
3. **Published as guidance only:** Standards are developed as set of best practices only. Compliance is not mandatory or enforced.

Figure 10: Benchmarking of jurisdictions' compliance models across three archetypes

① Centrally mandated and enforced	② Centrally mandated, but not enforced	③ Published as guidance only
 UK Government  Singapore Government  Government of Ontario  NSW Government	 Australian Government  Danish Government  Western Australian Government  South Australian Government  Queensland Government  Victorian Government	 US Federal Government  Finnish Government  New Zealand Government  UNDP

There are pros and cons for each of the three archetypes, and several reasons were identified as to why governments might take one approach over another. The main drivers included organisational culture, political window/opportunity, and availability of sufficient powers and resourcing to assess and enforce compliance.

Archetype 1: Centrally mandated and enforced

The centrally mandated and enforced approach can lead to faster adoption of the standard compared to non-enforced mandates and sends a strong signal for change to the government community. It provides a mechanism to intervene in failing projects and avoid negative service delivery outcomes (e.g. through de-risking project, or halting delivery). It can also be quite effective as a lever to drive change by giving delivery teams across WofG the authority to challenge the status quo and push for adoption of new ways of working. Overseas, it has also proven to be an effective signal for change to the market (system integrators).

Challenges associated with this approach include that there are political trade-offs, especially in highly de-centralised or federated delivery environments. Compliance activities such as staged assessments also have the potential to be resource intensive and may introduce administrative burden to both the assessment team and delivery teams. If assessment activities are not fully integrated, they can also fail to drive real change (e.g. assessment at the start of a project only assesses intent). Another challenge other jurisdictions have tackled include that some aspects of the standards by necessity are not prescriptive, and may be perceived as subjective, and lead to ambiguity in assessments.

Jurisdictions typically this approach when:

- The central digital office has sufficient powers to enforce consequences for non-compliance including spend controls or domain controls
- The organisational culture favors top-down mandates or executive orders to drive change.

Archetype 2: Centrally mandated, but not enforced

When standards are centrally mandated, but not enforced there is still potential to send a signal for change across government. In addition, teams across WofG are still provided the authority to challenge the status quo and push for adoption of new ways of working; without significant resourcing required for compliance activities.

A key challenge with this approach is that mandating without consequences or levers to enforce can undermine authority in the long term. In addition, adoption is likely to be slower than centrally mandated and enforced standards, unless paired with useful supporting components and enablement techniques which make using the standard easier than any other delivery approach (e.g. reusable tools with compliance out-of-the box).

Jurisdictions typically this approach when:

- Mandate obtained, but central digital agency lacks powers to enforce consequences, or resources to conduct assessments
- The organisational culture favors top-down mandates or executive orders to drive change

Archetype 3: Published as Guidance Only

When standards are published as guidance only, they can also be very effective at driving adoption of best practices, but only if paired with useful supporting components and bolstered by enablement and awareness activities.

The upside of taking this approach is that there are less political trade-offs. However, this approach is also less likely to send a strong signal for change and there is potential for only some agencies or teams to adopt the standards, which can lead to pockets of excellence and widening the maturity gap and service quality differential across government. The guidance-only approach will not provide teams with the same level of authority to challenge the status quo and drive change within the agencies.

Jurisdictions typically this approach when:

- The government is highly de-centralised from either a delivery model or organisational culture perspective
- They favor other mechanisms to drive change (e.g. legislation)
- Active choice to focus on empowering agencies to deliver outcomes through capability uplift and enablement, rather than enforcement

Both archetypes 1 and 3 have the potential to drive good outcomes in service delivery, as long as key success factors are considered for each compliance model. The best approach to gaining compliance is to either move to the right or the left on the scale of enforcement to avoid undermining authority with a mandate that is not enforced. Key success factors for both archetypes are included in Figure 11 below.

Figure 11: Key success factors for best approaches to compliance

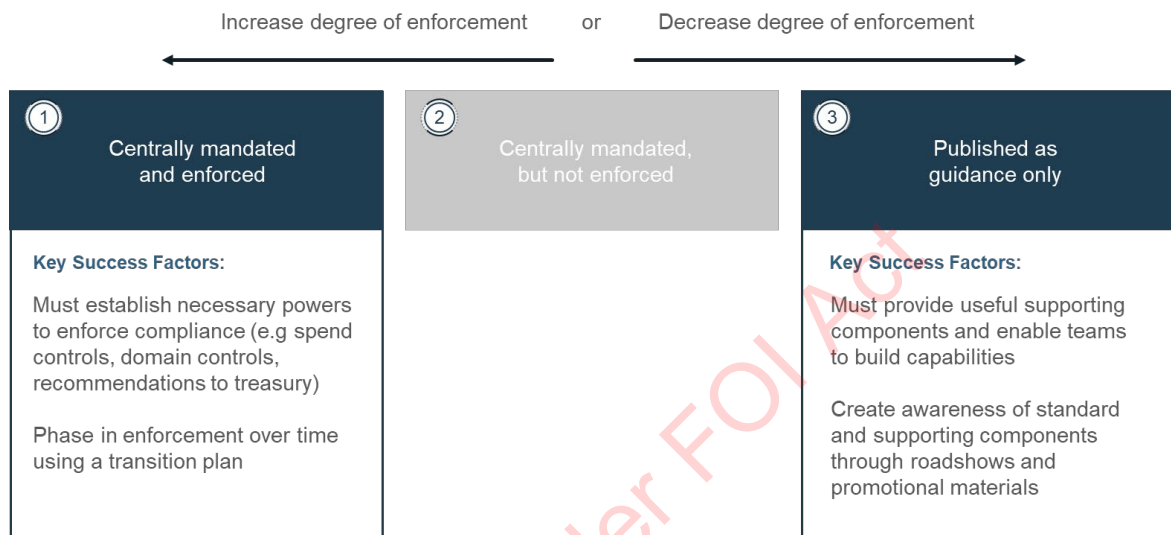


Figure 12 below provides additional detail as to how each jurisdiction governs compliance to digital service standards.

Figure 12: Detailed comparison of jurisdictions' compliance mechanisms

		Investment approval	Cadence of Assessments				Assessor			Publicly Published Results
			Ad hoc	Discovery	Development	Live	Central Govt.	Self	Third party	
① Centrally mandated and enforced	UK Govt	✓			✓	✓	✓	<10,000 annual transactions		✓
	Singapore Govt		✓				✓		✓	
	Govt of Ontario			✓	✓	✓	✓			
	NSW Govt	✓		• Rapid Assessment for Projects <\$5m • Digital Restart Fund Periodic assessments			✓			
② Centrally mandated but not enforced	Australian Govt	✓			✓	✓	✓	✓	Current Approach	✓
	Danish Govt							✓		
	WA Govt							✓		
	SA Govt				✓	✓			✓	
	Queensland Govt	✓	✓					✓		
③ Published as guidance only	Victorian Govt							✓		
	US Federal Govt									
	Finnish Govt									
	New Zealand Govt									
	UNDP									

✓ Stated
 ✓ Enforced

Case studies for three of the government jurisdictions which mandate and enforce compliance to digital service standards are included as follows:

Case Study | Rapid assessments conducted for projects <\$5m to check alignment to NSW Design Standards

What they did:

3 main assessment mechanisms are implemented in NSW for digital projects:

- **Rapid Assessments completed on projects <\$5M delivered through Restart Fund (specifically assesses alignment to NSW Design Standards):** This includes mostly small seed and scale projects and is conducted at 3 points in project delivery to assess compliance to NSW Design Standards. Assessments are not mandatory unless something is identified to be failing and include attending ceremonies and reviewing project backlog over a few days.
- **Assurance for all projects funded through the Digital Restart Fund:** Project assurance and assessment for alignment to Digital Service Standards is conducted at various stages throughout delivery. These assessments do not specifically assess alignment to NSW Design Standards.
- **Assurance through the wider Gateway Review Process:** Health checks completed across project delivery lifecycle; however focus is broader and not directly linked to compliance against the NSW Design Standards.

Lessons learned on key success factors:

- Digital Restart Fund provides strong levers for enforcement to standards, and has been important to enabling NSWs approach
- Rapid assessments are funded through \$15k charge back model, providing more sustainability to resourcing approach
- Assessments to date specifically against the NSW Design Standards have focused on lower value/risk projects. Conducting assurance at scale for larger projects specifically against these standards will require increased integration with WofG digital assurance processes.

Case Study | UK Service Standard mandated and enforced through spend controls and domain controls

What they did:

Assessments are conducted throughout project lifecycle, at defined stages in the delivery process. They are run by a panel of 4-5 experienced specialists from the digital government community and take approximately 4 hours to complete.

Agenda includes:

1. **10 Mins:** Overview of service including problem statement, target users, user needs, and work done to understand users' wider journey
2. **20 mins:** Walkthrough of user journey and what has been
3. **2-3 hours:** Questions from the panel on decisions made and process for building service. These questions change based on where the project is in the delivery cycle

Service is assessed as 'met' or 'not met,' and outcomes are published.

Lessons learned on key success factors:

- **Domain Control:** Power to prevent services from being published to any GOV.UK domain if they do not meet requirements
- **Spend Controls:** Mandate to prevent release of funding to projects during delivery, which were not meeting standards
- **Peer Review Model:** Experts seconded from across WofG to perform assessments, reducing resource intensiveness. Participation in this process viewed as a "corporate responsibility"
- **Published Results:** Publicly publishing results of assessment provides incentives to align with standards
- **Lightweight Assessment Process:** Assessment process not intended to drive creation of new content or large time dedication; limited to half day activity

Case Study | Ontario Government moved to mandate and enforce service standards over time

What they did:

Where they began: Started journey by developing a helpful best practice standard without a mandate or compliance mechanism and then began to integrate into assurance processes over time. Before mandate established, they achieved buy-in by socialising the standard with the CIOs of each agency and establishing credibility through a realistic yet aspirational and useful set of principles and supporting components. Focus was largely on enablement and included providing services to support agencies to deliver (e.g. trusted delivery partner/advisor services out to government). Assessments were optional and self-completed.

Where they are now: Over time they increased mandate and implemented a team to conduct more formalised compliance and assurance activities. Today more than 150 assessments are conducted per year. They built increased authority through:

- Embedding requirement to comply with standards and use design system in broader government directives and legislation
- Working with Treasury to embed into the budget process, with treasury directing projects to conduct assessments
- Over time working with various boards across WofG to integrate into broader WofG ecosystem

When completed, assessments receive “pass/course correct/halt” recommendation and advice on how to course correct. Focus is still largely on enablement through leveraging assessments to identify projects that need help, and then providing support, advice and delivery partner services.

Lessons learned on key success factors:

- Ontario was able to successfully increase authority over time, by first building robustness in standards and credibility
- Assessments are framed as an opportunity to receive support, rather than enforcement an activity focused on consequences
- Dedicated assessment team with strong capability and capacity drives compliance and adoption activities

Common challenges

As shown in Figure 12 previously, while most jurisdictions have instated mandates, many are not enforced in practice. Many jurisdictions, including the Australian Government, are experiencing similar challenges with mandates that make them difficult to enforce in practice, for example:

- **Lack of enforcement levers:** It is difficult to drive alignment to the standards without levers to enforce consequences. For example, in the UK the central digital agency has the right to refusal for publishing services on the central government platform (domain control) and spend controls for WofG digital services (through recommendation to His Majesty's Treasury). Similarly, the NSW Government Digital Restart Fund provides spend control levers for projects delivered through the fund and the Government of Ontario can recommend interventions, or for projects to halt.
- **Resource intensity:** Regular checks throughout the project lifecycle can require significant time and resource investment. Depending on the number of services in scope, a dedicated team of assessors may be needed to conduct assessments regularly. The UK government has overcome this challenge through leveraging resource capacity from across WofG, in the form of secondments to perform assessments (see previous case study).
- **Subjectivity of process-based criteria:** Certain principles and criteria have historically proven to be difficult to assess against, especially those that set expectations for processes and ways of working. A review of New Zealand's Digital Service Design Standard in 2019 found it would be difficult to provide an assessment and reporting framework without specific points to assess and report. Recommendations included the addition of specific measurable, assessable and reportable outcomes to each principle of the standard
- **Ineffective to assess intent only:** Some jurisdictions assess alignment to standards during the funding approval process only. When compliance checks occur at the start of projects, they only assess intent. Reviewing the project plan only at the onset leaves room for deviation during delivery.

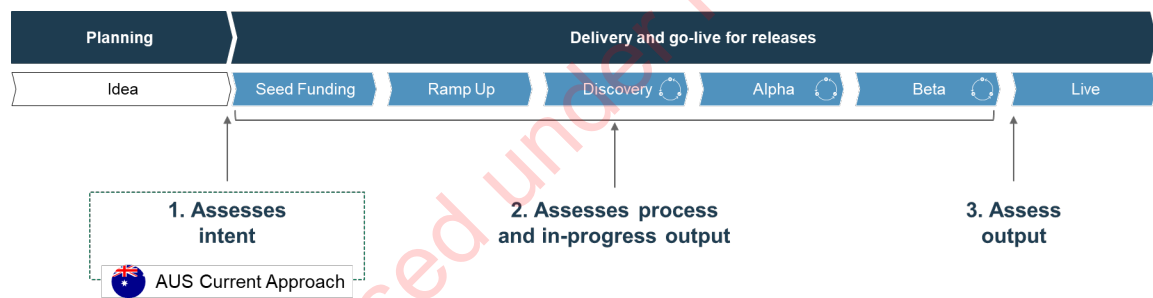
Assessments across project lifecycle

Most jurisdictions that enforce standards through assessments conduct checks at various stages in the project lifecycle. Figure 12 presented previously illustrates the points at which jurisdictions are currently implementing assessments.

There are benefits to reviewing projects at each stage in the lifecycle: assessing up front provides the opportunity to set the program up for success, assessing during delivery provides the opportunity to intervene early or recommend changes, and assessing before go-live provide quality assurance.

The most successful models assess projects at each of these points—not just at the start or before go-live—to avoid only assessing intent or reviewing projects too late in the process once the service has already been built and failure to comply can mean it is not feasible to influence change, as compliance may require significant rework and investment.

Figure 13: Options for cadence of assessments throughout the project lifecycle



Driving compliance without mandates

Jurisdictions without strong central mandates and powers are successfully driving adoption and compliance through focusing on making the standards useful. They are doing this through building service manuals, playbooks, guides, reusable tools, and design systems, to increase usefulness for design teams, drive adoption and enable compliance. They are also focusing on enablement (e.g. training), to drive best practices across WofG, and increase alignment to standards. Additional details on approaches other jurisdictions have taken to build useful supporting components is included in section 5 of this report.

Lessons Learned

Begin with establishing necessary levers: The mandate and enforce approach is most effective once the foundational controls are in place - compliance activities without levers to enforce can undermine authority. Enforcement mechanisms could include funding levers, control over publishing to the central platform, or the ability to recommend project halts. Assessments should also be integrated into WofG assurance processes to give the standards additional credence from the top-down.

Make meeting the standard measurable: In defining what it means to achieve objectives, clear, measurable criteria should be established to objectively assess achievement.

Include assessments across project lifecycle: Assessing services at all stages of the project lifecycle is the most effective compliance approach as it provides the ability to set projects up for success at the start, intervene early, and conduct quality assurance along the way.

Have a lightweight assessment process: Design assessments to be light weight such that they do not drive creation of significant new content and limit time and resources required. Avoid uncontrolled addition of new requirements over time, as doing so can create additional bureaucracy and resource intensity as the list of criteria grows.

Leverage peer assessments: Using experts seconded from across government to conduct peer assessments can help to create an environment where assessments are viewed as constructive learning opportunities rather than audits and also provides the benefit of leveraging resource capacity to avoid needing a dedicated assessment team.

Have a transition plan: Enforcement of mandates can be progressively phased in over time to drive familiarity with the processes involved and understanding of target outcomes. A transition plan defines which services will need to comply and when, prioritising higher impact services first. For example, Queensland Government has developed a detailed transition plan which defines requirements across 3 phases. Recommendations from the review of New Zealand's Digital Service Design Standard in 2019 included phasing in mandatory assessment and reporting over a 2-year period to provide agencies with adequate preparation time.

5. Supporting Components

Regardless of degree of enforcement used, research showed that all jurisdictions aim to drive compliance and adoption by making the standards useful through easy-to-use guides, tools, and reusable components that teams want to use because they make their jobs easier and uplift capabilities required to deliver good services.

Guides, design systems and tools

Many government jurisdictions have built service manuals, playbooks, guides, reusable tools, and design systems to increase usefulness for design teams and drive adoption.

Service manuals, playbooks and guides

This includes easily accessible and digestible guidance that supports teams to deliver great digital services by providing thought leadership and direction on key topics. The intention of these materials is to target capabilities that require uplift and focus on enabling teams through development of specific skillsets.

Case Studies | Guidance supports teams to align with service standards

NSW Government has published detailed guides that are housed in their digital service toolkit to build delivery team capabilities across a range of topics relevant to good service delivery. Topics include agile delivery, user research, testing and continuous improvement, technology and tools, accessibility.

UK Government provides thorough guidance on how to meet accessibility requirements in the “accessibility and assisted digital” section of their service manual. Content includes advice on designing and setting up assisted digital support, but also provides detailed explanation on how to navigate related government processes such as accessibility audits.

Victorian Government publishes 23 digital guides covering a range of topics including accessibility, producing multilingual content, making projects open source, researching user experience, deciding if a mobile app is needed, measuring how content performs, and understanding API design principles.

Design systems

Design systems are a collection of reusable components, patterns, and style elements which can be used out-of-the-box by design teams delivering digital services. They aim to increase ease and speed of delivery and consistency and quality of digital services.

Case Studies | Design systems enable delivery of services that consistently meet service standards requirements, at speed and scale and with ease

The Danish Government has built a design system to serve as a free resource for teams across WofG to achieve compliance and target outcomes without having to invest resources and time themselves. Aspects of the standard such as accessibility are built into components so that teams who leverage the design system automatically comply with standards.

The US Federal Government Web Design System (previously the US Web Design Standards) is a library of design components that can help government developers quickly make trustworthy, accessible, and consistent digital government services. The Design System was originally developed collaboratively by the US Digital Service (USDS) and 18F. It is open source and free for agencies to use; it includes buttons, tables, navigation, typography, forms and colour. The 18F team provides training to federal agency teams on how to implement the Design System or build custom design elements to meet an agency's specific needs.

The **UK Governments' Design System**^{2, 3} was launched in 2018 to drive consistency and accessibility and includes styles, components and patterns. In 2020 it was reported that the code base was found in more than 300 services on GOV.UK, and it was estimated to have saved the government £17 million annually. It is maintained by a team at the UK Government Digital Service (UK GDS).

1. [18F Website](#)
2. [GOV.UK \(GDS Blog\)](#)
3. [GOV.UK Design System Webpage](#)

Other reusable tools

This includes helpful toolkits, templates, method cards, and analytics platforms that enable teams to incorporate approved methods into their delivery processes. These tools help to increase ease and speed of delivery and reinforce good practices in areas where additional support is needed.

Case Studies increase ease of delivery

Queensland Government has a widely used Human Centred Design (HCD) toolkit that includes case studies, checklists, method cards, templates, interview guides and key questions to help teams put people at the centre of the design process. Not only do these tools help to build critical design skillsets, but they also help to streamline the research and design processes with ready-made materials and resources.

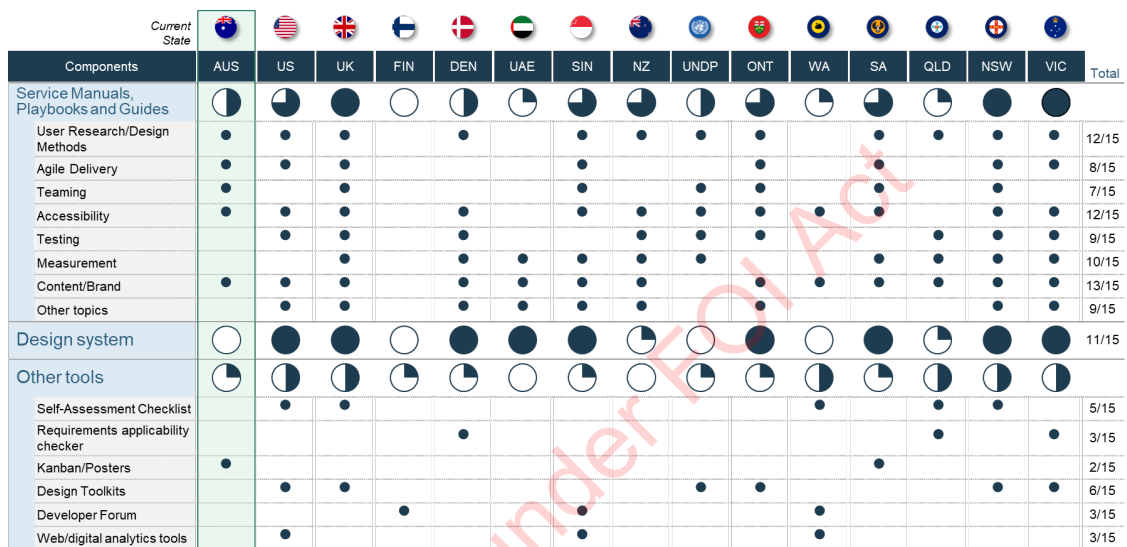
The **Government of Ontario** provides a toolkit on inclusive design. It includes posters, design cards, guidance on questions to identify communication barriers in delivery, and a detailed guide on how to meet requirements.

Singapore Government offers a low cost WofG web analytics tool (that supports their digital service standard by enabling agencies to integrate measurement capabilities into their services. It couples with reusable components which agencies can use to collect customer feedback, and also provides recommendations and self-assessment functionality to identify areas for improvement (e.g. accessibility).

Comparison across jurisdictions

All jurisdictions researched have some combination of these components to support their digital service standards. There are several common themes across these supporting components, but level of maturity and areas of focus vary. Figure 14 illustrates the topics covered and relative maturity (represented by Harvey-balls) for each jurisdiction's guides, design systems, and other tools.

Figure 14: Benchmarking of supporting components by jurisdiction



This comparison reveals 3 key insights:

- The **UK, Victorian and NSW Governments** provide the most mature sets of guides, manuals and playbooks, with detailed guidance across a range of topics including but not limited to user research, agile delivery, accessibility, testing, measurement and branding.
- **9 out of 15** jurisdictions have a design system, and both New Zealand and Queensland are currently in the process of developing them.
- **Wide variety** of other reusable tools provided, with Design Toolkits, and awareness tools being the most common.

Research into private sector design practices revealed a trend towards reusability over time. More specifically, most private sector organisations started their journey by establishing design principles and basic standards on brand or iconography. As digital maturity increased, companies shifted towards more comprehensive digital service standards, useful guidelines, and design systems. This indicates a preference towards reusability and usefulness once foundational digital capabilities are in place.

Enablement and awareness

Increases in digital maturity have necessitated the move from early-stage educator to mature advisor to ensure the highest quality and consistency in services. In addition to useful guides and tools, governments are providing enablement and awareness activities to drive adoption of their digital service standards.

More specifically, they are investing heavily in enabling teams to use the standards through training on critical digital capabilities, enablement/trusted advisory services, vibrant CoPs, and promotion of the standards and their value proposition. Interviews identified that other jurisdictions view these activities as critical to the success of the standards.

Training

This includes e-learning modules, in-person trainings, and informal knowledge sharing to create a common understanding of the standards and how to implement them in practice. Additionally, trainings can be provided to build the digital capabilities needed to deliver the requirements of the standards, covering topics such as inclusive design, agile methodologies, and others.

Enablement

Expert practitioners and members of the government community advise and support delivery teams at various stages of the project lifecycle to augment capabilities where gaps are identified and to drive alignment to standards.

Communities of Practice

Teams of expert practitioners and topic enthusiasts that convene to share best practices and lessons learned and, in some cases, maintain a body of knowledge or thought leadership relevant to the implementation of the digital service standards. CoPs serve as a mechanism to provide teams with guidance and support and drive uptake of standards across the WofG community.

Awareness and Visibility

Materials intended for promotional and awareness purposes, including outreach materials to publicise the standards and the value they deliver. Posters, stickers, printable Kanban boards, and infographics can help to align the government community and increase awareness of the core tenants of the standards.

Case Studies | Governments globally are investing in enablement and awareness to drive the success of digital service standards

UK Government provides free training and certifications through the Civil Service Learning platform. This includes a 45-minute overview of the UK Government's Service Standard, aimed at individuals working in multi-disciplinary teams that are developing digital services. The training is intended to educate teams on the purpose and use of the standard so that they know how to implement it in practice.

Government of Ontario has a team of experts in service delivery that are available to provide design assistance to delivery teams across agencies when requested. The central team serves as a trusted delivery partner and advisor to address capability gaps and focus on the most challenging areas within the standard.

Victorian Government has several well-established CoPs made up of subject matter experts that develop, own and maintain a robust set of how-to guides to provide practical support for service delivery. The CoPs regularly provide feedback on, and review and update the guides to reflect the latest advancements in service delivery and ensure that they are living documents.

Singapore Government has created infographics and published them publicly to generate awareness of the standard and provide them in an easily consumable format for quick reference.

What others are finding most useful

When interviewed, government practitioners indicated that some of these supporting components are regarded as especially useful by their stakeholders. Table 3 below highlights the supporting components deemed most useful across jurisdictions interviewed.

Table 3: Most useful supporting components in jurisdictions interviewed

Jurisdiction	Additional principles adopted
UK Government	• Service Standard • Service Manual • Design System
Danish Government	• Accessibility out of the box (through the Design System)
Queensland Government	• Guidance on testing • Guidance on measures • Reusable toolkits • Design Systems (under development, seeing high demand)
Victorian Government	• Human Centred Design Toolkit • Guides (in general) • Design and Architecture CoPs
New South Wales Government	• Reusable patterns for websites
Government of Ontario	• Reusable patterns • Style guides, headers, footers, fonts

Lessons Learned

Above all else, focus on making the standards useful: Make the standard more useful, and drive adoption and compliance by investing in building supporting components such as guides, playbooks and reusable tools and components that improve speed of delivery for design teams, making their jobs easier.

Create useful packages: Package materials in way that makes it easy for practitioners to apply the standards. For example, this could include grouping materials by topic or creating bundles of minimum requirements that clearly define which requirements design teams (or delivery partners) must meet.

Avoid reinventing the wheel: Use open-source resources where possible and avoid investing effort into developing content which already exists or is easily accessible externally (e.g. link to guidance provided by other jurisdictions).

Be practical: Reduce barriers to adopting central tools and guides by making them easy to find and use. Take a journeys-based approach to the standards themselves that considers what practitioners actually need at various phases in the design process. Provide practical guidance on what it means to apply the standards, accounting for links to broader government processes.

Enable people: Provide training and support to build capabilities that enable practitioners to meet the minimum requirements of the standard. Deliver support to ensure they are confident in using the standard itself.

Build strong Communities of Practice: Bring together design and architecture experts from across government to actively share learnings and contribute to and champion WofG digital service design best practices and thought leadership, and drive awareness and adoption of the standard.

Align with your purpose: Prioritise investment in components that support strategic objectives most. For example, digital service standards can drive high consistency and speed to delivery, while guides and playbooks can uplift digital capability.

Drive awareness: Communicate the value and purpose of your standards and drive awareness of and familiarity with the content, processes and requirements. This will generate buy-in and increased adoption and compliance. For example, the Danish Government promotes their Design System as a free resource for agencies that enables faster delivery and provides accessibility out-of-the-box.

6. Measuring Performance

Digital service standards aim to raise the bar on service delivery and governments are interested in understanding how services are performing against this ambition.

Research focused on two key questions to determine how governments are measuring performance: What are other governments including in their standards about measurement and how are they approaching measurement of service delivery at the WofG level?

Review of other jurisdictions found that governments are including principles on performance measurement, recommending metrics, providing guidance on selection of additional context-specific metrics and building reusable tools to enable measurement of individual services. Few are measuring performance at the WofG level, but those that do are mandating core metrics, establishing central reporting mechanisms, and building WofG analytics platforms.

Recommended metrics

Across jurisdictions analysed, approximately 85 per cent provided suggestions on metrics which can be used to measure performance for individual services. Figure 15 below depicts the 6 most commonly recommended metrics.

Figure 15: Benchmarks on recommended metrics

Metric	# of jurisdictions recommending metric	 AUS current approach
 Cost per transaction	9/12	✓
 Digital take-up	8/12	✓
 Completion rate	8/12	✓
 Customer satisfaction	7/12	✓
 Time to completion	5/12	✓
 # Page visits	4/12	
✓ Recommended as minimum metric by Australian Govt.		✓ Other metrics suggested by Australian Govt

Error! Not a valid bookmark self-reference. below provides a list of other metrics suggested within the Australian Government's DSS and additional metrics recommended by other jurisdictions. All metrics listed were recommended by between 1 and 3 jurisdictions included in this analysis.

Table 4: Additional metrics recommended across jurisdictions, aligned to 5 categories

Category	Metrics recommended by Australian Government	Additional metrics recommended by other jurisdictions
Usage	• % audience reached	• Page visits • Page visit duration • Page referral • Transaction volume • Concurrent users • Context (platform, device, country) • Popular pages • Active users (daily, weekly, monthly) • Search referral
Usability	• Readability • Scroll depth • Search bar use	• Conversion rate • User error in completion • Bounce rate • Accessibility score • SEO Score • Sessions with search • Cycle time • # users who reach step/drop off • Search click throughs • Search click order • Findability • Sessions with search • Start points
Satisfaction		• Voice of Customer (VOC) feedback (Pain Points, Helpfulness) • Ease of completion • User confidence • New vs. returning users • Rate of escalation in complaints • Alignment with user expectations
Reliability and Efficiency	• Uptime • Error rates • Response time • Repeatability	• System level resource utilisation • Latency • Throughput • Performance Score
Value	• Return on investment • User outcomes/benefits	• Social outcomes/benefits

Many jurisdictions provided a distinction between strongly recommended metrics and additional suggested metrics to be considered when selecting context-specific measures. Some jurisdictions also provided differentiated guidance on approach to selecting good metrics for informational or transactional services

Case Study | Victorian Government structures guidance on selecting metrics around type of service

Victorian Government provides separate recommendations and suggested metrics for informational and transactional services. For example, digital guides stipulate that agencies should measure user satisfaction, value and discoverability for informational services, and completion rate and cost per transaction for transactional services. Additional suggested metrics and recommended measurement tools are also provided based on type of service. For example, the guide recommends average time on page for informational services and percentage of user errors for each field/task for transactional services (using an analytics tool).

Mandated metrics

It should be noted that only 1 out of the 12 jurisdictions included in this analysis⁴ mandate any specific metrics or central reporting thereof (UK Government). Across other jurisdictions, measurement of metrics is recommended or encouraged but not formally required.

Case Studies | UK Government mandates 4 core metrics and provides additional suggestions for optional metrics

UK Government mandates the measurement of customer satisfaction, completion rate, digital take up and cost per transaction for all transactional services. Additional metrics referenced in guidance include completion time, user error in completion, alignment with user expectations, ease of completion and user confidence.

⁴ Analysis of mandated and recommended metrics includes a subset of jurisdictions. UAE Federal Government, German Government, and Estonian Government digital service standards not included in this analysis due to lack of publicly available information on metrics

Measuring WofG performance

Most often, governments are recommending measurement of these metrics to inform future service improvement at an agency level only, but there are three jurisdictions where measurement is occurring at the WofG level. For example:



Singapore Government: A WofG analytics platform (WOGAA) is used to provide insight into 6 key metrics across WofG: customer satisfaction, completion rate, uptime, search engine optimisation (SEO) score, accessibility score, and page load time. The tool enables automated collection and central reporting of these metrics. It is also used to measure website traffic, page visit duration, and user feedback and ratings. Targets are set for the 6 key metrics, and in the future, alerts may be provided when metrics consistently fall below targets. Dashboard also provides benchmarks against WofG averages, recommendations to improve site performance, and ability to run self-assessments to identify improvement opportunities. The tool is maintained centrally and provided at very low cost for agencies to use if desired.



Estonian Government: Approach includes leveraging a platform for central reporting of key metrics across government. Metrics include customer satisfaction, cost per transaction, completion rate and time or money saved. It is not mandated that agencies report metrics centrally, but agencies are encouraged to measure these metrics through funding mechanisms and performance is published publicly.



UK Government: Approach includes mandatory central reporting of 4 core metrics, and until 2021 these were publicly reported via a Performance Dashboard. Before its retirement, the Performance Dashboard also displayed page load times and uptimes for services across WofG. Operational data is currently collected on some services across WofG such as number of users and enquiries submitted and displayed publicly on the Great.Gov.UK Performance Dashboard.

Some jurisdictions with WofG platforms have been able to go further to measure more granular metrics for services delivered through these platforms using unified dashboards. Examples are included as follows:



Service New South Wales: Leverages unified dashboard to provide real-time information on service delivery performance across channels, accessible only internally. The public-facing [Performance Dashboard](#) publishes key service delivery metrics across channels for services delivered by Service NSW (SNSW) as the WofG central service delivery agency. Metrics include calls answered, customer satisfaction, service centre customer visits, SNSW personal accounts, SNSW business accounts, active mobile app users, and key statistics by service (e.g. drivers licence). Services delivered by other agencies not included.



Service Oklahoma: Developed unified dashboards to monitor platform performance and service resolution times across channels (including non-digital). Includes metrics such as service time variability, wait time variability, monthly service time standard deviation, on-site customer satisfaction, metrics on contact centre performance, and metrics on specific service performance (e.g. productivity). Dashboards include metrics for services delivered by Service Oklahoma only and do not include data for other agencies across WofG.

Additional Guidance and Tools

Beyond recommended metrics, 7 out of 12 jurisdictions also provide additional guidance and support on how to use metric data to improve services once collected.

Highlighted examples include:



Victorian Government: Provides guidance on recommended actions if not meeting minimum performance threshold (e.g. update or retire services with less than 1000 session per year or low customer satisfaction)



UK Government: Provides guidance on how to choose analytics tools and how to complete usability benchmarking for a website or transactional service



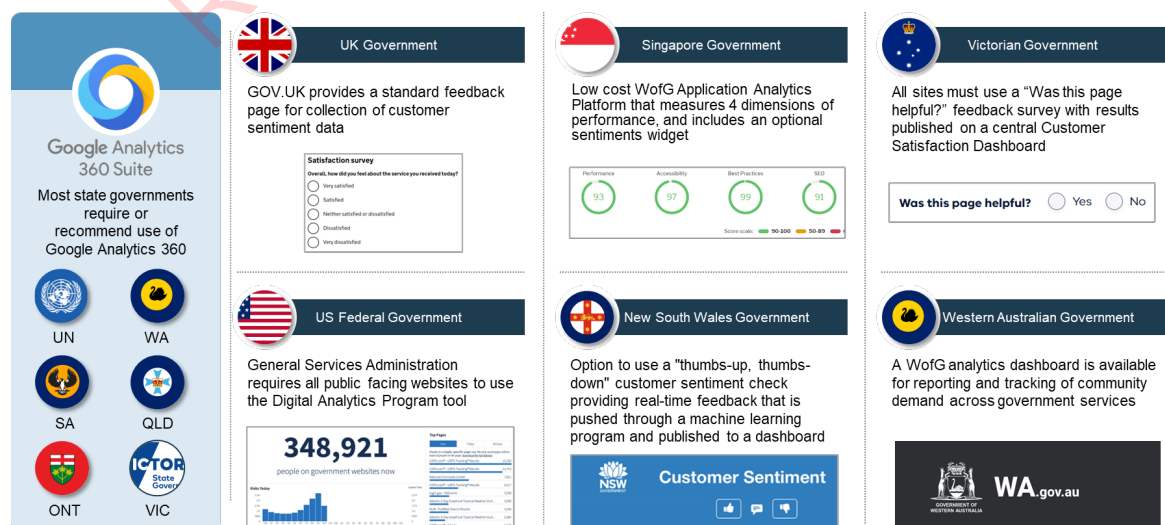
New Zealand Government: Advises teams to identify unusual patterns using analytics and performance measurement tools, make changes to services based on the results of analysis, and further use analytics to measure the success of changes



New South Wales Government: Recommends setting up an ongoing monitoring process throughout the life of the service and identifying triggers (e.g. set amounts of time, drops in technical performance, defined increases or decreases in metrics) to signal the need for improvements or fixes to the service

Multiple jurisdictions are also providing access to useful tools such as Google Analytics 360 suite, other WofG analytics platforms, and reusable components to capture customer satisfaction to make it easier for design teams to measure performance.

Figure 16: Performance Measurement Tools and Reusable Components



Lessons Learned

Get everyone to measure the basics: Encourage teams to measure the 4 core metrics at minimum: customer satisfaction, digital uptake, completion rate, cost per transaction. This provides a baseline to compare individual service performance over time, and potentially can be used to compare performance to benchmarks or WofG targets

Provide guidance on how to select good metrics beyond this: Provide guidance on the process for selecting metrics that align with the context of individual services (e.g. user base or type of service).

Put the data in context: Set high-level targets for the core metrics and provide guidance to put the metrics in context. For example, the Singapore Government sets targets for 6 key metrics and provides visibility of WofG averages/benchmarks through the WofG analytics platform.

Provide support to make the data actionable: Expand upon measurement guidance to provide suggestions for how to use the data collected, including for continuous improvement. Also provide guidance on what actions might be appropriate if performance is low, and where to find additional support to address recommended actions. For example, Victorian Government provides guidance to update or retire services with less than 1000 session per year or low customer satisfaction.

Provide reusable WofG tools: Provide access to reusable tools that can be embedded into services to help teams measure performance easily. For example, some central digital agencies provide reusable components to capture customer satisfaction and feedback such as ready-made sentiment checkers that can be embedded into service. WofG tools and analytics platforms can also be useful in providing detailed information about service performance and highlighting areas requiring improvement.

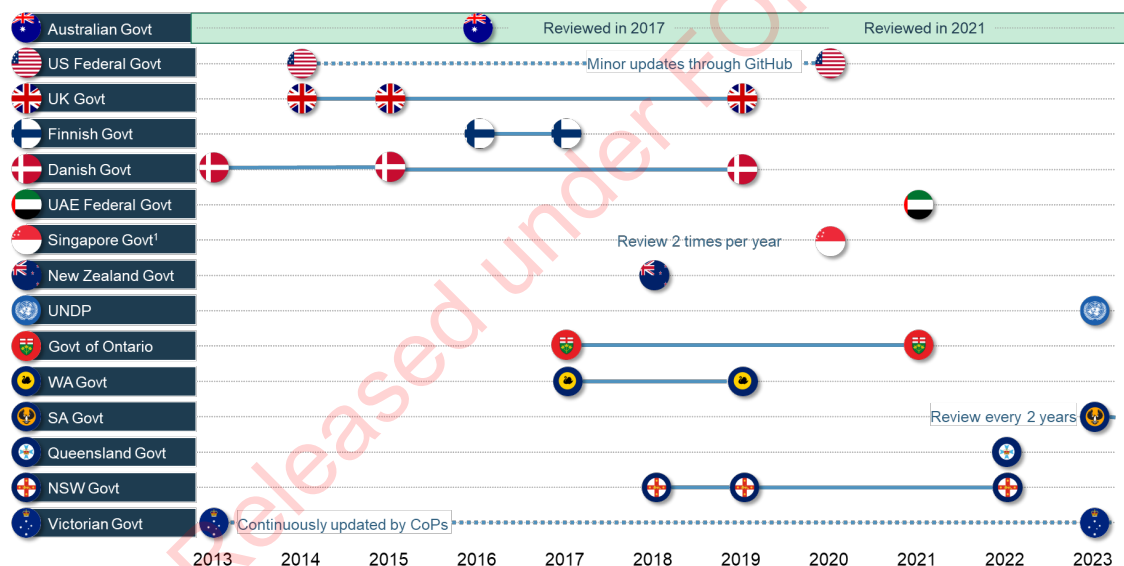
Measure performance across WofG: Provide central reporting mechanism for teams to report on core metrics to give an indication of WofG progress towards customer centric service delivery goals. This can be in the form of central reporting platforms or automatic capture and transmission of data through web analytics platforms.

7. Maintaining the Standard

Refreshing the standard

Most jurisdictions researched have reviewed and refreshed their standards at some point since development in order to keep them relevant, up-to-date, and useful for stakeholders. However, few have established a regular cadence for review and refresh with the exception of the South Australian Government, which reviews its standards every 2 years, and the Singapore Government, which conducts twice-yearly reviews.

Figure 17: Benchmarking of digital service standards refreshes across jurisdictions



In jurisdictions where multiple reviews have occurred, refreshes have been prompted by changes in strategic objectives (e.g. release of new WofG digital strategy), digital maturity or practitioner needs. Case studies for 3 of the government jurisdictions with frequent refreshes are included as follows.

Case Studies | Governments have refreshed standards to address changes in strategic objectives and practitioner needs

UK Government refreshed standards to better meet design team needs:

UK Government first updated its standard in 2015 to consolidate the original 25 principles down to 18, focusing on the points that required most capability uplift based on understanding of practitioner needs. A second refresh occurred in 2019 to further reduce the number of principles down to 14. This refresh also removed “digital” from the title of the standard to emphasise the importance of solving the whole user problem.

Danish Government refreshed standards to reflect changes in strategic

objectives: The Danish Government refreshed its standard in 2015 to align with the objectives articulated in newly released digital government strategy, shifting focus from “digital by default” to citizen centric service delivery. At this stage, the government released new design principles and started on their journey to build a common design system. Currently, the Danish digital service standard is under review with a focus on inclusivity and accessibility.

New South Wales Government refreshed standards to better meet design

team needs: NSW Government completed Beta testing of its standard in 2019, which generated feedback on usability of the standards. Based on the findings from Beta testing, the standard was published in two separate formats to meet the needs of different audiences—a holistic view of principles for policymakers, executives and communications professionals and a project checklist view for product managers and delivery teams. In 2022, the standard was again refreshed to better serve practitioner needs by streamlining the principles, revising the structure to be more practical for day-to-day work and streamlining content to fit more seamlessly into existing processes.

Refreshes to the standards and principles themselves are often centrally driven, with dedicated teams managing reviews, consultations, and the resulting changes. However, some jurisdictions leverage a de-centralised model to update and maintain the standard and supporting components. For example:

- Principles, guides, and manuals are most commonly maintained by a central team, but the United States and Ontario use GitHub to solicit input from the broader community. Public input is then reviewed and approved by government before being integrated.
- The Victorian Government's Digital Guides are developed, owned and updated by its CoPs rather than a central team. Design systems, on the other hand, are typically open source or community driven, allowing for more frequent updates and distribution of resource utilisation.

Figure 18 below illustrates three common models for maintenance and ownership of standards, guides and design systems.

Figure 18: Benchmarking of ownership models for digital service standard components

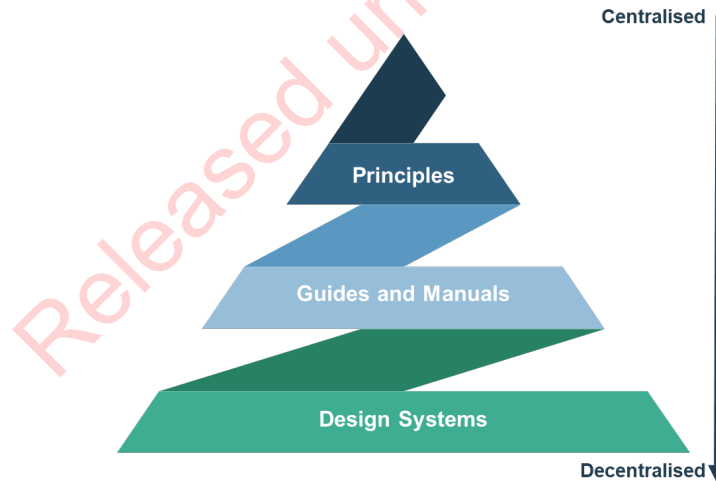
	Central team							Government community (closed group)			Broader community (open source) ¹		
Principles	 AUS	 UK	 FIN	 DEN	 UAE	 SIN	 NZ				 US		
		 UN	 WA	 SA	 QLD	 NSW	 VIC				 ONT		
Guides and Manuals	 AUS	 UK	 DEN	 UAE	 SIN	 NZ	 VIC				 US		
	<i>Current approach</i>	 UN	 WA	 SA	 QLD	 NSW					 ONT		
Design Systems	 UAE							 DEN	 SA	 SIN	 US	 UK	
								 ONT			 NZ	 NSW	 VIC

1. Reviewed and approved by government before inclusion

One potential model for ownership of the digital service standard components is depicted in Figure 19. In practice, this model might comprise of the following approaches:

1. **Principles:** centrally owned and maintained with significant input from WofG stakeholders through broad consultation; principles reviewed every 2-3 years on a regular cadence to align with broader refreshes to the digital strategy and account for any major shifts in government and stakeholder needs.
2. **Guides and Manuals:** WofG community driven, leveraging expertise from government practitioners with potential to also incorporate input from industry and private sector experts; materials continuously updated to reflect the latest advancements in digital service delivery.
3. **Design Systems:** WofG community driven, leveraging expertise from government practitioners and design experts, with potential to solicit feedback from the broader community of design experts outside of government through open-source platforms (e.g. GitHub). Design systems continuously updated to keep templates and patterns useful and relevant and to fix bugs as they appear.

Figure 19: Degree of centralisation for ownership of standards components



Expert interviews suggest that this model could deliver benefits with respect to overcoming resource constraints, in that it distributes the workload across WofG rather than relying solely on a central team. The approach could also generate greater buy-in, ownership, awareness and adoption of the standard and supporting components and create confidence in the content by incorporating collective expertise and peer review. This approach can also enable more frequent updates to ensure continuous alignment to best practices and rapid adaptation to meet changing agency and practitioner needs (e.g. due to rapid advancements in technology).

Measuring effectiveness

Analysis of research and interviews determined that few governments have robust methodologies in place to measure the effectiveness of the standards. Generally, this was regarded as a challenge, as there is no clear proxy which isolates the impact of the standard. Metrics such as customer satisfaction, digital take-up and digital service indices are influenced by a number of other factors.

Instead, most jurisdictions currently rely on informal feedback, formal surveys and basic indicators such as number of page visits or downloads of materials to measure the effectiveness of standards:



Victorian Government: Leverages ongoing discussions within CoPs to provide a continual feedback loop and an understanding of how the standard is being used and which parts are most effective. In addition, the government conducts trainings on the standard and relevant service delivery topics, which are followed by surveys to collect feedback from the users of the standard. Indicators such as page views/downloads are also referenced to understand which digital guides are used most frequently.



Danish Government: Currently planning a cross-government survey to determine if and how the standards and design system are being used. Review is specifically intended to understand the current degree of awareness and helpfulness to inform future updates.



UK Government: Dedicated cross-government heads of profession convene CoPs that hold brainstorming sessions to elicit input and feedback on the standard, helping to identify gaps or areas for future development of content. These communities also use collaboration tools and forums (e.g. Slack) to informally gather feedback on content from the broader government community and users of the standards.



Singapore Government: Centrally owned and managed WofG analytics platform provides capabilities to assess services against key requirements of the standard and provide technical scores and recommendations for improvement (e.g. accessibility score). Effectiveness of tool itself as a supporting component to standard is measured through comparison of assessment results before/after implementing recommendations.

Lessons Learned

Review standards regularly: Establish a regular review cycle (e.g. every 2-3 years in alignment with digital strategy refreshes) and make updates to account for changes in digital maturity, technology, government strategic priorities, and practitioner needs. For example, the New South Wales Government has tested the usability of its standards with stakeholders and updated the structure and format several times to address practitioner needs.

Avoid conducting refreshes in a silo: Centralise ownership of principles but consult widely during refreshes. Principles should be owned and managed by a central team but updated using input and feedback from the broader community through CoPs, surveys, collaboration platforms or formal consultation.

Continuously improve supporting components: Guides, manuals and other tools should be seen as living artifacts that are continually updated to capture the latest advancements in service delivery

Harness capacity and expertise from WofG community: Leverage the WofG community and external experts to build robustness into guides and materials and ensure that they align with capability needs. Use a distributed or open-source model for guides and design systems where practical.

Measure effectiveness: Understand how the standard is being used and identify areas for improvement through basic indicators (e.g. page downloads, number of assessments completed) and formal and informal feedback. Leverage CoPs to provide an ongoing feedback loop and conduct regular surveys to inform refreshes.

8. Conclusion

Research across the focus areas revealed several key findings which can be used to inform future updates to the DSS.

Governments globally are designing their digital service standards and principles to signal change and target areas of lower digital maturity. Most standards set expectations for both ways of working and service delivery outcomes to cater for variability in WofG digital maturity. Research provides insight on themes to consider integrating into DTA's DSS when it is refreshed. Findings also include opportunities to potentially de-emphasise some areas which may no longer be resonating or where modern ways of working are already being established across WofG.

When designing standards to be used in service delivery, governments must determine which services are within the scope of the standard. Across jurisdictions researched, most apply standards to new or renewed (i.e. rebuilt or undergoing significant updates) informational and transactional services that are public facing. Many governments are expanding the scope of standards to also include internal employee-facing services, specifically those that are high impact, cross agency or connected to front-end services.

While governments all have the common objective of driving compliance and adoption of their digital service standards, there are several approaches to achieving this goal. Three main archetypes can be used to define the various models for assessing and enforcing compliance to standards, each with pros and cons. These include standards which are centrally mandated and enforced, those that are centrally mandated, but not enforced, and those that are published as guidance only. The selection of approach to compliance is dependent on a jurisdiction's culture and preferred levers for driving change, level of centralisation of delivery models, political trade-offs, availability of resources, and presence of powers to enforce consequences (e.g. funding controls, domain controls). Both approaches of enforcing mandates and publishing standards as guidance have potential to drive positive outcomes, but key success factors must be considered for each. When choosing the enforcement approach, it is critical that the necessary levers are in place to derive compliance. When publishing standards as guidance only, governments must provide support and enable teams to build the capabilities needed to deliver good services.

Regardless of degree of enforcement used, all jurisdictions aim to drive compliance and adoption by making the standards useful through supporting components. Governments

can promote use of the standards by accompanying them with service manuals, playbooks, guides, reusable tools and design systems that people want to use because they help make their jobs easier. They can also increase compliance by building capabilities and enabling teams through the training and support that designers and developers need most to be successful.

Increases in digital maturity have necessitated the move from early-stage educator to mature advisor to ensure the highest quality and consistency of services. Leading governments have invested significantly in enabling teams to use the standards by delivering training to increase digital capabilities, providing trusted advisory services to agencies, cultivating vibrant CoPs, and creating awareness of the standards and their value proposition for customers and government.

Most jurisdictions researched use their digital service standards as a way to encourage teams to measure service delivery outcomes. Almost 80 per cent include a principle within their standards on measuring performance of services, and 90 per cent provide both recommended metrics for measurement and detailed guidance to support teams in the selection of additional metrics. Many also provide suggestions for ways to use the data collected to improve services moving forward. Often governments have recommended measurement of 4 core metrics: customer satisfaction, digital take-up, cost per transaction, and completion rate. Three government jurisdictions measure performance against core metrics at a whole-of-government level. Some also provide teams with access to WofG analytics platforms to enable more granular measurement and benchmarking of performance across WofG.

Lessons learned indicate that standards should be refreshed regularly (e.g. every 2-3 years) and supporting components should be continually maintained. Some jurisdictions are leveraging the broader government community to drive development and maintenance of guides, tools and other supporting components. While many jurisdictions are not formally measuring the effectiveness of their standards, many rely on formal and informal feedback (e.g. surveys and feedback from CoPs) and other basic indicators (e.g. page downloads, assessments completed) to understand how the standard is used.

9. List of abbreviations

Acronym	Definition
AGA	Australian Government Architecture
AUS	Australian Commonwealth Government
APS	Australian Public Service
BCG	Boston Consulting Group
CoP	Communities of Practice
DEN	Danish Government
DSS	Australian Government Digital Service Standard
DTA	Australian Digital Transformation Agency
FIN	Finnish Government
GER	Federal Government of Germany
Govt	Government
HCD	Human Centered Design
NSW	State Government of New South Wales
NZ	New Zealand Government
ONT	Government of Ontario
QLD	State Government of Queensland
SA	State Government of South Australia
SEO	Search Engine Optimisation
SIN	Singapore Government
UAE	UAE Federal Government
UK	UK Government
UK GDS	United Kingdom Government Digital Service
UNDP	United Nations Development Programme
US	United States Federal Government
USDS	U.S. Digital Service
VOC	Voice of Customer
VIC	State Government of Victoria
WA	State Government of Western Australia
WofG	Whole-of-Government

Appendix A: Principles

Figure 20: Comparison of Australian Govt DSS principles to other jurisdictions

	Current state																	
Principle	AUS	US	UK	FIN	DEN	UAE	SIN	NZ	GER	UN	ONT	WA	SA	QLD	NSW	VIC	Total	
1 Understand user needs	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	15/16	
2 Have a multidisciplinary team	✓	✓	✓					✓		✓	✓		✓	✓	✓		9/16	
3 Agile and user centred process	✓	✓	✓	✓							✓	✓	✓	✓	✓	✓	10/16	
4 Understand tools and systems	✓	✓	✓					✓					✓	✓	✓		7/16	
5 Make it secure	✓	✓	✓	✓	✓			✓		✓	✓		✓	✓	✓	✓	12/16	
6 Consistent and responsive design	✓			✓	✓		✓		✓		✓	✓	✓	✓		✓	10/16	
7 Use open standards and common platforms	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	15/16	
8 Make source code open	✓	✓	✓	✓				✓		✓		✓	✓	✓	✓		10/16	
9 Make it accessible	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓		13/16	
10 Test the service	✓	✓	✓		✓			✓		✓		✓	✓	✓	✓		10/16	
11 Measure performance	✓	✓	✓		✓			✓		✓	✓		✓	✓	✓		10/16	
12 Don't forget the non-digital experience	✓	✓						✓			✓	✓	✓	✓			8/16	
13 Encourage everyone to use the digital service	✓					✓		✓		✓			✓	✓			6/16	

Country

Multi-country

State

Source: BCG research and analysis; relevant standards information and guidance published on agency websites as at 24 May 2023 ([Australia](#), [US](#), [UK](#), [Finland](#), [Denmark](#), [UAE](#), [Singapore](#), [New Zealand](#), [UNDP](#), [Ontario](#), [Western Australia](#), [South Australia](#), [Queensland](#), [New South Wales](#), [Victoria](#)); Germany Service Standard

Figure 21: Digital service standard principles adopted across jurisdictions (1 of 2)

															Total ¹
Category	Principle	US	UK	FIN	DEN	UAE	SIN	NZ	GER	UN	ONT	WA	NSW	VIC	Total ¹
Objectives and Measures	14 Clarity of objectives/solves problems							✓					✓	✓	3/16
	15 Publish performance		✓												1/16
Trust	16 Transparency and accountability							✓							1/16
	17 Do no harm									✓					1/16
	18 Be good data stewards	✓		✓	✓	✓		✓		✓	✓		✓		8/16
	19 Trusted by design													✓	1/16
	20 Make the service simple, easy and intuitive	✓	✓		✓		✓				✓	✓		✓	7/16
User Experience	21 E2E/complete experience	✓	✓				✓				✓			✓	5/16
	22 Ask for data only once			✓	✓	✓									3/16
	23 Provide joined up experience		✓											✓	2/16
	24 Use data/research to drive decisions	✓			✓				✓			✓	✓		5/16
	25 Common conventions for flow				✓										1/16
	26 Personalisation of services				✓										1/16
	27 Proactive government service					✓									1/16
	28 Adjust according to history				✓									✓	2/16
	29 Relevant services (aware of user)				✓		✓		✓					✓	4/16
	30 Design for constitutional/cultural env't							✓							1/16
	31 Use digital to enhance service delivery							✓							1/16
	32 Only include elements that have a purpose										✓				1/16
	33 Reduce red tape			✓											1/16

Country

Multi-country

State

Note: Australia, South Australia and Queensland included in total count but not shown. Source: BCG research and analysis; relevant standards information and guidance published on agency websites as at 24 May 2023 ([US](#), [UK](#), [Finland](#), [Denmark](#), [UAE](#), [Singapore](#), [New Zealand](#), [UNDP](#), [Ontario](#), [Western Australia](#), [South Australia](#), [Queensland](#), [New South Wales](#), [Victoria](#))

Figure 22: Digital service standard principles adopted across jurisdictions (2 of 2)

Category	Principle	US	UK	FIN	DEN	UAE	SIN	NZ	GER	UN	ONT	WA	NSW	VIC	Total ¹
Delivery and planning	34 Automate testing and deployment	✓													1/16
	35 Plan/resource for the lifetime of the service					✓	✓	✓		✓	✓		✓		6/16
	36 Budgets/contracts to support delivery	✓											✓		2/16
Reliability	37 Operate reliable, resilient services		✓	✓		✓								✓	4/16
Ways of working	38 Leadership and accountability	✓		✓				✓		✓			✓		5/16
	39 Challenge the status quo								✓						1/16
	40 Collaborate widely							✓					✓	✓	3/16
Continuous improvement and innovation	41 Continually test/improve (inc. after launch)		✓								✓		✓		3/16
	42 Innovate with purpose													✓	1/16
Reusable common platforms, components, patterns	43 Use Govt Digital Identity solution				✓										1/16
	44 Deliver services through central platform					✓									1/16
	45 Use and contribute to common components, patterns, platforms		✓	✓	✓		✓		✓			✓	✓	✓	8/16
Governance	46 Comply with guidelines and manuals				✓										1/16
	47 Review standards regularly						✓								1/16
	48 Only build apps if necessary						✓								1/16
	49 (Perhaps) don't build it									✓					1/16
Branding and consistency	50 Only display Govt content						✓								1/16
	51 Use standard domain						✓								1/16
Tech and tools	52 Modern tech stack	✓											✓		2/16

Country

Multi-country

State

Note: Australia, South Australia and Queensland included in total count but not shown. Source: BCG research and analysis; relevant standards information and guidance published on agency websites as at 24 May 2023 ([US](#), [UK](#), [Finland](#), [Denmark](#), [UAE](#), [Singapore](#), [New Zealand](#), [UNDP](#), [Ontario](#), [Western Australia](#), [South Australia](#), [Queensland](#), [New South Wales](#), [Victoria](#))

Australian Commonwealth Government

Table 5: Australian Commonwealth Government 13 Digital Service Standard Principles

#	Principle
1	Understand user needs
2	Have a multidisciplinary team
3	Agile and user centred process
4	Understand tools and systems
5	Make it secure
6	Consistent and responsive design
7	Use open standards and common platforms
8	Make source code open
9	Make it accessible
10	Test the service
11	Measure performance
12	Don't forget the non-digital experience
13	Encourage everyone to use the digital service

Source: [DTA Digital Service Standards](#) as at 24 May 2023

US Federal Government

Table 6: US Federal Government Digital Services Playbook Principles

#	Principle
1	Understand what people need
2	Address the whole experience, from start to finish
3	Make it simple and intuitive
4	Build the service using agile and iterative practices
5	Structure budgets and contracts to support delivery
6	Assign one leader and hold that person accountable
7	Bring in experienced teams
8	Choose a modern technology stack
9	Deploy in a flexible hosting environment
10	Automate testing and deployments
11	Manage security and privacy through reusable processes
12	Use data to drive decisions
13	Default to open

Source: [Digital Services Playbook](#) as at 24 May 2023

UK Government

Table 7: UK Service Standard Principles

#	Principle
1	Understand users and their needs
2	Solve a whole problem for users
3	Provide a joined-up experience across all channels
4	Make the service simple to use
5	Make sure everyone can use the service
6	Have a multidisciplinary team
7	Use agile ways of working
8	Iterate and improve frequently
9	Create a secure service which protects users' privacy
10	Define what success looks like and publish performance data
11	Choose the right tools and technology
12	Make new source code open
13	Use and contribute to open standards, common components and patterns
14	Operate a reliable service

Source: [Service Standard](#) as at 24 May 2023

UAE Federal Government

Table 8: UAE Federal Government Customer and Digital Government Services Policy Principles

#	Principle
1	Design easy and proactive government services
2	Government entities should request for information one-time and follow laws and regulations on data sharing or exchange
3	Government agencies should provide all their digital services through the unified digital platform
4	Government entities should raise awareness and promote their shared digital services and bundles to ensure their use

Source: [Digital Customer and Digital Government Service Policy](#) as at 24 May 2023

Finnish Government

Table 9: Finnish Government Principles of Digitalisation

#	Principle
1	We will provide services based on customers' needs
2	We will cut unnecessary red tape
3	We will build easy-to-use and secure services
4	We will produce benefits for our customers quickly
5	We will also serve in case of disruptions
6	We will ask for new information only once
7	We will make full use of the existing public and private online services
8	We will provide open data, open access to information and open interfaces for businesses and citizens
9	We will designate an owner for every service and its implementation

Source: [Principles of Digitalisation](#) as at 24 May 2023

German Government

Table 10: German Government User Experience Portal Guide Principles

#	Principle
1	Start with the user need
2	One for all and less is more
3	Decide based on data
4	Making things easy is hard work
5	Context of the use comes first, not device
6	Be consistent but not uniform

Source: User Experience Portal Guide version 1.0 (no longer published on agency website)

Danish Government

Table 11: Danish Government Common Requirements for Digital Services

#	Principle
1	Early user involvement
2	Language
3	Conventions for flow and functionality
4	Field validation
5	Personalisation
6	Support for operating systems and browsers
7	Support of screen sizes
8	Pass the joint public user test
9	Collection of knowledge about users' use of digital solutions
10	Use of infrastructure components and other components
11	Reuse of data sources
12	Compliance with agreed architectural standards
13	Solutions that must be on borger.dk and Virk must comply with the portals' common design systems and integration process.

Table 12: Danish Government Common Requirements for Digital Services – External Requirements

#	Requirement
1	The Administration Act
2	Security Legislation
3	Single Digital Gateway (YourEurope Portal)
4	Connection to Danish eID-Gateway
5	Web Accessibility

Source: [Common Requirements for Digital Services](#) as at 24 May 2023

Singapore Government

Table 13: Singapore Digital Service Standards Principles

#	Principle
1	To stay relevant and effective with changes in user needs and technology, digital services shall be reviewed at least once every three years and terminated as soon as they are irrelevant or ineffective
2	To reduce duplication and wastage of resources, mobile applications shall be implemented only if the same objectives cannot be met with web-based digital services
3	To avoid being seen as endorsing products or services of private-sector organisations, digital services shall display only content that is owned by, or under the control of, Agency or other Agencies. The digital service shall indicate clearly if the Agency has partial or full ownership of the content
4	To help the public identify legitimate government digital services and to enable Agencies to streamline their websites, a single website with gov.sg domain shall be used for each Agency (e.g. www.agency.gov.sg), except for Agencies in the area of education which may use the.edu.sg domain
5	To allow individuals and business to transact with the Government digitally from start to finish, digital services shall provide end-to-end services (except for those with physical or legal restrictions) including digital alternatives to wet ink signatures
6	To ensure that individuals and businesses can easily interact with the Government digitally, digital services must be well-designed to be: - Intuitive and usable: - Identify, access and navigate a service easily - Track and monitor transactions more efficiently - Complete a transaction or interaction more effortlessly - Accessible and inclusive: - Perceivable: Ensure contents are available in forms such as speech, large print, or Braille - Operable: Ensure functions are accessible through a keyboard, mouse or other assistive devices - Understandable: Clear, concise content that avoids jargon - Robust: Service can be accessed across devices - Relevant to the needs of users and provide a consistent experience across the Government - Adopt common design elements such as a standard masthead for a consistent user experience - Conduct regular reviews to ensure contents and services are up to date - Provide clear and relevant content

Source: [Design Principles](#) as at 24 May 2023

New Zealand Government

Table 14: NZ Government Digital Service Design Standards Principles

#	Principle
1	Identify your users and understand their ongoing needs
2	Be clear about what you are trying to change and why
3	Integrate security and privacy proportionate to risk from the outset
4	Be inclusive, and provide ethical and equitable services
5	Design and resource for the full lifetime of the service
6	Create and empower an interdisciplinary team
7	Work in the open
8	Collaborate widely, reuse and enable reuse by others
9	Design for our unique constitutional and cultural environment
10	Use digital technologies to enhance service delivery
11	Be a good data and information steward
12	Be transparent and accountable to the public

Source: [Digital Services Design Standard](#) as at 24 May 2023

UN Development Programme (UNDP)

Table 15: UNDP Digital Standards Principles

#	Principle
1	Plan for the long term
2	Default to open
3	Follow The UNDP Data Principles
4	Measure what matters
5	Form the right team
6	Do no harm
7	(Perhaps) Don't build it
8	Test early and often
9	Bridge the digital divide
10	Start with the need

Source: [UNDP Digital Standards](#) as at 24 May 2023

Government of Ontario

Table 16: Government of Ontario Digital Service Standard Principles

#	Principle
1	Understand users and their needs
2	Establish the right team
3	Be consistent
4	Design the service from start to finish
5	Ensure users succeed the first time
6	Test the end-to-end service
7	Make it accessible and inclusive
8	Be agile and user centred
9	Use open standards and common platforms
10	Embed privacy and security by design
11	Support those who need it
12	Measure performance
13	Be good data stewards

Table 17: Government of Ontario Design System Principles

#	Principle
1	Understand users and their needs
2	Only include elements that have a purpose
3	Be consistent
4	Design for everyone
5	Ensure users succeed the first time
6	Start simple
7	Continually test and improve – even after launch

Source: [Digital Service Standard, Design System](#) as at 24 May 2023

Western Australian Government

Table 18: WA Government Digital Service Design Standard Principles

#	Principle
1	Start with needs: user needs, not government needs
2	Do less
3	Design with data
4	Do the hard work to make it simple
5	Iterate. Then iterate again.
6	This is for everyone
7	Understand context
8	Build digital services, not websites
9	Be consistent, not uniform
10	Make things open: it makes things better
11	Take a one government approach

Source: [Digital Service Design Principles](#) as at 24 May 2023

New South Wales Government

Table 19: NSW Government Design Standard Principles

#	Principle
1	Work in a flexible, iterative way
2	Plan and protect users' privacy
3	Look to reuse and make reusable
4	Make it safe and secure from the start
5	Measure and improve, don't spin up and drop
6	Have a multidisciplinary team
7	Build in the open
8	Make it for everyone
9	Choose the right tech and tools
10	Deliver outcomes for customers, before solutions for government

Source: [Design Standards](#) as at 24 May 2023

Queensland Government

Table 20: QLD Government of Digital Service Standard Principles

#	Principle
1	Understand user needs
2	Have a sustainable multidisciplinary team
3	Use agile and customer-centred processes
4	Understand the tools and systems required
5	Make digital services secure
6	Build consistent and responsive design
7	Use open standards and/or common platforms
8	Make source code open by default
9	Make digital services accessible
10	Test the digital service
11	Measure the performance and improve
12	Don't forget the non-digital experience
13	Encourage a shift to the digital channel

Source: [Digital Service Standard](#) as at 24 May 2023

Victorian Government

Table 21: Victorian Government Digital Design Principles

#	Principle
1	Easy to use: Make digital the first choice for our customers
2	Simple: Leads directly to the most used services and information
3	Available: 24/7 access
4	Useful: Designed to solve problems
5	Consistent: Works the same way for common functions, like data collection
6	Joined together: Integrated between agencies
7	Mobile: Designed for mobile and tablet first
8	Complete: Support customers to complete activities online, without manual steps
9	Clear: Use clear, active language
10	Fast: Quick to submit, and provide an efficient end-to-end service
11	Aware of history: Able to provide a record of past interactions where appropriate
12	Aware of user: Able to use known information from previous interactions with government

Table 22: Victorian Government Design Principles

#	Principle
1	Focus on the customer
2	Solve the right problem
3	Make it simple
4	Build on the standard
5	Progress over perfection
6	Trusted by design
7	Connect and partner
8	Innovate with purpose

Source: [Digital Design Principles](#); [Design Principles](#) as at 24 May 2023

Appendix B: Structure

Figure 23: Singapore's standard is structured around outcome-focused principles, supported by output requirements

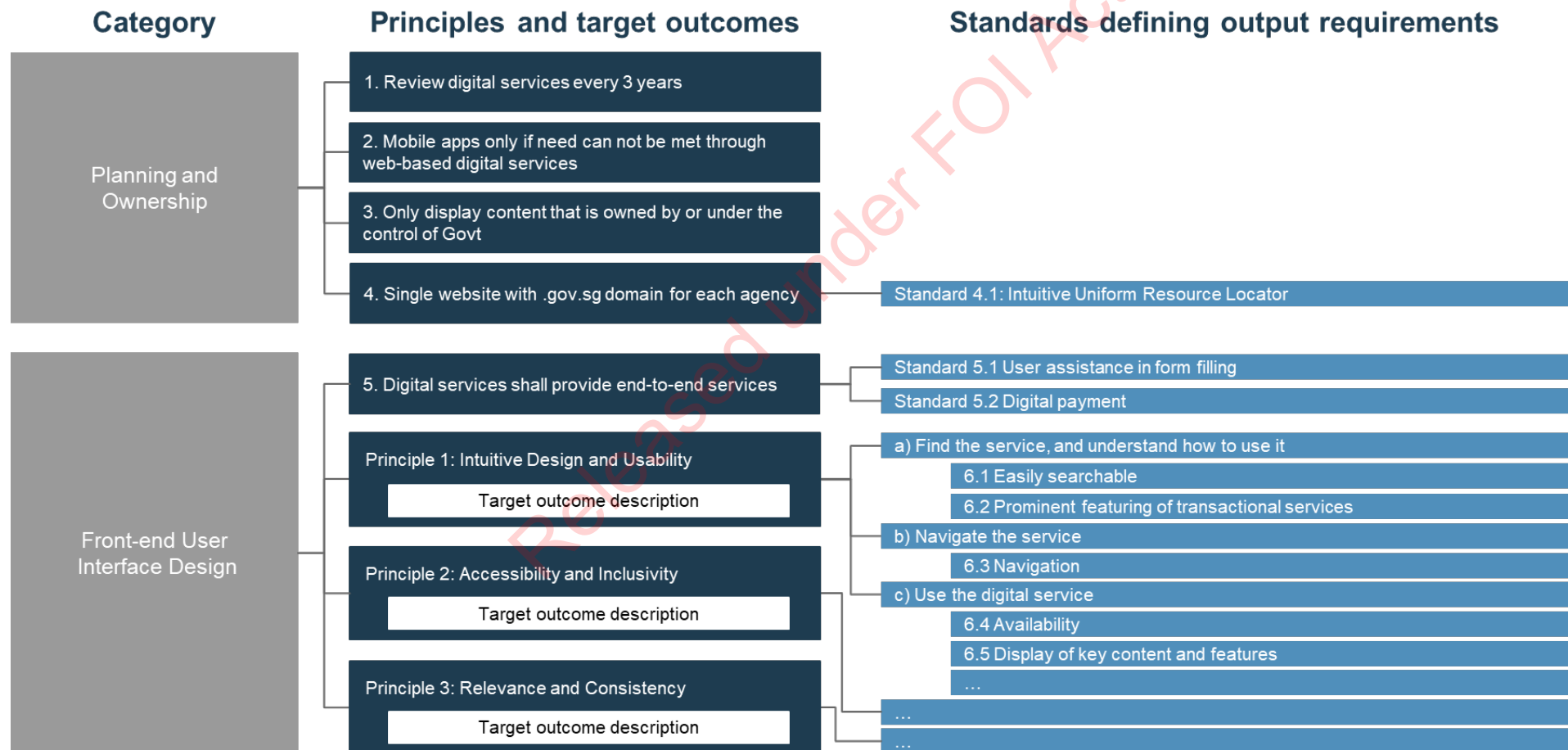


Figure 24: NSW Design Standard's structure provides guidance for each principle, mainly focused on inputs, process and outputs

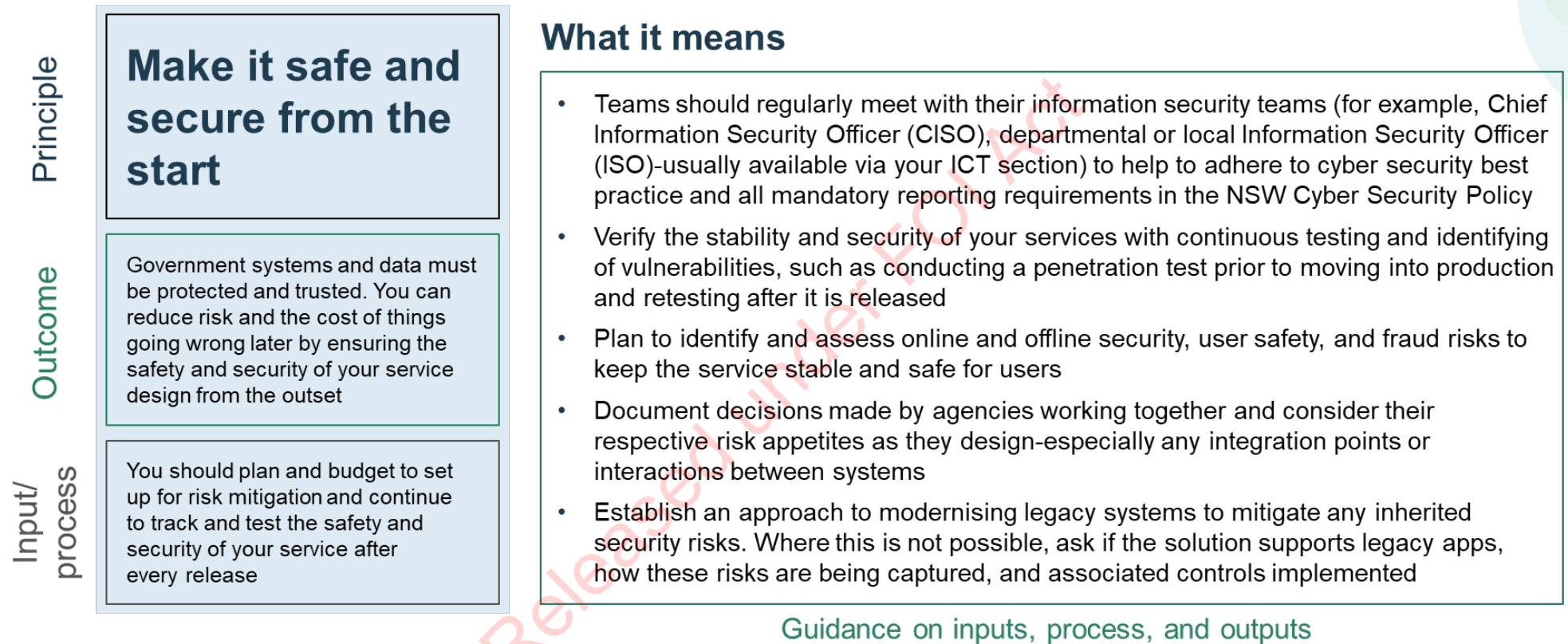


Figure 25: New Zealand's Digital Services Design Standard covers both process and outcomes through a clear, repeatable structure

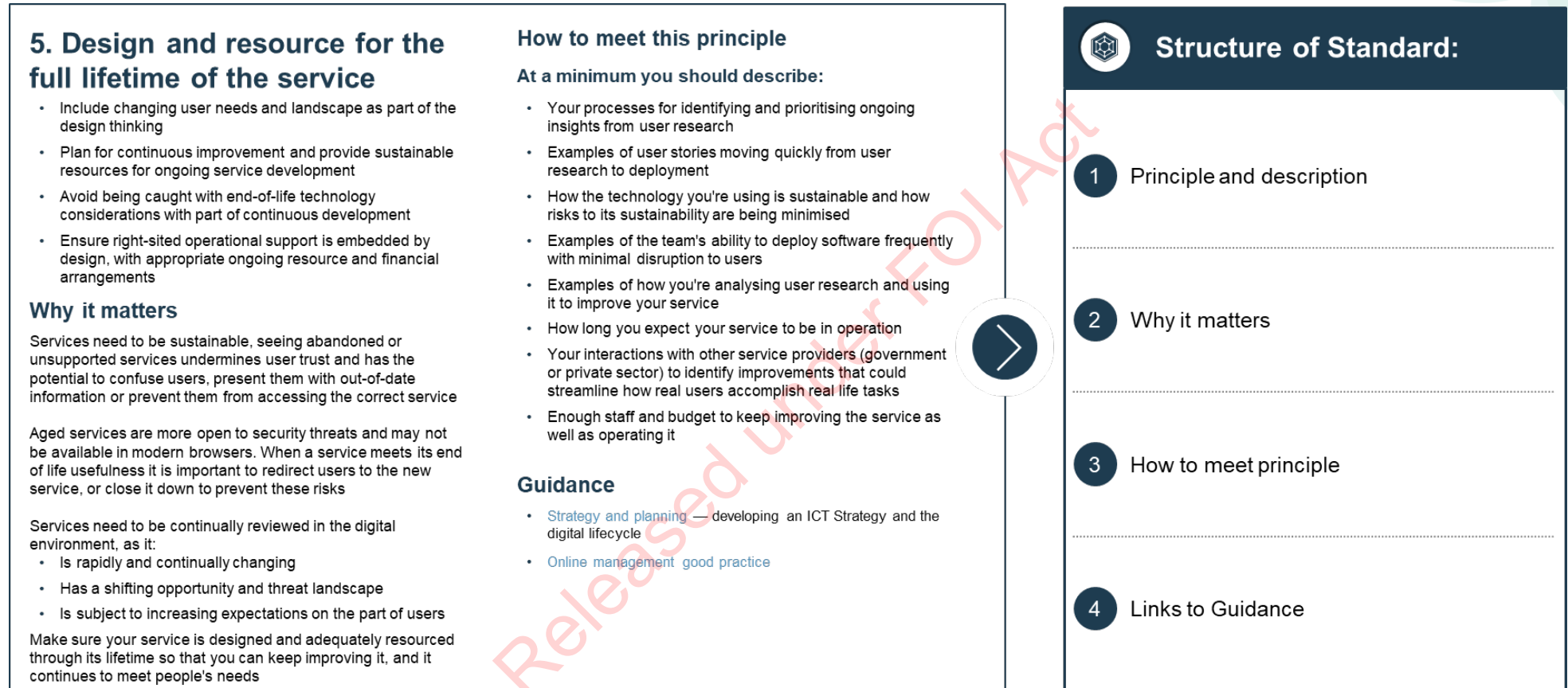


Figure 26: Victorian Government's Digital Design Principles are supported by detailed guides and standards

Digital Design Principles	Principle Type	Guidance on inputs/process and outputs contained in Digital Guides
➤ Easy to use: Make digital the first choice for our customers	Outcome	Digital guides - Digital guide home - Make content accessible - Producing multilingual content - Design and develop a digital presence - Make your project open source - Research user experience (UX) - Create and manage email newsletters - Decide if you need a mobile app - Measure how content performs - Understand the API design principles - Create a content strategy and manage content
➤ Simple: Leads directly to the most used services and information	Outcome	
➤ Available: 24/7 access	Outcome	
➤ Useful: Designed to solve problems	Outcome	
➤ Consistent: Works the same way for common functions, like data collection	Output	
➤ Joined together: Integrated between agencies	Output	
➤ Mobile: Designed for mobile and tablet first	Output	
➤ Complete: Support customers to complete activities online, without manual steps	Outcome	
➤ Clear: Use clear, active language	Output	
➤ Fast: Quick to submit and provide an efficient end-to-end service	Outcome	
➤ Aware of history: Able to provide a record of past interactions where appropriate	Output	
➤ Aware of user: Able to use known information from previous interactions with government	Output	

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-6

The following is the annexure marked **FT-6** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains the DTA document 'Digital Service Standard — Feedback and Actions Register'.

.....
Daniel Davison
Solicitor

Digital Service Standard – Feedback and Actions Register

Feedback/request	Action taken	Notes/comments
Andrew Morrison		
(Via comment on slide 5) - Will we also explore the development of EX metrics as a part of this? https://www.forrester.com/blogs/ex-measurement-best-practices-metrics-and-data-sources/	Noted.	We are still working out the specifics of how the metrics will be applied and if different metrics are required from an internal to government perspective. We will review this link in that context.
(Via comment on slide 6) Will the scope also explore the development of EX metrics as part of this?	No action • Do you have any exemption policies, and if so, to what do they relate? • To whom is this applicable? • How does one get an exemption? Must they apply? • How is the exemption outlined, and what is the process? Is it a case of 'if you tick the following boxes, then you get one' or is it more like 'tell us your situation and we can go from there'? • Who developed this policy? • Who was this in consultation with? • Does someone own this, currently, is it updated, at all? • Why do you have an exemption policy? What is it that made you think that this would be needed? • Did you pre-emptively create the policy, or did it come off the back of people expressing the need for such a policy? • What are the implications of someone being exempt from the main policy?	We consider this is incorporated as part of criteria 9 and 10. We also note that the DSS should not be applied in a linear way and therefore it will be applied consistently throughout the project lifecycle. We will make sure the guidance reflects this.

	What exactly does the exemption mean, is it merely a deadline extension? taken	
(Via comment on slide 6) 'clarify your objectives' – may want to clarify what our definitions of success are for the service	No action taken	We consider this is incorporated as part of criteria 9 and 10. We also note that the DSS should not be applied in a linear way and therefore it will be applied consistently throughout the project lifecycle. We will make sure the guidance reflects this.
(Via comment on slide 6) 'Do you understand the policy lever this service is trying to address? The impact to the citizen?'	Added policy as part of the following dot point: <i>Understand how your service supports delivery of policy and strategic government initiatives such as the Data and Digital Government Strategy.</i>	Agreed. We have updated the text accordingly.
(Via comment on slide 6) If we are removing the 'Don't forget the non-digital experience' should we be encouraging at this stage to also identify how the service can be accessed outside of the scope of digital to keep the services in alignment at least?	Added a dot point to refer back to Services Australia's Customer Experience Standard. <i>Consider the non-digital experience through Service Australia's Customer Experience Standard</i>	We have been working with Services Australia on their multi-channel <i>Customer Experience Standard</i> , so have referred to this as the appropriate angle for considering the non-digital experience.
(Via comment on slide 7) – There is a train of thought around Personas being dead, and a shift to mindsets. May be worth considering if we want to articulate that explicitly. https://www.nsw.gov.au/onecx/blog/designing-content-for-customer-mindsets https://govservicedesign.net/programme/mindsets-vs-personas	No action taken	We do not have a lot of detail about this concept. Lisa will reach out to Andrew to discuss further.

https://codefor.ca/blog/goodbye-personas-how-mindsets-can-help-you-build-empathy-and-reduce-bias		
(Via comment on slide 8) It may be also worth around digital inclusivity also around bandwidth, device (mobile vs desktop), connectivity (poor or sporadic internet availability)	Updated to incorporate language from the DDGS around digital inclusion on Slide 8. <i>Consider the non-digital experience through Service Australia's Customer Experience Standard</i>	We have been working with Services Australia on their multi-channel <i>Customer Experience Standard</i> , so have referred to this as the appropriate angle for considering the non-digital experience and those with poor connectivity.
(Via comment on slide 8) Should we call out explicit standards such as the Flesch-Kincaid readability test, and factor that into the AGA as a standard?	Have included a reference to the Australian Government Style Manual. <i>Use plain English to support people to understand what they need to do, through the Australian Government Style Manual.</i>	We have referred back to the Australian Government Style Manual to support alignment with Government requirements. We could connect to the other resources mentioned in the criteria's resource section (once built out).
(Via comment on slide 9) - Would we also activity encourage engagement with states and local for a true-joined up experience? So 'For Bonus Points - join up with the states!'	Updated slide 9 to include: <i>Consider how you can link-up with existing state and territory digital services, where appropriate.</i>	
(Via comment on slide 9) - Not only ask for it once, but from the outside, architect what you must have, and what is nice to have. What will you do with the data from a cybersecurity perspective? Only use it for the transaction and then discard it? Keep it ongoing? Will you make that data available to other services or systems?	No action taken.	We consider this is addressed in criteria 7.
(Via comment on slide 9) - Also support interoperability between sharing common datasets (open data)	Updated slide 9 to include: <i>Encourage interoperability between sharing common datasets (open data).</i>	
(Via comment on slide 10) – Should we be also encouraging to seek out during this stage what are the security requirements, or breach notification	Updated slide 10 to include the following dot point:	

requirements? The Cybersecurity theme may not be strong enough in this message	<i>Consider the cyber security requirements needed to support your service.</i>	
(Via comment on slide 11) - Are we actively dropping the making 'source code open by default' principle? Is there a reason that we aren't encouraging the share-back approach?	Noted.	Chris has highlighted a preference to move away from open source to open standards. It would be good to understand the two sides of this argument a bit further – we will schedule some time with you to discuss.
(Via comment on slide 11) - Could we make this stronger to help understand at this point what the spectrum of reuse may be? The service they are designing could be anywhere on the spectrum of 1. Re-use of documentation/process (business case, architecture, operating models, procurement approaches) 2. Re-use of the system (make the system modular/configurable so that it is relatively easy to provide a copy of the service or solution to someone else to build upon/extend your solution or change it slightly) 3. Is it a candidate for a white-label service (or components of your service)? What components could you white-label to allow others to use in real-time also? (an API gateway to a service, a dataset). What costs or operating model should be considered? I think this is an important piece, as it really goes to re-use. Reuse doesn't have to be the whole system, but we should try to articulate what parts could be re-used.	Updated Slide 11 to include: <i>Understand what processes or documentation could be re-used.</i>	
(Via comment on slide 12) - Including data lifecycle and retention management. Do you need to store it? What is the risk of capturing it and being able to	Updated slide 12 with the following dot point:	

use it, vs storing it and increasing risk around compromise?	<i>Consciously consider the data lifecycle, including how you will collect, manage, store and use data.</i>	
(Via comment on slide 14) - There is a risk that if the question of 'how will you monitor your service' isn't asked earlier on, all monitoring will be retrofitted. This means it could impact on the way that solutions are architected - or worse impact on the WofG ability to be able to aggregate and monitor performance. We should relatively quickly try to establish some baseline metrics that agencies should capture at a minimum.	No action taken	While we understand your point, the DSS should not be applied in a linear way and therefore it will be applied consistently throughout the project lifecycle. We will make sure the guidance and detailed documentation reflects this.
(Via comment on slide 14) - This will also have importance of 'how will you monitor' for Employee or Internal Experience. Will employee services need to report against WofG measurements?	Noted.	We are still working out the specifics of how the metrics will be applied and if different metrics are required from an internal to government perspective.
Lauren Mills		
Align the language used in the DSS to the DGGS eg. 'connected services' instead of 'joined-up' services, 'all people in the business' instead of 'everyone'.	Updated criteria 3 and 4 to reflect the DGGS language.	
Section 47E		
(Via DSS consultation) Feedback from agencies is that there is no guidance on how to ensure accessibility	Noted.	Agreed. As discussed in our follow up meeting, we are keen to provide as much guidance and support to agencies as possible on accessibility. We have been meeting with a number of stakeholders who have got resources that we could potentially link to, but any further suggestions, please send through.
Section 47E		
(Via comment on slide 8) - Defence model incorporates the consideration of fundamental inputs they have eight standardised elements:	Updated Criteria 1 – clarify your objectives to include the following:	A very good point, but we consider this fits well in the first criteria as people are considering the objectives of their service.

Organisation, personnel, collective training, major systems, supplies, facilities, support, command and management. Obviously not all relevant but they go to considering all elements of success are considered and not overlooked. A good example I have found was where a focus was on building a plane but everyone forgot about alterations to the runway. If you are joining up services they need to design in consideration for not only users but those integrating with the service. Design for everyone is implied but might need more detail	<i>Consider the fundamental inputs and integration required for your service.</i>	
(Via comment in slide 8)- people may consider from only a UX perspective rather than a back-end perspective	Noted.	
(Via comment in slide 9) - Can reference AGA on reusable technology	No action taken.	This is reflected on slide 11 – criteria 6.
(Via comment in slide 10)- There could be a missing piece around POCs and pilots to build trust through testing and design. smaller investments over large big bang approach that try's to do too much but then doesn't deliver.	Noted.	We will build on this throughout the detailed DSS document and guidance.
(Via comment in slide 12)- Consider adding in a reference to check AGA for the latest advice and guidance,	No action taken.	We consider this is covered on slide 11 under criteria 6.
(Via comment in slide 14)- Agree there should be something about establishing a what good looks like before you even start and understanding desired end state and mapping out how you PLAN to get there. Metrics should be set around success milestones ie if your not adding value along the way	Noted.	While we understand your point, the DSS should not be applied in a linear way and therefore it will be applied consistently throughout the project lifecycle. We will make sure the guidance and detailed documentation reflects this.

then you should be considering stopping or amending your path.		
(Via comment in slide 14)- Also reference to check AGA on latest advice.	Updated slide 14 to include the following dot point: <i>Check the Australian Government Architecture for the latest guidance on whole of government measurements.</i>	
(Via comment in slide 16)- Consider adding in AGA or have a separate mapping to AGA as the AGA has relevant domains and capabilities across the DSS for agencies to reference real life examples and support from agencies who have developed before or lessons learned. Given its evolving mapping can easily assist agencies find what they are after. Team could assist with this.	Updated slide 16 to include AGA in the 'Enabling and supporting Components' section	
Section 47E		
(Via email) notes the differences between the DSS as a policy and as a standard	Noted.	
Section 47E		
(Via email) 'design for everyone' is redundant if not all digital products are made accessible to WCAG standards	Noted. Updated slide 8 to include the following dot point: <i>Design your service to meet latest WCAG AA guidelines.</i>	
(Via comment in slide 4) Section on procurement? APS should be following Australian Government ICT Standards for Accessible Procurement ... https://www.financeminister.gov.au/media-release/2016/08/22/access-technology-made-easier-for-more-detail-on-state-government-implementation-see-procurement-section-at:	Noted.	Given we are not setting policy in the DSS, we have not reflected this. Noting that we consider this is an interesting idea, we will share it with our procurement colleagues here in the DTA.

https://www.accessibility.sa.gov.au/policy/south-australian-government/online-accessibility-policy		
(Via comment on slide 5) - Working in State Government, this was the single point of failure for the old/current standard. The Digital Service Standard was quoted as a reason why internal solutions were not being made accessible (out of scope) when teams redevelop internal facing solutions such as intranets, learning management systems, records management etc. In general APS and State Gov staff are trying to do the right thing but just having the scope as public facing seems at odds with the quoted move to increase employment opportunities for people with disability in the APS (if internal solutions are not being made accessible, how are we going to attract and keep staff with visible and hidden disability?). For an example of internal facing see scope at: https://www.accessibility.sa.gov.au/policy/south-australian-government/online-accessibility-policy	Updated slide 5 to include the following dot point: <i>Internal to government (staff facing) services, such as:</i> • <i>Intranets</i> • <i>Learning management systems</i> • <i>Records management system</i>	We may reach out to you to understand this one further and how we can build out the definition in the detailed DSS document.
(Via comment in slide 5)- Why just 'high volume'? Shouldn't this be setting the standard required from/expected by government for all digital channels whether public facing or staff facing? APS as the employer of choice etc. SAGOV experienced the same issue when redesigning their policies, when should the new policy apply, as in it's not feasible or realistic to retrofit existing/old solutions	Noted. Updated to remove 'high volume' as language could be confused with 'existing high volume services'.	

In the end settled on "All new or significantly upgraded SA Government online applications" after wide-ranging consultation ... sets clear expectation going forward and draws line in the sand etc etc etc		
(Via comment in slide 5)- change to 'internal and public facing	No action taken.	We are trying to demonstrate that the same criteria applies with the addition of internal services so have kept this slide as is.
(Via comment on slide 8) - Change to "Design your service to meet the latest WCAG level AA guidelines" ... future proofing and will help to keep the standard current and in line with international best practice. This will also align it with the Data and Digital Strategy ("ensuring all websites and services meet the latest Web Content Accessibility Guidelines")	Updated to 'Design your service to meet latest WCAG AA guidelines.'	Updated to align with the DDGS language.
Section 47E		
(Via DSS consultation in reference to slide 5)- make the language stronger	Updated slide 5 to include the following dot point: <i>Internal to government (staff facing) services, such as:</i> • <i>Intranets</i> • <i>Learning management systems</i> • <i>Records management system</i>	We may reach out to you to understand this one further and how we can build out the definition in the detailed DSS document.
Section 47E		
(Via DSS consultation)- What strategies do we have in place for measuring when services need to be retired?	Noted.	We consider this is incorporated as part of criteria 9 and 10. We will make sure the guidance reflects this.
Section 47E		
It would be beneficial to continue to emphasise the core principle of discovery first, following by testing of concepts/prototypes and then attempting to	Noted.	We will consider this as we build out the detailed DSS documentation.

deliver the product or service. Whether this takes on the old 'discover, alpha, beta, live' or possibly a re-arrangement of the 10 principles to articulate the importance of a staged approach.		
How are we considering the non-digital experience/channels? It's important to draw attention that digital or one channel is unlikely in any service and that designers, researcher and developers need to consider the integration to deliver a seamless experience. This should consider things like digital literacy or experience overlaps.	Added a dot point to refer back to Services Australia's Customer Experience Standard. <i>Consider the non-digital experience through Service Australia's Customer Experience Standard</i>	We have been working with Services Australia on their multi-channel <i>Customer Experience Standard</i> , so have referred to this as the appropriate angle for considering the non-digital experience.
Slide 7 - User researchers prefer "behavioural archetypes" or "user types" which may have been mentioned in slide 6 by other commenters. There is an ongoing debate in this space and the language may shift over time, but there is a preference for this language currently over "personas". The first article you provided to the group when seeking feedback also outlined the reasons for this language.	Updated to include the below dot point: <i>Identify your user groups and any behavioural archetypes that need consideration.</i>	
Slide 18 - There are a number of external forums that this can be tested with. This includes the "Data and Digital Professions members' community" run by APSC Digital Profession.	Noted.	We are running a session with the Digital Profession community in 2 weeks to take them through this.
(Via email) It's worth considering how these guidelines will be used by non-government designers, researchers, product managers, and developers as a signpost for best practice. It is extremely valuable to have something with gravitas to point to when you are working in the private sector. To this end, it might be beneficial to reach out to private sector users for feedback about accessing the standard and any additional	Noted.	If you have any suggested private sector partners that we could engage with, we would appreciate you passing on their details.

considerations. This will go toward furthering the DTA's strategic position as a trusted authority on digital best practice.		
The BCG report looked across jurisdictions to evaluate similar schemes. There is benefit in sharing more widely to test new DSS concepts with agencies.	Noted.	
Section 47E		
(Via comment on slide 6) A Privacy Impact Assessment or threshold assessment can assist and support this	Included a dot point re PIAs on slide 12: <i>Undertake a Privacy Impact Assessment to understand the privacy implications of your service.</i>	We have strengthened this as part of criteria 7.
(Via comment on slide 7) Recommend that a Privacy Impact Assessment (PIA) or at a minimum Threshold assessment be conducted to map or identify to ensure privacy compliance is addressed as the forefront of any new system/project.	Included a dot point re PIAs on slide 12: <i>Undertake a Privacy Impact Assessment to understand the privacy implications of your service.</i>	We have strengthened this as part of criteria 7.
(Via comment on slide 7) The Following OAIC Consumer data Right Privacy Safe Guidelines may need to be considered. https://www.oaic.gov.au/consumer-data-right/consumer-data-right-guidance-for-business/consumer-data-right-privacy-safeguard-guidelines	Noted. We will link to this as part of the resource section for Criteria 5 and 7.	
(Via comment on slide 12)- Consider future use of the data, eg they might want to survey participants. or use it for law enforcement., etc	Updated slide 12 to include the following dot point: <i>Consider and communicate any future uses of the data (including if it will be made open and or shared).</i>	We will add further details about what those future uses could be in the more detailed version of the document.

(Via comment on slide 14)- Consider establishing a 12mth or 6mth review/audit.	Noted.	We will consider specific timeframes for review/audit as we build out the detailed DSS documentation.
(Via comment on slide 15)- Consider publishing updates, results and findings.	Updated slide 15 to include the following dot point: <i>Consider publishing updates, results and findings, to promote transparency.</i>	
Section 47E		
(In reference to slide 13)- It's hard to measure 'excellent' services, it's a nebulous term	Updated to change 'excellent' to 'high quality'	
(In reference to slide 6)- Add – Focus on the benefits for customers rather than the solution	We consider this is covered under criteria 2 – Understand User Needs.	
(In reference to slide 8)- Include alternatives (other channels) for the service to cater for all Australians	Added a dot point to refer back to Services Australia's Customer Experience Standard. <i>Consider the non-digital experience through Service Australia's Customer Experience Standard</i>	We have been working with Services Australia on their multi-channel <i>Customer Experience Standard</i> , so have referred to this as the appropriate angle for considering the non-digital experience.
(In reference to slide 12)- Add - Clearly communicate when your data will be made open and or shared	Updated the following dot point to include 'clearly' <i>Consider and clearly communicate any future uses of the data (including if it will be made open and or shared).</i>	
(In reference to slide 15)- Add - Conduct regular user and system testing to ensure that changes applied are fit for purpose	No action taken.	We consider this is included in Criteria 2 – understand user needs.
(Via email) - What's missing – Build Support - Build the capability of staff to support the service etc. (this would fit under Action Mission 5 Data and Digital Foundations and would link to the APS Reform Agenda)	Updated slide 15 to include the below dot point: <i>Invest in your people by building the capability of staff to support the service.</i>	

(Via email) - User and system testing is missing from the design and build of services	No action taken.	We consider this is included in criteria 2 – understand user needs.
(Via email) How will you measure the DSS?	No action taken.	We are proposing to use our new digital service measurements to help measure the success of the DSS. This builds on the work Nous did for our branch last financial year. Happy to take you through this if you have any questions.
(Via email) Needs to be more aligned to the DDGS – e.g. simple and seamless services	Updated criteria 3 and 4 to reflect the DDGS language.	We will continue to incorporate the DDGS language throughout the more detailed DSS document.
(Via email) Are there checks and balances in place for a new service before it goes live – i.e. to check that it meets the DSS?	Noted.	We are currently discussing how we can best incorporate the DSS under existing IOF process (e.g. through Contestability and Assurance states). Grateful for any thoughts you might have on this.
Lucy Poole		
(Via consultation with Lisa) Would like to see something in here about considering Indigenous Inclusion	Updated slide to include the following dot point: <i>'Consider First Nations digital inclusion in respect to access, affordability, and digital ability'</i>	NIAA have a First Nations Digital Inclusion Plan (2023-26) https://www.niaa.gov.au/indigenous-affairs/economic-development/first-nations-digital-inclusion-plan The dot point added is a direct reflection of the language used on their website
Section 47E		
(Via email on slide 6) - it might be helpful to encourage consideration of any interdependencies such as systems, processes or policies that relate or could be impacted by transitioning to or making major changes to a digital solution.	Updated slide 6 to include the following dot point: <i>Consider the fundamental inputs and integration required for your service – including systems, processes and policies.</i>	
(Via email on slide 7)– the guidance around conducting regular user research and observation points seem to fit more within the 'monitor' element, especially if this is a transition to a new	Noted. We have included the following dot point to slide 7:	We consider that regular user research sits better under this criteria as the 'monitoring' criteria is more around understanding the success of a service. We also note that the DSS

digital solution and the current users are not offered a digital option. It may need to be refined to guide the initial user consultation and exploration of available digital technologies to support user needs. Further, a point about involving users in the development, build, and testing of the initial design.	<i>Involve users in the development, build and testing of the service.</i>	should not be applied in a linear way, so agencies will be using it at different points.
(Via email on slide 8)– this seems to overlap with the previous element and might need to consider the cultural diversity within the Australian citizen base. There are over 3 million migrants and about 30% of citizens that were born overseas and English is not their first language (in some regions up to 60% of citizens are born overseas). In addition, there are different levels of digital literacy, provision of internet connectivity, and barriers to access such as those with disabilities, and other vulnerable groups within the population (e.g., prisoners, domestic violence, refugees, etc.).	Noted.	Based on feedback from stakeholders, we consider that it is important to keep criteria 2 and 3 separate. Criteria 3 is very much about increasing accessibility and inclusion in digital services. In the detailed DSS documentation, we will be sure to draw out the differences between 2 and 3 in a more clear way.
(Via email on slide 9)– the more commonly used digital systems term could be ‘connected’ rather than ‘joined-up’. An issue that is often raised around connected services is the limitations of citizen consent and the obligations under the Privacy Act, especially in relation to the use of personal or sensitive information.	Updated criteria 4 to reflect the DDGS language of ‘connected’.	
(Via email on slide 10)– it may be beneficial to consider the selection of providers and their sub-contractors within this element. It could also be helpful to reference alignment with the whole-of-government Hosting Strategy and compliance with the Hosting Certification Framework requirements for providers that host government data. In addition, a point about budgeting to seek expert	Updated slide 10 to include the following dot point: <i>Understand how your service will align to the Whole of Government Hosting Strategy and the Hosting Certification Framework.</i>	We will build out the broader guidance on this as part of the detailed DSS document.

advice for the legal, security, and other aspects of the design. Another important consideration could be having a mechanism for users to report bugs, security issues, lodge a complaint and escalate, if needed.		
(Via email on slide 11)– I’m not sure if using an & and dropping the ‘of’ is appropriate for a standard. There are digital government systems that are used by Australian citizens located offshore (e.g., DFAT, Defence, born overseas, on holiday) It could be good to add a point about any relevant international standards and requirements such as the need to process international payments. Another consideration is sector specific standards and patterns such as the Fast Healthcare Interoperability Resources (FHIR) standard for exchanging digital health data for use in a variety of settings and systems.	Noted.	We will build out the broader guidance on this as part of the detailed DSS document.
(Via email on slide 12)– some data has legislated retention obligations that may need to be considered, such as those within the National Archives Act. There are also requirements under the Privacy Act that may need to be considered around the collection, use and storage of different types of information. Some specific uses and sectors have additional ethical and legal obligations such as ethics for medical research or specific legislation for systems such as the My Health Record Act and Rules.	Noted.	We will build out the broader guidance on this as part of the detailed DSS document.
(Via email on slide 13)– perhaps another consideration is the need to balance the use of new technology with the rate of user adoption, user expectations and perceptions (may not want the	Updated slide 13 to include the following dot point:	

government to be leading edge) and trust of the technology. It also requires funding a significant change management effort to train citizen or APS users.	<i>Understand the rate of adoption of new technologies and if users would want to see it in a government service.</i>	
(Via email on slide 14)– it may be relevant to refer to the whole-of-government Digital and ICT Benefits Management Policy, noting that it is voluntary but offers policy standards, assessment criteria and guidance on measuring the benefits of a new digital solution. Another consideration would be transparent reporting of the appropriate measurements of the success and user satisfaction with the solution. The Benefits Management Policy could also be flagged in the first element ‘clarify your objectives’ as best practice is to consider the metrics that will be used and/or reported to demonstrate the objectives have been achieved.	Updated slide 14 to include the following dot point: <i>Consider and apply the Whole of Government Digital and ICT Benefit Management Policy</i>	We consider that the transparency piece fits best in criteria 10 (as it currently sits).
(Via email on slide 15)– it could be valuable to consider a broad range of stakeholder and user feedback for continuous improvement. For example, global trends, consultation across government with service owners of similar solutions, following online relevant technical and user forums, etc. I suggest the regular user research and observations point may belong here too. the service owner may also want to understand and schedule regular meetings with providers to have input into the technology roadmap for the solution. For example, what are the technology providers plans to improve or release new versions and what is the duration of the support for the version in use. Another consideration may be incorporating a	Noted.	We consider this is included as part of criteria 2. We will be sure to link back to it as part of the more detailed DSS document.

mechanism for users to provide immediate feedback on the user experience.		
(Via email) Does the proposed scope of the new Digital Service Standard meet your expectations? What is your overall impression of the proposed scope of the Digital Services Standard? The draft has a good coverage of the generic scope of a new digital service. There are some opportunities for minor refinements that are outlined above. I also agree with the comments Andrew Morrison has added to the slide deck. I'm not an expert on usability and accessibility standards that have been referenced by Cliff Edwards.	Noted.	Have updated accordingly.
(Via email) Do any statements stand out more than others? I was a bit unsure of the difference between 'understand user needs' and 'design for everyone'.	Noted.	As highlighted above, based on feedback from stakeholders, we consider that it is important to keep criteria 2 and 3 separate. Criteria 3 is very much about increasing accessibility and inclusion in digital services. In the detailed DSS documentation, we will be sure to draw out the differences between 2 and 3 in a clearer way.
(Via email) Are any statements obsolete/redundant? Which, if any, statement may be obsolete or redundant? I wonder if the 'Understand User Needs' and 'Design for Everyone' statements could be combined.	Noted	As above.
(Via email) Are any statements unattainable? Which, if any, statements are unattainable? I'm not sure if all service owners would have sufficient and current data to make 'data-driven decisions'. Perhaps 'evidence-based decisions' could more achievable.	Noted.	We will consider this as we build out the detailed DSS documentation and guidance.

(Via email) Is there anything that you think that we have missed? What's missing? I think there are other Australian and International standards, policies, and frameworks that could be relevant (see above). Some guidance on considering sector-specific requirements may also be helpful. There are also government targets for SME, Net Zero Emissions, Indigenous Participation, etc. that may need to be factored into the Standard.	Noted.	We will incorporate these as part of the detailed DSS documentation.
(Via email) Is there anything that you consider needs more emphasis in the Standard? What needs more emphasis? Its not entirely clear if the use of the Standard is mandatory and if any reporting, assurance checks, etc. may be required.	Updated slide 3 to include the following dot point: <i>Better enforce the use of the Standard across agencies.</i>	
(Via email) How could we enforce the DSS to ensure it meets its intended purpose? In addition to the answer to the question above, I wonder if the approach required to foster use of the Standard is enforcement or education and awareness through the provision of additional guidance materials such as templates, links, resources, etc.	Noted.	We are currently putting together a list of guidance materials and resources that we can connect agencies to. We would love any suggestions you may have in this space.
(Via email) Could anything be done to improve/ drive sentiment/ commitment? What could be done to improve or drive sentiment and commitment to the applying the Standard? There are only two resources referenced at the start of this presentation and both are non-government sources. I'm not sure if this is demonstrating sufficient research and consultation was conducted to develop/improve this version of the Standard. It could be good to state the problem that this version	Noted.	This is an early draft and we have a plan to engage heavily across government over the coming months commencing week of 14 August. We have also already commenced informal engagement with agencies.

is designed to solve and the value proposition it offers to benefit the service owner. Examples: Will this save you time or money or both? Will it prevent user issues and what types?		
(Via email) Do you know of any stakeholders or forums we should consult with externally? Who should we consult with on this draft Standard? a. Industry and Community Peak Bodies b. Office of the Australian Information Commissioner c. Australian Cyber Security Centre d. Australian Competition and Consumer Commission (insights on Consumer Data Rights currently for banking industry but may expand) e. Other government departments and agencies (federal, state and local levels)	Noted.	
Section 47E		
(Via email) The revised DSS principles align well with the Contestability perspective and should result in better outcomes, in particular the shift towards ongoing assessment throughout the lifecycle of the service. Some specific favourable commentary regarding the transaction threshold was received as stakeholders have raised this question with us in the past.	Noted.	We will continue to engage with you over the coming months about how we can support the Contestability role and what guidance is required.
(Via email) The team would be a keen to see visualisation of the changes between the existing, and future DSS and understand the delta between the two.	Noted.	We have included a slide in the pack to support this.
(Via email) The rationale behind open-source vs open standards would be good to share. There is a very that the DTA has historically been a champion for use of open-source technologies.	Noted.	The CEO has highlighted a preference to move away from open source to open standards. It would be good to understand the two sides of

		this argument a bit further – we will schedule some time with you to discuss.
(Via email) The team is keen to see how the underlying execution, processes and assessment will work. DSS is currently considered as part of the existing DCAP processes so this will result in some changes in this space.	Noted.	We will continue to engage with you over the coming months about how we can support the Contestability role and what guidance is required.
(Via email) As communicated in the session, Agencies routinely express concern with the quantity of data the DTA already asks for as part of Wave and other data collection mechanisms.	Noted.	We are looking into how we can reuse existing data collection mechanisms to reduce burden on agencies. We would be interest in discussing this further with you to understand where the pain points are.
(Via email) The DSS content aligns with the AGA in specific areas such as re-use, so it is worth noting that Contestability is working with the AGA team to align processes and understand the re-use mandate and its enforceability. Our interest is in ensuring that agencies are consulted, aware of their obligations, and are provided with sufficient tools to successfully comply. This extends to understanding Contestability's' role in any assessment or enforcement activities.	Noted.	We will continue to engage with you over the coming months about how we can support the Contestability role and what guidance is required.

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-7

The following is the annexure marked **FT-7** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains email correspondence between me and Mr Chris Fechner, CEO of the Digital Transformation Agency, dated 9 July 2026 (my email) and 17 July 2026 (Mr Fechner's response).

.....
Daniel Davison
Solicitor



➔ **Fraser Tweedale**

to Chris Fechner ▼

Jul 9 (18 days ago)

Sent



Reply to all

Actions ▼

Dear Mr Fechner,

Forgive my boldness in reaching out to the CEO directly.

I am on a mission to find out why the DSS v1 criterion 8 "Make source code open" was not included in DSS v2.

DTA staff have been diligent and worked in good faith with respect to my FOI activity in pursuit of understanding this change. A series of requests has so far yielded only a little concrete information, including the following comments from a document entitled "Digital Service Standard - Feedback and Actions Register":

The CEO has highlighted a preference to move away from open source to open standards.

and

Chris has highlighted a preference to move away from open source to open standards.

Rather than tie up yet more Agency time in FOI requests, I thought it would be more efficient to contact you directly, since the information uncovered so far points to you. Are you able to shed light on why this change in DSS v2.0? Could DTA give administrative access to any relevant policy document, feedback, or internal correspondence relevant to my inquiry - and/or could you provide your personal recollection or reflections on this topic?

Yours sincerely,

Fraser Tweedale



Chris Fechner <Chris.Fechner@dta.gov.au>
to Fraser Tweedale, cc Office of the CEO ▾

Jul 17 (10 days ago)

Inbox



Reply to all

Actions ▾

OFFICIAL

Dear Fraser,

Thank you for your email and for the constructive way you have engaged with the DTA on this matter.

The removal of the specific criterion "*Make source code open*" from the Digital Service Standard was not intended to signal opposition to open-source software. During the development of DSS v2, there was a deliberate effort to make the Standard more principles-based and applicable across a wider range of digital services and agency contexts.

My view has always been that the Australian Government operates in a mixed technology environment, comprising both open-source and proprietary solutions. I do not oppose open source and recognise the significant value it can provide. However, I continue to be particularly conscious of the importance of interoperability across government, and of the role that open standards play in enabling that interoperability regardless of the underlying technology choices made by agencies.

The references to open standards in the feedback register reflected this focus. Standards such as those developed by W3C, along with JSON, OData, OAuth, SAML and WCAG, help ensure systems can exchange information, integrate effectively and remain accessible and portable over time. The change was not a move away from open source, but rather an emphasis on the standards that allow diverse systems and technologies to work together across the Australian Government.

Where government entities choose to use or develop open-source software, we continue to support open and transparent development practices, within appropriate security, privacy and other legislative requirements.

I appreciate your interest in the evolution of the Digital Service Standard and hope this context is helpful.

Kind regards,

Chris

Chris Fechner

Chief Executive Officer | Head of the [Digital Profession](#)

Digital Transformation Agency

chris.fechner@dta.gov.au | dta.gov.au

Ngunnawal Country | 11 Moore Street, Canberra ACT, 2601

Executive Assistant: Amy Vizy

amy.vizy@dta.gov.au | oceo@dta.gov.au

Ph: +61 73 798 561

The DTA acknowledges Traditional Owners of Country throughout Australia and recognises their continuing connection to lands, waters and communities. We pay our respect to Aboriginal and Torres Strait Islander cultures; and to Elders both past and present.

ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA

2025/4916

FRASER TWEEDALE

Applicant

CEO, SERVICES AUSTRALIA

Respondent

ANNEXURE FT-8

The following is the annexure marked **FT-8** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains the report entitled 'Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software' (the **Shifting the Balance report**), which was published in October 2023 by the Australian Cyber Security Centre (ACSC) - a department of the Australian Signals Directorate (ASD) - jointly with the apex cyber security agencies of USA, Canada, UK, Germany, Netherlands, Norway, New Zealand, Korea, Israel, Japan, Singapore, Czech Republic, and the Organization of American States (OAS).

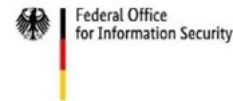
.....
Daniel Davison
Solicitor



SHIFTING THE BALANCE OF CYBERSECURITY RISK:

PRINCIPLES AND APPROACHES FOR
SECURE BY DESIGN SOFTWARE





Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**



National Cyber Security Centre
Ministry of Justice and Security



National Cyber
Security Centre
a part of GCHQ



CSIRT Americas
Network



NSM
NORWEGIAN NATIONAL
CYBER SECURITY CENTRE



National Cyber
and Information
Security Agency



Contents

Overview: Vulnerable By Design.....	4
What's New	6
How To Use This Document.....	7
Secure by Design	8
Secure by Default.....	9
Recommendations for Software Manufacturers	9
Software Product Security Principles.....	10
Principle 1: Take Ownership of Customer Security Outcomes.....	11
<i>Explanation</i>	11
<i>Demonstrating This Principle</i>	14
Principle 2: Embrace Radical Transparency and Accountability	20
<i>Explanation</i>	20
<i>Demonstrating This Principle</i>	21
Principle 3: Lead from the Top	26
<i>Explanation</i>	26
<i>Demonstrating This Principle</i>	27
Secure by Design Tactics	28
Secure by Default Tactics.....	30
Hardening vs Loosening Guides.....	32
Recommendations for Customers.....	33
Disclaimer	34
Resources	35
References	36

OVERVIEW: VULNERABLE BY DESIGN

Technology is integrated into nearly every facet of daily life, as internet-facing systems increasingly connect us to critical systems that directly impact our economic prosperity, livelihoods, and even health, ranging from personal identity management to medical care. One example of the disadvantage of such conveniences are the global cyber breaches resulting in hospitals canceling surgeries and diverting patient care. Insecure technology and vulnerabilities in critical systems may invite malicious cyber intrusions, leading to potential safety¹ risks.

As a result, it is crucial for software manufacturers to make secure by design and secure by default the focal points of product design and development processes. Some vendors have made great strides driving the industry forward in software assurance, while others continue to lag behind. The authoring organizations strongly encourage every technology manufacturer to build their products based on reducing the burden of cybersecurity on customers, including preventing them from having to constantly perform monitoring, routine updates, and damage control on their systems to mitigate cyber intrusions. We also urge the software manufacturers to build their products in a way that facilitates automation of configuration, monitoring, and routine updates. Manufacturers are encouraged to take ownership of improving the security outcomes of their customers. Historically, software manufacturers have relied on fixing vulnerabilities found after the customers have deployed the products, requiring the customers to apply those patches at their own expense. Only by incorporating secure by design practices will we break the vicious cycle of constantly creating and applying fixes. **Note:** The term “secure by design” encompasses both secure by design and secure by default.

To accomplish this high standard of software security, the authoring organizations encourage manufacturers to prioritize the integration of product security as a critical prerequisite to features and speed to market. Over time, engineering teams will be able to establish a new steady-state rhythm where security is truly designed-in and takes less effort to maintain.

Reflecting this perspective, the European Union reinforces the importance of product security in the [Cyber Resilience Act](#), emphasizing that manufacturers should implement security throughout a product’s life-cycle in order to prevent manufacturers from introducing vulnerable products into the market.

¹ The authoring organizations recognize that the term “safety” has multiple meanings depending on the context. For the purposes of this guide, “safety” will refer to raising technology security standards to protect customers from malicious cyber activity.

To create a future where technology and associated products are safer for customers, the authoring organizations urge manufacturers to revamp their design and development programs to only permit the shipping of products secure by design and default. Well before development, products that are secure by design are conceptualized with the security of customers as a core business goal, not just a technical feature. Secure by design products start with that goal before development starts. Existing products can evolve to a secure by design state over multiple iterations. Secure by default products are those that are secure to use “out of the box” with little to no configuration changes necessary, and security features available without additional cost. Together, these two philosophies move much of the burden of staying secure to manufacturers and reduce the chances that customers will fall victim to security incidents resulting from misconfigurations, insufficiently fast customer patching, or many other common issues.

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI) and the following international partners² provide the recommendations in this guide as a roadmap for software manufacturers to ensure security of their products:

- » Australian Cyber Security Centre (ACSC)
- » Canadian Centre for Cyber Security (CCCS)
- » United Kingdom’s National Cyber Security Centre (NCSC-UK)
- » Germany’s Federal Office for Information Security (BSI)
- » Netherlands’ National Cyber Security Centre (NCSC-NL)
- » Norway’s National Cyber Security Center (NCSC-NO)
- » Computer Emergency Response Team New Zealand (CERT NZ) and New Zealand’s National Cyber Security Centre (NCSC-NZ)
- » Korea Internet & Security Agency (KISA)
- » Israel’s National Cyber Directorate (INCD)
- » Japan’s National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
- » OAS/CICTE Network of Government Cyber Incident Response Teams (CSIRT) Americas
- » Cyber Security Agency of Singapore (CSA)
- » Czech Republic’s National Cyber and Information Security Agency (NÚKIB)

The authoring organizations recognize the contributions by many private sector partners in advancing security by design and security by default. This product is intended to progress an international conversation about key priorities, investments, and decisions necessary to achieve a future where technology is safe, secure, and resilient by design and default. To that end, the authoring organizations seek feedback on this product from interested parties and intend to convene a series of listening sessions to further refine, specify, and advance our guidance to achieve our shared goals.

For more information on the importance of product safety, see CISA’s article, [The Cost of Unsafe Technology and What We Can Do About It](#).

² Hereafter referred to as the “authoring organizations.”

WHAT'S NEW

The initial publication of this report generated a significant amount of conversation within the software industry. Daily news of organizations and individuals being compromised highlights the need for more conversation regarding how to address chronic and systemic problems in software products.

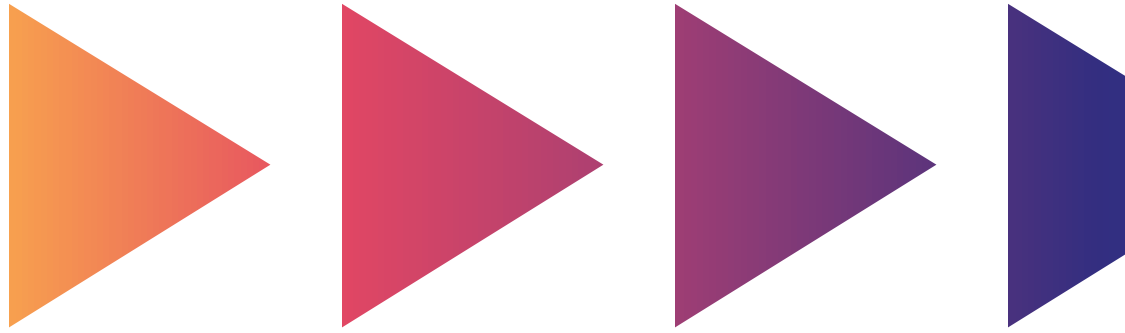
After the release in April 2023, the authoring organizations (henceforth referred to as “we” and “our”) received thoughtful feedback from hundreds of individuals, companies, and trade associations. The most common request in the feedback was to provide more detail on the three principles as they apply to both software manufacturers and their customers. In this document, we expand on the original report and touch on other themes such as manufacturer and customer size, customer maturity, and the scope of the principles.

Software is everywhere and no single report will be able to adequately cover the entire range of software systems, development of software products, customer deployment and maintenance, and integration with other systems. For guidance below that does not clearly map to a particular environment, we look forward to hearing from the community how the practices described in this paper led to particular security improvements.

This report applies to manufacturers of artificial intelligence (AI) software systems and models as well. While they might differ from traditional forms of software, fundamental security practices still apply to AI systems and models. Some secure by design practices may need modification to account for AI-specific considerations, but the three overarching secure by design principles apply to all AI systems.

We recognize that transforming a software development lifecycle (SDLC) to align with these secure by design principles is not a simple task and may take time. Further, smaller software manufacturers may struggle to implement many of these suggestions. We believe that the software industry needs to make widely available the tools and procedures that make products safer. As more people and organizations focus their attention on software security improvements, we believe there is room for innovations that will narrow the gap between larger and smaller software manufacturers to the benefit of all customers.

This update to the original secure by design report is part of our commitment to build partnerships with the many interconnected stakeholder communities that underpin our technological ecosystem. It is the result of feedback from many parts of that ecosystem, and we will continue to listen and learn from perspectives. Although there are many challenges ahead, we are incredibly optimistic as we learn more about people and organizations that have already adopted a secure by design philosophy, often with success.



HOW TO USE THIS DOCUMENT

We urge software manufacturers to adhere to the principles within this document. Software manufacturers can demonstrate their commitment by publicly documenting their actions taken, in line with the steps listed below. We encourage software manufacturers to find tactics that meet the spirit of these principles and to create artifacts that will build a compelling case to even skeptical current and potential customers that they are embodying the secure by design philosophy.

In addition to actions software manufacturers should take, customers can also leverage this document. Companies buying software should ask hard questions of their vendors, drawing inspiration from the examples of adhering to the principles listed in this document. In doing so, customers can help to shift the market towards products that are more secure by design. An example of questions customers can ask of vendors is given in [CISA's Guidance for K-12 Technology Acquisitions](#).

We encourage enterprise customers to incorporate these practices into procurement processes, vendor due diligence assessments, enterprise risk acceptance decisions, and other steps taken when evaluating vendors. Customers should also push their vendors to publicly document the secure by design actions each vendor takes. Collectively, this can create a strong demand signal for security, which can encourage and enable software manufacturers to take steps towards greater security. In other words, just as we seek to create a pervasive secure by design philosophy within software manufacturers, we need to create a "secure by demand" culture with their customers.

Secure by Design

“Secure by design” means that technology products are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure. Software manufacturers should perform a risk assessment to identify and enumerate prevalent cyber threats to critical systems, and then include protections in product blueprints that account for the evolving cyber threat landscape.

Secure information technology (IT) development practices and multiple layers of defense—known as defense-in-depth—are also recommended to prevent malicious actors from compromising systems or obtaining unauthorized access to sensitive data. The authoring organizations further recommend manufacturers use a tailored threat model during the product development stage to address all potential threats to a system and account for each system’s deployment process.

The authoring organizations urge manufacturers to take a holistic security approach for their products and platforms. Secure by design development requires the strategic investment of dedicated resources by software manufacturers at each layer of the product design and development process that cannot be “bolted on” later. It requires strong leadership by the manufacturer’s top business executives to make security a business priority, not just a technical feature. This collaboration between business leaders and technical teams extends from the preliminary stages of design and development, through customer deployment and maintenance. Manufacturers are encouraged to make hard tradeoffs and investments, including those that will be “invisible” to the customers (e.g., migrating to programming languages that eliminate widespread vulnerabilities). They should prioritize the features, mechanisms, and implementation of tools that protect customers rather than product features that seem appealing but enlarge the attack surface.

There is no single solution to end the persistent threat of malicious cyber actors exploiting technology vulnerabilities, and products that are “secure by design” will continue to suffer vulnerabilities; however, a large set of vulnerabilities are due to a relatively small subset of root causes. Manufacturers should develop written roadmaps to align their existing product portfolios with more secure by design practices, ensuring to only deviate in exceptional situations.

The authoring organizations acknowledge that taking ownership of the security outcomes for customers and ensuring this level of customer security may increase development costs. However, investing in secure by design practices while developing innovative technology products and maintaining existing ones can substantially improve the security posture of customers and reduce the likelihood of compromise. Secure by design principles not only strengthen the security posture for customers and brand reputation for developers but the practice also lowers maintenance and patching costs for manufacturers in the long term.

The Recommendations for Software Manufacturers section listed below provides a list of product development practices and policies for manufacturers to consider.

Secure by Default

“Secure by default” means products are resilient against prevalent exploitation techniques out of the box without added charge. These products protect against the most prevalent threats and vulnerabilities without end-users having to take additional steps to secure them. Secure by default products are designed to make customers acutely aware that when they deviate from safe defaults, they are increasing the likelihood of compromise unless they implement additional compensatory controls. Secure by default is a form of secure by design.

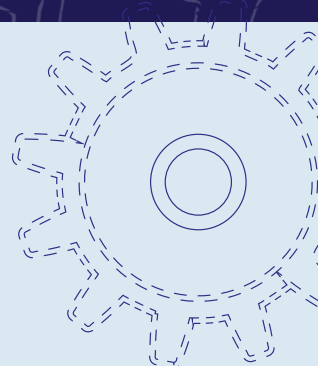
- » A secure configuration should be the default baseline. Secure by default products automatically enable the most important security controls needed to protect enterprises from malicious cyber actors, as well as supply the ability to use and further configure security controls at no additional cost.
- » The complexity of security configuration should not be a customer problem. Organizational IT staff are frequently overloaded with security and operational responsibilities, thus resulting in limited time to understand and implement the security implications and mitigations required for a robust cybersecurity posture. Manufacturers can aid their customers by optimizing secure product configuration—securing the “default path”—ensuring their products are manufactured, distributed, and used securely in accordance with “secure by default” standards.

Manufacturers of products that are “secure by default” do not charge extra for implementing added security configurations. Instead, they include them in the base product like seatbelts are included in all new cars.

Security should not be a luxury option, but should be considered a right customers receive without negotiating or paying more.

RECOMMENDATIONS FOR SOFTWARE MANUFACTURERS

This joint guide provides recommendations to manufacturers for developing a written roadmap to implement and ensure IT security. The authoring organizations recommend software manufacturers implement the strategies outlined in the sections below to take ownership of the security outcomes of their customers through secure by design and default principles.



SOFTWARE PRODUCT SECURITY PRINCIPLES

Software manufacturers are encouraged to adopt a strategic focus that prioritizes software security. The authoring organizations developed the following three core principles to guide software manufacturers in building software security into their design processes prior to development, configuration, and shipment of their products.

1

Take ownership of customer security outcomes and evolve products accordingly. The burden of security should not fall solely on the customer.

2

Embrace radical transparency and accountability.

Software manufacturers should pride themselves in delivering safe and secure products, as well as differentiating themselves from the rest of the manufacturer community based on their ability to do so. This may include sharing information they learn from their customer deployments, such as the uptake of strong authentication mechanisms by default. It also includes a strong commitment to ensure vulnerability advisories and associated common vulnerability and exposure (CVE) records are complete and accurate. However, beware of the temptation to count CVEs as a negative metric, since such numbers are also a sign of a healthy code analysis and testing community.

3

Build organizational structure and leadership to achieve these goals.

While technical subject matter expertise is critical to product security, senior executives are the primary decision makers for implementing change in an organization. Executives need to prioritize security as a critical element of product development across the organization, and in partnership with customers.

To enable these three principles, manufacturers should consider several operational tactics to evolve their development processes.

Convene routine meetings with company executive leadership to drive the importance of secure by design and secure by default within the organization. Policies and procedures should be established to reward production teams that develop products adhering to these principles, which could include awards for implementing outstanding software security practices or incentives for job ladders and promotion criteria.

Operate around the importance of software security to business success. For example, consider assigning a “software security leader” or a “software security team” that upholds business and IT practices that directly link software security standards and manufacturer accountability. Manufacturers should ensure they have robust, independent product security assessment and evaluation programs for their products.

Use a tailored threat model during resource allocation and development to prioritize the most critical and high-impact features. Threat models consider a product's specific use-case and enable development teams to fortify products. Finally, senior leadership should hold teams accountable for delivering secure products as a key element of product excellence and quality.

As part of the October 2023 update to this guidance, these three principles are expanded upon through the following explanations, demonstrations, and evidence.

PRINCIPLE 1: Take Ownership of Customer Security Outcomes

EXPLANATION

Modern best practices dictate that software manufacturers invest in product security efforts that include **application hardening**, **application features**, and application **default settings**.

Software manufacturers need to implement **application hardening** by using processes and technologies that raise the cost for a malicious actor wishing to compromise applications. Application hardening protocols and procedures help products resist attacks by intelligent malicious actors. Terms like hardening, product security, and resilience are all closely related to product quality. The idea is that security must be “baked in,” and not “bolted on.” [1] By baking in security, software manufacturers can not only increase their customers’ security but also increase their products’ quality. Sample tactics include ensuring user input is validated and sanitized, and isn’t entered directly into code (i.e., by using parameterized queries instead), using a memory safe programming language, rigorous software development life cycle (SDLC) management, and using hardware-backed cryptographic key management.

Applications need to support **application features** that relate to cybersecurity. Sometimes called “capabilities,” these features extend the functionality of a product or service in ways that help maintain or increase the security posture of a customer.

Sample security-related features include supporting transport layer security (TLS) for all network connections, single sign on (SSO) support, multi-factor authentication (MFA) support, security event audit logging, role-based access control (RBAC), and attribute-based access control (ABAC).

Some of these product features are configurable allowing customers to more easily integrate the product into their existing environments and workflows. Those configurations mean applications must have **default settings** set until customers configure them. Those default settings need to be set securely “out of the box” so that customers expend fewer resources to make their stack of technology products more secure.

Each of these elements – application hardening, application security features, and application default settings – plays a role in the security of the application, and the resulting security posture of the customer. Software manufacturers should think about each of these elements and how they relate to each other. Manufacturers should think about more than just their investments to incorporate these elements into their products. Manufacturers should take it a step further and consider how those elements change the real-world security posture of their customers, for better or for worse.

Manufacturers should take ownership of their customers’ security outcomes rather than measuring themselves solely on their efforts and investments. The responsibility should be placed upstream, with the manufacturers, where it has the greatest likelihood of reducing the chances of compromise.

Unfortunately, that’s not the case today. Too many manufacturers place the burden of security on the customer rather than investing in comprehensive **application hardening**. For example, when the manufacturer patches one vulnerability, we often see similar vulnerabilities exposed because they addressed the symptom rather than the root cause of that defect. The product might implement different mitigations in various parts of the code base for the same class of vulnerability. As a case in point, after the manufacturer fixed one input sanitization vulnerability, researchers or attackers found code paths that did not benefit from the improved input sanitization. The manufacturer applied fixes one at a time rather than unifying the codebase to eliminate that class of vulnerability across the entire application.

Application features can create both benefits and risk for customers. Features that allow integration points with many external systems and versions can greatly increase the value of a product. And yet supporting features without a retirement plan, like a networking protocol, can leave customers vulnerable if they lack an understanding of the implications of ongoing use of that feature. For example, some products continue to use networking protocols that have their origins in the 1990s or 2000s and are now known to be unsafe. There are numerous factors that can slow how fast customers upgrade and deploy modern security measures. They may use products that integrate with the rest of the organization’s network, but lack modern security measures, preventing the IT team from modernizing. Still, software manufacturers can factor these patterns into their planning process to encourage customers to stay current.

Application default settings are an added area of potential risk for customers. Manufacturers often choose certain default settings, making it easier for customers to use the application features they want. The downside is that this practice increases the attack surface for customers who may not need certain features and protocols that are enabled by default. Additionally, many security controls are toggled off by default or require customers to take time to configure their settings to increase security. Explicit threat modeling is a tactic that may help inform the decision of which features should be on by default or which settings are needed to be secure by default. Another tactic is to investigate ways to make features more discoverable for the administrator.

Some manufacturers ship products with defaults that can create risk for some or all their customers. Rather than set safer defaults, they often opt to produce a **hardening guide** that customers must implement at their own expense. Hardening guides suffer from several common problems. Some hardening guides are hard to find and are not well supported. Others are complex to implement, occasionally requiring software development to write an extension module. Still, others assume the reader has extensive cybersecurity experience to understand the ways in which various settings change the attack surface. Practitioners who have an incomplete understanding of the ways in which attackers work may fail to properly implement hardening guide instructions, especially if the instructions do not make the trade offs clear. Further, not all hardening guides are written by engineers who are intimately familiar with attacker tactics and economics, causing them to create hardening guides that are ineffective even if faithfully implemented. Millions of customers are taking on the responsibility to harden multiple instances of software or systems, often in resource-constrained environments. Relying on hardening guides simply doesn't scale.

An application's settings should be continuously evaluated whether the settings were the default or set by the customer, against the manufacturer's current understanding of the threat landscape. Applications should be made with clear indicators about the potential risks that may result from those settings and should make those indicators known. Just like a modern car has an indicator about seatbelts and expresses that indicator by sounding an alert if you try to drive without buckling up, software should express indicators about the state of security of a system. If an application is configured to not require MFA for administrator accounts, it should make the administrators regularly aware that they and their entire organization are in danger if they do not configure MFA. Additionally, if an application is configured to support older protocols that are now known to implement weak cryptography, it should regularly make it clear to the administrators that the organization is in danger and provide resources to resolve the situation. We urge manufacturers to implement routine nudges that are built into the product rather than relying on administrators to have the time, expertise, and awareness to interpret hardening guides. Opportunities clearly exist for innovation to balance security and usability considerations.

Each of the above elements creates an untenable situation in which customers need to research, fund, purchase, staff, deploy, and monitor additional **security products** to reduce the chance of compromise. Small and medium sized organizations (SMOs) are generally unable to facilitate these options. They face scarcity in expertise, funding, and time which taxes bandwidth and function, forcing security to a lower priority, and, in the aggregate, exacerbates collective risk. Conversely, security investments by the relative few manufacturers will scale. A common phrase that summarizes the problem is that the software industry needs more secure products, not more security products. Software manufacturers should lead that transformation.



The software industry needs more secure products, not more security products. Software manufacturers should lead that transformation.

Today, we sometimes read comments from manufacturers explaining that a customer was compromised due to not enabling a particular security feature or following specific hardening guidance. Instead, after a compromise, manufacturers should explain whether a particular security feature or specific hardening guidance would have prevented the compromise and consider making it the default at no charge. In those cases where the product itself was not sufficiently hardened in the design and implementation phases, the manufacturer should explain how they are working to eliminate that class of vulnerability from their product lines.

Software manufacturers have a responsibility to ensure that their products are designed and developed with security as a top priority. To that end, they should **objectively measure the results** of their efforts in the field. We call on manufacturers to not just focus on their internal efforts, but to objectively measure and regularly report the results and effectiveness of a product's security efforts and configurations, and to build a feedback loop that creates changes in the SDLC that lead to measurable improvements in customer safety and more secure products. Reporting should include anonymized data that the academic and security research community could use to track high-level trends and measure progress ecosystem wide.



DEMONSTRATING THIS PRINCIPLE

Software manufacturers and online services should find ways to demonstrate successes in implementing this principle. They should seek to provide evidence in the form of artifacts for outsiders to examine. No single artifact by itself will prove that a manufacturer is implementing a robust secure by design program, but by providing various artifacts they will build a case of the manufacturer's commitment to developing secure products. This approach is in the spirit of "show, rather than tell."

To demonstrate this principle, software manufacturers should consider steps such as those in the following list. The authoring organizations recognize that few software manufacturers will be able to immediately implement these practices and produce corresponding artifacts at the start of their secure by design journey. Further, software manufacturers will need to prioritize this list depending on how the customers deploy the product in the field to achieve the largest security benefits.

SECURE BY DEFAULT PRACTICES



1. Eliminate default passwords. Default passwords continue to be implicated as the cause of many attacks every year. Making a commitment to eliminate this chronic problem will deny easy access to attackers. Similarly, manufacturers should consider what password practices should be implemented, such as minimum password length and disallowing known breached passwords.

2. Conduct field tests. As technology continues to evolve and become more complex, it is increasingly important for software manufacturers to conduct security-centric user testing to understand their products' security posture in the field. Similar to how user research informs software development requirements, software manufacturers should also conduct security-focused user research to understand where the security user experience (UX) falls short. By observing how customers deploy and use their products in real-world environments, software manufacturers can gain valuable insights into the usability and effectiveness of their security features and controls. These insights can help identify areas for improvement and refine their products to better meet the security needs of customers. For example, field tests might suggest changes in UX flow, defaults, alerting, and monitoring. Field tests may also show where past improvements in the product's design reduce the velocity of security patches, reduce configuration errors, and minimize attack surface.

Manufacturers should consider the following:

- Do customers correctly implement the hardening guide?

- Do the product's existing security features perform as expected in the field?
- Do those features actually resist real-world attacks?
- Which features would better reduce the likelihood of compromise?

Note: To gain deeper insights into these elements, software manufacturers may wish to partner with customers to conduct red team exercises to see how the product resists attacks. These field tests might take place at the customer's physical site, virtually, or via telemetry from the application in a privacy-preserving manner.

3. Reduce hardening guide size. Manufacturers can improve customers' security postures by streamlining or even eliminating product hardening guides and focusing on the most critical security measures that customers should prioritize when deploying their products. Rather than overwhelming customers with a laundry list of security measures, manufacturers should identify the top security risks that their products are susceptible to and provide clear and concise guidance on how to mitigate these risks. In addition, manufacturers should provide customers with tools and automation that simplify the process of implementing security controls, such as scripts that can easily be deployed in their environment. These tools should additionally be able to verify and clearly show the changes made from the original baseline. By streamlining hardening guides and providing customers with easy-to-use tools and automation, manufacturers can reduce the burden on their customers and help ensure that their products are deployed in a secure manner. One tactic would be to consider implementing the Pareto principle to reduce the number of steps for the common use cases (the 80%), and then providing contextual guidance and tooling for less common scenarios (the 20%). In this way, software manufacturers will be making

the simple things simple, and the hard things possible. Field testing will be a powerful tool in measuring how long it takes customers to discover, understand, and implement hardening guides. Manufacturers should consider how the product could nudge administrators to take action within the product itself rather than relying on them to implement tasks from a hardening guide.

4. Actively discourage use of unsafe legacy features.

Prioritize security through clear upgrade paths over backwards compatibility. Publish blog posts showing the adoption of safer features and protocols, and deprecate unsafe features by announcement, possibly from within the product itself. A significant number of customers have demonstrated that they will not keep their systems current with modern network, identity, and other critical security features. In some cases, customers fear existing functionality will break with an upgrade. By making upgrades as seamless as possible, customers will likely upgrade and get security fixes more often and quickly. Software manufacturers should aggressively nudge customers along upgrade paths that reduce customer risk.

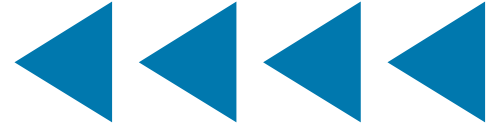
5. Implement attention grabbing alerts.

Similar to seat belt chimes in cars that continuously make noise when seat belts are not fastened, manufacturers should implement timely and repeated alerts when users or admins are in truly unsafe states, warning administrators that they are using deprecated protocols in their environments and suggest upgrade paths. Implement timely and repeated alerting when users or admins, or the application configuration, are in an unsafe state. Make the unsafe mode clear to the administrators on a regular basis. An additional feature could require a super administrator to acknowledge the lack of MFA on their account upon each login, or even disable certain key features until they enable MFA. There is room to innovate to achieve these goals while not creating alert fatigue.

6. Create secure configuration templates.

These templates can pre-set certain configurations to safe settings based on an organization's risk appetite. While it might be overly simplistic to have low/medium/high security templates, that example illustrates how many settings could be updated to manage risk for the organization. Templates can be supported by hardening guides on the risks the manufacturer has identified.

SECURE PRODUCT DEVELOPMENT PRACTICES



1. **Document conformance to a secure SDLC framework.** Secure SDLC frameworks provide objectives and examples across people, processes, and technologies. Consider publishing a detailed description of which secure SDLC framework controls have been implemented and describe any alternate controls which have been used. Within the US, consider using the NIST Secure Software Development Framework (SSDF). While not a checklist, the SSDF “describes a set of fundamental, sound practices for secure software development.”
2. **Document Cybersecurity Performance Goals (CPG) or equivalent conformance.** When an organization attests that they conform to the NIST SSDF standard, they are asserting that their SDLC is informed by well-understood best practices. However, it is not sufficient for them to only have a robust SDLC. They also need to protect their own enterprise and development environments from malicious actors who would seek to manipulate the security properties of the product while it is still in development. This is not a theoretical class of attack, but one that has been carried out with adverse effects to customers, and by extension national security. Organizations should consider publishing details on the organization’s conformance to the CISA CPGs, the NIST Cybersecurity Framework (CSF), or other cybersecurity program frameworks.
3. **Vulnerability management.** Some manufacturers have a vulnerability management program that focuses on patching vulnerabilities discovered internally or externally, and little more. More mature programs incorporate extensive data-driven analysis of vulnerabilities and their root causes, taking steps to systemically eliminate entire classes of vulnerability³. They implement formal programs around setting quality planning, quality control, quality improvement, and quality measurement. They view defect management as a business matter, not merely a security matter. These programs are not dissimilar in some ways to quality and safety programs in other industries.
4. **Responsibly use open source software.** When open source software is used, be responsible by vetting open source packages, fostering code contributions back to dependencies, and helping sustain the development and maintenance of critical components. For reference, Japan’s Ministry of Economy, Trade, and Industry (METI) has published [“Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security.”](#)
5. **Provide secure defaults for developers.** Make the default route during software development the secure one by providing safe building blocks for developers. For example, given the prevalence of SQL injection vulnerabilities causing real-world harm, ensure that developers use a well-maintained library to prevent that class of vulnerability. Also known as “paved roads” or “well-lit paths,” this practice ensures both speed and security, and reduces human error.
6. **Foster a software developer workforce that understands security.** Ensure that your software developers understand security by training them on secure coding best practices. Further, help transform the broader workforce by updating hiring practices to evaluate security knowledge and working with universities, community colleges, bootcamps, and other educators to weave security into computer science and software development curriculums.

³ NIST SSDF, PO 1.2, Example 2: “Define policies that specify the security requirements for the organization’s software, and verify compliance at key points in the SDLC (e.g., classes of software flaws verified by gates, responses to vulnerabilities discovered in released software).”

7. **Test security incident event management (SIEM) and security orchestration, automation, and response (SOAR) integration.** In addition to conducting field tests, work jointly with popular SIEM and SOAR providers in conjunction with select customers to understand how incident response teams use logs to investigate suspected or actual security incidents. Few software developers have experience responding to an incident and may create log entries that don't help responders as much as they would expect. By working both with SIEM and SOAR technologies and real incident response professionals, the development team can create logs that tell the correct and complete story, saving time and reducing uncertainty during an incident.
8. **Align with Zero Trust Architecture (ZTA).** Align product deployment guides with, for example, the NIST ZTA models and the [CISA Zero Trust Maturity Model](#). Encourage customers to incorporate these principles in their environments.



PRO-SECURITY BUSINESS PRACTICES



1. Provide logging at no additional charge.

Cloud services should commit to generating and storing security-related logs at no additional charge. On-premises products should likewise generate security-related logs at no additional charge. Further, the product should log security events by default since many customers may not understand their value until after an incident. These tactics may require a thorough review of what security events should be logged to provide cybersecurity state awareness, how a customer may configure logging, for what time period logs are retained, how log integrity and storage are protected, and how logs can be analyzed. In some cases, the review may suggest the need for a refactoring of the application's log management architecture to help make them actionable and at a cost that works for the manufacturer. Working with incident response (IR) experts can increase the chances that the logs will be useful to investigators in the field. See the section on SIEMs.

- ## 2. Eliminate hidden taxes.
- Publish a commitment to never charge for security or privacy features or integrations. For example, within the larger scope of identity and access management (IAM), there are services called single sign-on (SSO) services. Some manufacturers charge more to connect their system to a SSO service (sometimes referred to as an identity provider). This "SSO tax" means that good identity and access management is out of reach for many SMOs, preventing them from achieving a strong security posture. Some services charge more to enable MFA for users. **Security should not be priced as a luxury good but considered a customer right.** Some manufacturers have argued that few customers request these features, and they cost more to maintain. These

arguments ignore the fact that few customers will call to complain or bargain, not all customers actually understand what the benefits of these features are, and that all features cost something to maintain. Yet we don't see many manufacturers charging extra for availability or data integrity. The costs to support those key attributes are built into the price all customers pay, much like the costs to include seatbelts, collapsible steering columns, and airbags that save lives in accidents.

- ## 3. Embrace open standards.
- Implement open standards, especially around common network and identity protocols. Avoid proprietary protocols when open standards are available.
- ## 4. Provide upgrade tooling.
- Many customers are reluctant to adopt the latest version of the product, including deploying newer and more secure features like secure network connections. Software manufacturers can increase customer adoption of new upgrades by providing tooling to help reduce uncertainty and risk. Offer free licenses for customers to test upgrades and patches in a test environment as a way to motivate customers.



PRINCIPLE 2: Embrace Radical Transparency and Accountability

EXPLANATION

Software manufacturers should pride themselves in delivering safe and secure products, as well as differentiating themselves from the rest of the manufacturer community based on their ability to do so.

Let's address a common concern about transparency. When practitioners discuss radical transparency, there is a tendency for the conversation to get bogged down in a concern that they are providing a "roadmap for attackers." However, the overwhelming evidence is that attackers are doing just fine without such roadmaps, and such concerns should take a back seat to transparency that benefits direct customers, indirect customers, supply chains, and the entire software industry.

Transparency helps the industry establish conventions—in other words, what "good" looks like. It helps those conventions change over time in response to customer needs, changes in threat actor tactics or economics, or technology evolution. Transparency helps manufacturers with fewer resources learn from those with more mature and capable resources. Conversations about information sharing should expand beyond real-time threat indicators, to include the elements below.

Transparency forces decisions around security to be made early in the development process, and to be a continuous activity of business leaders as well as engineers and

security professionals. Transparency builds accountability into the product.

A note on the choice of the adjective “radical” in front of “transparency.” Today, it is uncommon for software manufacturers to publish detailed information about how they develop and maintain software and how they mature their programs using data over time. In the software industry, few manufacturers offer guided tours of how they design their software. There are few opportunities for software manufacturers to see how peer organizations structure their SDLC programs, and how those programs hold up in the customer environments against real attackers. The collective industry would benefit from more information sharing on topics such as strategies to measure the cost of security defects and to eliminate classes of vulnerability. As a result of these common practices, every software manufacturer must learn how to deal with product security on their own. Perhaps by not placing a luxury tax on security features, safety and security therefore become a cost center rather than a profit center, and companies would benefit by lightening the load through collaboration and transparency.

We want to focus on the tactics that will materially accelerate the evolution of the software industry. We can no longer afford to make opportunistic, incremental improvements. If we are to collectively overcome the threats posed by intelligent and adaptive adversaries, we must embrace levels of transparency that will feel uncomfortable today, but that will drive the industry forward. There are manufacturers today who embody some of these secure by design principles. As William Gibson said, “the future is already here, it’s just not very evenly distributed.” **Radical transparency will help distribute that information and benefit the defenders more than our adversaries.**

Transparency can do more than help peer organizations mature their SDLCs. Prospective customers and investors can learn more about the investments and tradeoffs manufacturers have made, and the security posture those investments have created for customers. Manufacturers who embrace radical transparency will give customers information to help them make purchasing decisions not just on price and features, but on security as well.

As hard as organizations work to secure their supply chain and their SDLC, companies have had their builds processes compromised in the recent past. Embracing radical transparency should lead to public disclosure of the attack as well as the improvements the company made to prevent and detect future attacks. That form of information sharing will help other organizations learn without having to suffer the same fate.

DEMONSTRATING THIS PRINCIPLE

To demonstrate this principle, software manufacturers should take steps including the following:

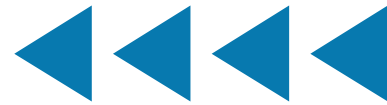
SECURE BY DEFAULT PRACTICES



1. **Publish aggregate security relevant statistics and trends.** Example topics include MFA adoption by customers and administrators and use of unsafe legacy protocols.
2. **Publish patching statistics.** Detail what percent of customers are on the latest version of the product, and what you are doing to make updates easier and more reliable.
3. **Publish data on unused privileges.** Publish aggregate information on excessive permissions across your customer base as well as the nudges and other changes to the product you are making to reduce the customers' attack surfaces. These unused privileges are likely to be good candidates for administrator alerts, like seatbelt chimes.



SECURE PRODUCT DEVELOPMENT PRACTICES



1. Establish internal security controls.

Many companies have seen the benefits of moving their data to cloud providers. Now those cloud providers become the target of attackers. Software as a Service (SaaS) providers should publish statistics of their internal controls. For example, SaaS providers should publish statistics on their internal deployment of [phishing-resistant MFA](#), like Fast Identity Online (FIDO) authentication. Ideally, they should be able to say that no staff member can access customer or other sensitive data without authenticating via phishing-resistant MFA.

2. Publish high-level threat models.

Secure by design products start with written threat models that describe what the creators are trying to protect and from whom. Effective threat models are informed by the way intrusions happen in the wild, and should cover both the enterprise and development environments, as well as the way the software manufacturers intend for it to be used in customer environments.

3. Publish detailed secure SDLC self-attestations.

Manufacturers following NIST SSDF, or other similar frameworks are actively working towards a mature software development lifecycle. Publishing a self-attestation of which controls the manufacturer has enacted, and for which products, would demonstrate a commitment to adhering to these best practices and provide an increased level of confidence to their customers. Other certification schemes include the Israel Cyber Supply Chain Methodology, for instance.

4. Embrace vulnerability transparency.

Publish a commitment that will ensure that identified product vulnerabilities

will be published as CVE entries that are correct and complete. That's especially true for the common weakness enumeration field that identifies the root cause of the vulnerabilities. The more correct and complete the public CVE database is, the more the industry can track how products are becoming more secure, and which classes of vulnerabilities are most prevalent. However, beware of the temptation to count CVEs as a negative metric, since such numbers are also a sign of a healthy code analysis and testing community. As manufacturers implement a secure by design philosophy, it's possible that at first their raw CVE count will go up due to more comprehensive discovery and remediation of vulnerabilities in existing code. Manufacturers should publish analysis of past vulnerabilities, including any patterns and measures that were taken to address the entire class of vulnerabilities. For example, if a large percentage of a company's CVEs were related to cross-site scripting (XSS), documenting the root cause analysis, response (such as shifting to web template frameworks that prevent XSS), and results would signal to customers that they will not be victimized by a class of vulnerability for which mitigations have been understood for decades.

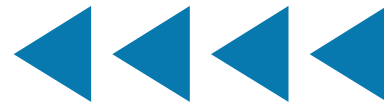
5. Publish Software Bills of Materials (SBOMs).

Manufacturers should have command of their supply chains. Organizations should build and maintain SBOMs [2] for each product, request data from their suppliers, and make SBOMs available for downstream customers and users. This will help demonstrate their diligence in understanding the components they use in the creation of their products, their ability to respond to newly identified risks, and can help customers understand how to respond if one of the modules in the supply chain has a newly found vulnerability.

For reference, Japan's Ministry of Economy, Trade, and Industry (METI) has published [“Guide of Introduction of Software Bill of Materials \(SBOM\) for Software Management.”](#) Transparency should extend to firmware in embedded devices and the data and models used in AI/machine learning (ML). Beyond assisting in purchasing decisions and operational capabilities, SBOMs play an important role in the infrastructure to detect and respond to malicious supply chain attacks.

6. **Publish a vulnerability disclosure policy.** Publish a vulnerability disclosure policy that (1) authorizes testing against all products offered by the manufacturer and conditions for those tests, (2) provides legal safe harbor for actions performed consistent with the policy, and (3) allows public disclosure of vulnerabilities after a set timeline. Manufacturers should perform root-cause analysis of discovered vulnerabilities and, to the greatest extent feasible, take actions to eliminate entire vulnerability classes. See CISA's [Vulnerability Disclosure Policy Template](#) for reference language.

PRO-SECURITY BUSINESS PRACTICES



1. Publicly name a secure by design senior executive sponsor. In many organizations, security (like quality) is delegated to technical teams who have limited ability to make structural changes to dramatically improve the security of the products. Publicly naming a top business executive to oversee the secure by design program will transform the security of products into a top-level business concern.

2. Publish a secure by design roadmap. Manufacturers should document changes made to their SDLC to improve customer security, including details about field-test reports, actions taken to eliminate entire classes of vulnerability, and other items listed in the other principles. As in the case of quality improvement efforts, security improvement programs have distinct phases of planning, control, and improvement. In the spirit of showing rather than telling, publishing the roadmap and the details behind these phases will build confidence that the products are secure by design. After achieving meaningful progress, manufacturers can detail them in transparency reports. Doing so not only demonstrates a commitment to secure by design principles but can inspire others to adopt similar programs by showing an existence proof.

3. Publish a memory-safety roadmap.

Manufacturers can take steps to eliminate one of the largest classes of vulnerability by migrating existing products and building new products using memory safe languages. While this may not be possible in all cases, manufacturers can consider developing application wrappers in memory safe languages instead of re-writing entire applications. This can also include how manufacturers are updating hiring, training, code review, and other internal processes, as well as ways they are helping the open source community do the same.

4. Publish results. While updating their SDLC to embody a secure by design philosophy, organizations will find quick wins, more resource intensive wins, and some unexpected setbacks. By presenting their internal successes and roadblocks, the entire industry can learn from the results.



PRINCIPLE 3: Lead from the Top

EXPLANATION

While the overall philosophy is called “secure by design,” the incentives for customer safety begin well before the product design phase. They begin with business goals and implicit and explicit objectives and desired outcomes. Only when senior leaders make security a business priority, creating internal incentives, and fostering an across-the-board culture to make security a design requirement will they achieve the best results.

While technical subject matter expertise is critical to product security, it is not a matter that can be solely left to technical staff. It is a business priority that must start at the top.

Some people have wondered if a software manufacturer is embracing the first two principles and producing meaningful artifacts, is the third principle necessary? How a company establishes its vision, mission, values, and culture will affect the product, and those elements have a heavy component at the top. We see this in other industries that have made dramatic improvements in safety and quality. Noted quality expert J.M. Juran wrote:

Attainment of quality leadership requires that the upper managers personally take charge of managing for quality. In companies that did attain quality leadership, the upper managers personally guided the initiative. I am not aware of any exceptions. [3]

We believe that security is a sub-category of product quality. When security and quality become business imperatives rather than technical functions left solely to technical staff, organizations will be able to respond to the security needs of their customers more quickly and efficiently. Moreover, investing the necessary resources to ensure that software security is a core business priority from the beginning will reduce the long-term costs of addressing software defects—and in turn, lower the national security risks.

In the same way that leadership teams have implemented corporate social responsibility (CSR) programs, there is growing awareness that corporate boards, including those of software manufacturers, should take a more active role in guiding cybersecurity programs. The term corporate cyber responsibility (CCR) is sometimes used to describe this emerging idea.

DEMONSTRATING THIS PRINCIPLE

To demonstrate this principle, software manufacturers should take steps including the following:

1. Include details of a secure by design program in corporate financial reports.

If the manufacturer is a publicly traded company, add a section in each annual report devoted to secure by design efforts. It is common for automobile annual financial reports to include sections on driver and passenger safety, including information about centralized and distributed quality and safety committees. Detailing the secure by design program in a financial report will demonstrate that the organization is linking customer security and corporate financial outcomes and not simply adopting a term in marketing materials because it is in vogue.

2. Provide regular reports to your board of directors. Chief information security officer (CISO) reports to corporate boards usually include information about current and planned security programs, threats, suspected and confirmed security incidents, and other updates centered on the security posture and health of the company. In addition to receiving information about the security posture of the enterprise, boards should request information about product security and the impact it has on customer security. Boards should not look solely to the CISO, but primarily to other members of company management to drive customer risk down.

3. Empower the secure by design executive.

There is a significant difference between an organization where the technical teams have “executive buy-in,” and those where business leaders personally manage the customer security improvement process using standard business processes. The term “executive buy-in” implies that someone had to sell the idea of a customer safety program rather than it being a top-level business goal. This executive must be empowered to influence product investments to achieve customer security outcomes.

4. Create meaningful internal incentives. While being mindful to not create perverse incentives, align reward systems to improve customer security to match other valued behaviors and outcomes. From the secure by design executive to product management, software development, support, sales, legal, and other organizations, weave customer security incentives into hiring, promotions, salaries, bonuses, stock options, and other common processes in the running of the business. For example, when establishing criteria for promoting software developers, include considerations for improving the security of the product along with other criteria like uptime, performance, and feature improvements.

5. Create a secure by design council. In some industries, it’s common for organizations to create a central quality council, and to embed quality representatives in key divisions or business units. By including both centralized and distributed members, these groups work to improve quality against top level goals while receiving telemetry from deep in the organization. Similarly, a secure by design council would improve security against secure by design goals throughout the organization.

6. Create and evolve customer councils. Many software manufacturers have customer councils comprised of customers from different regions, industries, and sizes. These councils can provide a great deal of information about customer successes and challenges in deploying the company’s products. Structure the council agenda with dedicated topics addressing customer safety, even if it’s not currently top of mind for the participants. Consider where the customer council reports and how to tap participants for insights into the product’s security as deployed. For example, does the council have a bias towards marketing and sales purposes, or product management? The secure by design executive should help steer these customer interactions and should link them with other elements in this paper, such as field studies.

SECURE BY DESIGN TACTICS

The Secure Software Development Framework (SSDF), also known as the National Institute of Standards and Technology's (NIST's) [SP 800-218](#), is a core set of high-level secure software development practices that can be integrated into each stage of the software development lifecycle (SDLC). Following these practices can help software producers become more effective at finding and removing vulnerabilities in released software, mitigate the potential impact of the exploitation of vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences.

The authoring organizations encourage the use of secure by design tactics, including principles that reference SSDF practices. Software manufacturers should develop a written roadmap to adopt more secure by design software development practices across their portfolio. The following is a non-exhaustive illustrative list of roadmap best practices:

- **Memory safe programming languages (SSDF PW.6.1).** Prioritize the use of memory safe languages wherever possible. The authoring organizations acknowledge that memory specific mitigations may be helpful shorter-term tactics for legacy codebases. Examples include C/C++ language improvements, hardware mitigations, address space layout randomization (ASLR), control-flow integrity (CFI), and fuzzing. Nevertheless, there is a growing consensus that adoption of memory safe programming languages can eliminate this class of defect, and software manufacturers should explore ways to adopt them. Some examples of modern memory safe languages include C#, Rust, Ruby, Java, Go, and Swift. Read NSA's memory safety [information sheet](#) for more.
- **Secure Hardware Foundation.** Incorporate architectural features that enable fine-grained memory protection, such as those described by Capability Hardware Enhanced RISC Instructions (CHERI) that can extend conventional hardware Instruction-Set Architectures (ISAs), as well as other features like Trusted Platform Modules and Hardware Security Modules. For more information visit, University of Cambridge's [CHERI webpage](#).
- **Secure Software Components (SSDF PW 4.1).** Acquire and maintain well-secured software components (e.g., software libraries, modules, middleware, frameworks) from verified commercial, open source, and other third-party developers to ensure robust security in consumer software products.
- **Web template frameworks (SSDF PW.5.1).** Use web template frameworks that implement automatic escaping of user input to avoid web attacks such as cross-site scripting.
- **Parameterized queries (SSDF PW 5.1).** Use parameterized queries rather than including user input in queries, to avoid SQL injection attacks.
- **Static and dynamic application security testing (SAST/DAST) (SSDF PW.7.2, PW.8.2).** Use these tools to analyze product source code and application behavior to detect error-prone practices. These tools cover issues ranging from improper management of memory to error prone database query construction (e.g., unescaped user input leading to SQL injection). SAST and DAST tools can be incorporated into development processes and run automatically as part of software development. SAST and DAST should complement other types of testing, such as unit testing and integration testing, to ensure products comply with expected security requirements. When issues are identified, manufacturers should perform root-cause analysis to systemically address vulnerabilities.

- **Code review** (SSDF PW.7.1, PW.7.2). Strive to ensure that code submitted into products goes through quality control techniques such as peer review by other developers or “error seeding.”
- **Software Bill of Materials (SBOM)** (SSDF PS.3.2, PW.4.1). Incorporate the creation of SBOM⁴ to provide visibility into the set of software that goes into products.
- **Vulnerability disclosure programs** (SSDF RV.1.3). Establish vulnerability disclosure programs that allow security researchers to report vulnerabilities and receive legal safe harbor in doing so. As part of this, suppliers should establish processes to determine root causes of discovered vulnerabilities. Such processes should include determining whether adopting any of the secure by design practices in this document (or other similar practices) would have prevented the introduction of the vulnerability.
- **CVE completeness.** Ensure that published CVEs include root cause or common weakness enumeration (CWE) to enable industry-wide analysis of software security design flaws. While ensuring that every CVE is correct and complete can take extra time, it allows disparate entities to spot industry trends that benefit all manufacturers and customers. For more information on managing vulnerabilities, see CISA’s [Stakeholder-Specific Vulnerability Categorization \(SSVC\)](#) guidance.
- **Defense-in-Depth.** Design infrastructure so that the compromise of a single security control does not result in compromise of the entire system. For example, ensuring that user privileges are narrowly provisioned, and access control lists are employed can reduce the impact of a compromised account. Also, software sandboxing techniques can quarantine a vulnerability to limit compromise of an entire application.
- **Satisfy Cybersecurity Performance Goals (CPGs).** Design products that meet basic security practices. CISA’s [Cybersecurity Performance Goals](#) outline fundamental, baseline cybersecurity measures organizations should implement. Additionally, for more ways to strengthen your organization’s posture, see the UK’s [Cyber Assessment Framework](#) which shares similarities to CISA’s CPGs. If a manufacturer fails to meet the CPGs— such as not requiring phishing-resistant MFA for all employees— then they cannot be seen as delivering secure by design products.

The authoring organizations recognize that these changes are significant shifts in an organization’s posture. As such, their introduction should be prioritized based on tailored threat modeling, criticality, complexity, and business impact. These practices can be introduced for new software and incrementally expanded to cover additional use cases and products. In some cases, the criticality and risk posture of a certain product may merit an accelerated schedule to adopt these practices. In others, practices can be introduced into a legacy codebase and remediated over time.

⁴ Some of the authoring organizations are exploring alternate approaches to gaining security assurances around the software supply chain.

SECURE BY DEFAULT TACTICS

In addition to adopting secure by design development practices, the authoring organizations recommend software manufacturers prioritize secure by default configurations in their products. These should strive to update products to conform to these practices as they are refreshed. For example:

- **Eliminate default passwords.** Products should not come with default passwords that are universally shared. To eliminate default passwords, the authoring organizations recommend products require administrators to set a strong password during installation and configuration or for the product to ship with a unique, strong password for each device.
- **Mandate multifactor authentication (MFA) for privileged users.** We observe that many enterprise deployments are managed by administrators who have not protected their accounts with MFA. Given that administrators are high value targets, products should make MFA opt-out rather than opt-in. Further, the system should regularly prompt the administrator to enroll in MFA until they have successfully enabled it on their account. Netherlands' NCSC has guidance that parallels CISA's, visit their [Mature Authentication Factsheet](#) for more information.
- **Single sign-on (SSO).** IT applications should implement single sign on support via modern open standards. Examples include Security Assertion Markup Language (SAML) or OpenID Connect (OIDC.) This capability should be made available by default at no additional cost.
- **Secure Logging.** Provide high-quality audit logs to customers at no extra charge or additional configuration. Audit logs are crucial for detecting and escalating potential security incidents. They are also crucial during an investigation of a suspected or confirmed security incident. Consider best practices such as providing easy integration with security information and event management (SIEM) systems with application programming interface (API) access that uses coordinated universal time (UTC), standard time zone formatting, and robust documentation techniques.
- **Software Authorization Profile.** Software suppliers should provide recommendations on authorized profile roles and their designated use case. Manufacturers should include a visible warning that notifies customers of an increased risk if they deviate from the recommended profile authorization. For example, medical doctors can view all patient records, but a medical scheduler has limited access to certain information that is required for scheduling appointments.
- **Forward-looking security over backwards compatibility.** Too often, backwards-compatible legacy features are included, and often enabled, in products despite causing risks to product security. Prioritize security over backwards compatibility, empowering security teams to remove insecure features even if it means causing breaking changes.
- **Track and reduce "hardening guide" size.** Reduce the size of "hardening guides" that are included with products and strive to ensure that the size shrinks over time as new versions of the software are released. Integrate components of the "hardening guide" as the default configuration of the product. The authoring organizations

recognize that shortened hardening guides result from ongoing partnership with existing customers and include efforts by many product teams, including user experience (UX).

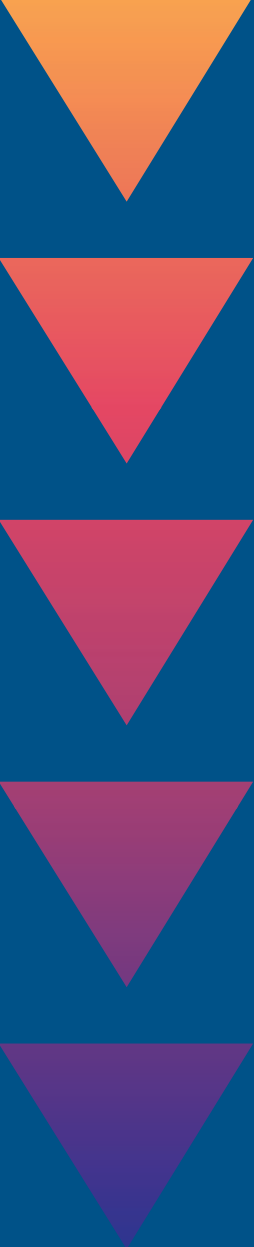
- **Consider the user experience consequences of security settings.** Each new setting increases the cognitive burden on end users and should be assessed in conjunction with the business benefit it derives. Ideally, a setting should not exist; instead, the most secure setting should be integrated into the product by default. When configuration is necessary, the default option should be broadly secure against common threats.

The authoring organizations acknowledge these changes may have operational effects on how the software is employed. Thus, customer input is critical in balancing operational and security considerations. We believe that developing written roadmaps and executive support that prioritize these ideas into an organization's most critical products is the first step to shifting towards secure software development practices. While customer input is important, we have observed important cases where customers have been unwilling or unable to adopt improved standards, often network protocols. It is important for the manufacturers to create meaningful incentives for customers to stay current and not allow them to remain vulnerable indefinitely.

HARDENING VS LOOSENING GUIDES

Hardening guides may result from the lack of product security controls being embedded into a product's architecture from the start of development. Consequently, hardening guides can also be a roadmap for adversaries to pinpoint and exploit insecure features. It is common for many organizations to be unaware of hardening guides, thus they leave their device configuration settings in an insecure posture. An inverted model known as a loosening guide should replace such hardening guides and explain which changes users should make while also listing the resulting security risks. These guides should be written by security practitioners who can explain the tradeoffs in clear language to increase the chances of them being applied correctly.

Rather than developing hardening guides that list methods for securing products, the authoring organizations recommend software manufacturers shift to a secure by default approach and providing "loosening guides." These guides explain the business risk of decisions in plain, understandable language, and can raise organizational awareness of risks to malicious cyber intrusions. Security tradeoffs should be determined by the customers' senior executives, balancing security with other business requirements.



RECOMMENDATIONS FOR CUSTOMERS

The authoring organizations recommend organizations hold their supplying software manufacturers accountable for the security outcomes of their products. As part of this, the authoring organizations recommend that executives prioritize the importance of purchasing secure by design and secure by default products. This can manifest through establishing policies requiring that IT departments assess the security of software before it is purchased, as well as empowering IT departments to push back if necessary. IT departments should be empowered to develop purchasing criteria that emphasize the importance of secure by design and secure by default practices (both those outlined in this document and others developed by the organization). Furthermore, IT departments should be supported by executive management when enforcing these criteria in purchasing decisions. Organizational decisions to accept the risks associated with specific technology products should be formally documented, approved by a senior business executive, and regularly presented to the board of directors.

Key enterprise IT services that support the organization's security posture, such as the enterprise network, enterprise identity and access management, and security operations and response capabilities, should be seen as critical business functions that are funded to align with their importance to the organization's mission success. Organizations should develop a plan to upgrade these capabilities to leverage manufacturers that embrace secure by design and secure by default practices.

Where possible, organizations should strive to forge strategic relationships with their key IT suppliers. Such relationships include trust at multiple levels of the organization and provide vehicles to resolve issues and identify shared priorities. Security should be a critical element of such relationships and organizations should strive to reinforce the importance of secure by design and secure by default practices in both the formal (e.g., contracts or vendor agreements) and informal dimensions of the relationship. Organizations should expect transparency from their technology suppliers about their internal control posture as well as their roadmap towards adopting secure by design and secure by default practices.

In addition to making secure by default a priority within an organization, IT leaders should collaborate with their industry peers to understand which products and services best embody these design principles. These leaders should coordinate their requests to help manufacturers prioritize their upcoming security initiatives. By working together, customers can help provide meaningful input to manufacturers and create incentives for them to prioritize security.

When leveraging cloud systems, organizations should ensure they understand the shared responsibility model with their technology supplier. That is, organizations should have clarity on the supplier's security responsibilities rather than just the customer's responsibilities.

Organizations should prioritize cloud providers that are transparent about their security posture, internal controls, and ability to live up to their obligations under the shared responsibility model.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. CISA and the authoring organizations do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial entities or commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise does not constitute or imply endorsement, recommendation, or favoritism by CISA and the authoring organizations. This document is a joint initiative by CISA that does not automatically serve as a regulatory document.

Resources

CISA

- » [CISA's SBOM Guidance](#)
- » [CISA's Cross-Sector Cybersecurity Performance Goals](#)
- » [Guidelines on Technology Interoperability](#)
- » [CISA and NIST's Defending Against Software Supply Chain Attacks](#)
- » [The Cost of Unsafe Technology and What We Can Do About It | CISA](#)
- » [Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products \(foreignaffairs.com\)](#)
- » [CISA's Stakeholder-Specific Vulnerability Categorization \(SSVC\) Guidance](#)
- » [CISA's Phishing Resistant MFA Fact Sheets](#)
- » [Cyber Guidance for Small Businesses | CISA](#)

NSA

- » [NSA's Cybersecurity Information Sheet on Memory Safety](#)
- » [NSA's ESF Securing the Software Supply Chain: Best Practices for Suppliers](#)

FBI

- » [Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective](#)
- » [The Cyber Threat - Response and Reporting](#)
- » [FBI's Cyber Strategy](#)

National Institute of Standards and Technology (NIST)

- » [NIST's Digital Identity Guidelines](#)
- » [NIST's Cyber Security Framework](#)
- » [NIST's Secure Software Development Framework \(SSDF\)](#)

Australian Cyber Security Centre (ACSC)

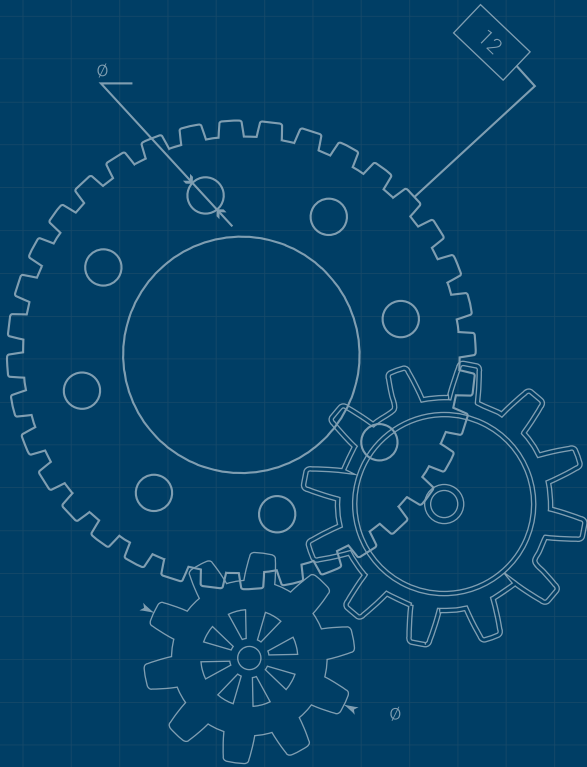
- » [ACSC's IoT Code of Practice Guidance for Manufacturers](#)

The United Kingdom's National Cyber Security Centre (UK)

- » [The UK's Cyber Assessment Framework](#)
- » [The UK NCSC's Secure Development and Deployment guidance](#)
- » [The UK NCSC's Vulnerability Management guidance](#)
- » [The UK NCSC's Vulnerability Disclosure Toolkit](#)
- » [University of Cambridge's CHERI](#)
- » [So long and thanks for all the bits - NCSC.GOV.UK](#)

Canadian Centre for Cyber Security (CCCS)

- » [CCCS's Guidance on Protecting Against Software Supply Chain Attacks](#)
- » [Cyber supply chain: An approach to assessing risks](#)
- » [Canadian Centre for Cyber Security's CONTI ransomware guidance](#)



Germany's Federal Office for Information Security (BSI)

- » [The BSI Grundschrift compendium \(module CON.8\)](#)
- » [The international standard IEC 62443, part 4-1](#)
- » [State of IT-security in Germany report, 2022](#)
- » [BSI practices of web application security](#)

Netherland's National Cyber Security Centre

- » [NCSC-NL's Mature Authentication Factsheet](#)

Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC)

- » [Japan's National Cybersecurity Strategy](#)

Japan's Ministry of Economy, Trade and Industry (METI)

- » [Guide of Introduction of Software Bill of Materials \(SBOM\) for Software Management](#)
- » [Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security](#)

Cyber Security Agency of Singapore

- » [Technical Advisory on Secure API Development](#)
- » [CSA SingCERT Vulnerability Disclosure Policy](#)
- » [CSA SingCERT Incident Response Checklist](#)
- » [CSA SingCERT Incident Response Playbooks](#)
- » [CSA Security by Design Framework](#)
- » [CSA Security by Design Framework Checklist](#)
- » [CSA Guide to Cyber Threat Modelling](#)
- » [CSA Cybersecurity Labelling Scheme](#)

Other

- » [How Complex Systems Fail](#)
- » [The New Look in complex system failure](#)

REFERENCES

- [1] <https://csrc.nist.gov/publications/history/ande72.pdf>
- [2] <https://www.cisa.gov/sbom> and SBOMs references in TR 03183-2 <https://www.bsi.bund.de/dok/TR-03183>
- [3] Juran on Quality by Design by J.M. Juran, 1992.

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-9

The following is the annexure marked **FT-9** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains screenshots of the DTA's post announcing the public release of the source code, entitled 'DTA publicly releases COVIDSafe application source code', published on 8 May 2020, as archived by Internet Archive Wayback Machine on 26 October 2021 and accessed on 27 July 2026 at

https://web.archive.org/web/20211026183349mp_/https://www.dta.gov.au/news/dta-publicly-releases-covidsafe-application-source-code

.....
Daniel Davison
Solicitor



We're working to support the Australian community during the COVID-19 emergency. [Visit australia.gov.au](https://australia.gov.au) for more information.



Australian Government
Digital Transformation Agency

What are you looking for today?

Search

Simple, clear and fast public services

[Help and advice](#)

[Our projects](#)

[About us](#)

[News and blogs](#)

[Digital Transformation Strategy](#)

[Contact us](#)

[Home](#) > DTA publicly releases COVIDSafe application source code

DTA publicly releases COVIDSafe application source code

8 May 2020

Tags: [Security](#) [Content design](#) [COVID-19](#) [COVIDSafe](#)

Today the Digital Transformation Agency released to the public the source code for the COVIDSafe application. Any member of the public can view the source code, which is hosted on a [GitHub repository](#).

Protecting the privacy of Australians downloading and using COVIDSafe is paramount. Prior to launching the application, the source code was reviewed by government security agencies, academics and industry specialists. We are releasing the app code, but to ensure the privacy of individuals and integrity of the overall system, the code that relates to the COVIDSafe National Information Storage System will not be released.

DTA welcomes feedback from the community

Now researchers, developers, academics and members of the public can also review the source code in detail.

You can provide feedback about the application's source code by emailing support@covid-safe.gov.au. We welcome the feedback that has already been provided following the app's launch.

While we may be unable to reply to every individual who provides feedback, please know that your feedback will be reviewed and triaged depending on its impact to security and usability.

In some instances, the DTA may contact you to gain a deeper understanding about the issues raised.

RSS feeds

[Our feeds](#)

Sign-up for DTA updates

If you would like to receive email notification when we publish news and blogs, please fill in the form.

* indicates required

Email address *

First name

Last name

State or territory

[Subscribe](#)

Improving the COVIDSafe application

In line with standard development and software practices, we are rolling out updated releases of the application and we will implement design changes based on their priority.

This week we rolled out the first update, which addressed some of the most common issues raised by the community, including:

- Content changes to make the app more user friendly. An example is better alignment between the registration process and help topics.
- Content changes to better explain to the user the process to upload data if a user tests positive to the virus.
- Changes to address minor registration issues associated with the name field.
- Changes to stop notifications for some iOS users looping to the registration screen.
- Changes to address the app causing issues with the operating system for a small number of Android users.

Future releases of COVIDSafe

Like all apps, we plan to iteratively enhance COVIDSafe and we already have a plan for the next couple of releases. These releases will focus on further strengthening the security of the application and improve its usability and accessibility. Our next update will occur during the week commencing 11 May 2020.

We are also working with Apple and Google as they develop technology that could enhance the COVIDSafe application.

Visit the [COVIDSafe](#) website for more information or to access the source code for the COVIDSafe application.

For media enquiries email us at media@dta.gov.au

For other enquiries email us at info@dta.gov.au



[Contact us](#) [Join our team](#) [Accessibility](#) [Cookies](#) [Privacy](#)
[Disclaimer and copyright](#)

© Commonwealth of Australia. With the exception of the Commonwealth Coat of Arms and where otherwise noted, this work is licensed under the CC BY 4.0 license.

Social media

Twitter
 Facebook
 LinkedIn
 YouTube

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-10

The following is the annexure marked **FT-10** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains screenshots of the DTA's post entitled 'Key COVIDSafe improvements enhance and protect your privacy', published on or around 7 September 2020, as archived by Internet Archive Wayback Machine on 17 June 2021 and accessed on 27 July 2026 at:

<https://web.archive.org/web/20210617234500/https://www.dta.gov.au/news/key-covidsafe-improvements-enhance-and-protect-your-privacy>

.....
Daniel Davison
Solicitor



We're working to support the Australian community during the COVID-19 emergency. [Visit australia.gov.au](https://australia.gov.au) for more information.



Australian Government
Digital Transformation Agency

Simple, clear and fast public services

[Help and advice](#)[Our projects](#)[About us](#)[News and blogs](#)[Digital Transformation Strategy](#)[Contact us](#)

[Home](#) > [Key COVIDSafe improvements enhance and protect your privacy](#)

Key COVIDSafe improvements enhance and protect your privacy

7 September 2020

Tags: [COVID-19](#) [COVIDSafe](#) [Privacy](#) [Security](#) [Service design](#)

Key improvements have been made to the COVIDSafe app to better protect the security and privacy of all users.

On 8 May 2020, we [released the app's source code to our GitHub repository](#). As part of our commitment to transparency, today we're releasing the [COVIDSafe Cryptography Specification](#). We have worked with government experts, academia, industry specialists and the tech community to make sure the best security and privacy protections possible for all COVIDSafe app users.

Information that COVIDSafe exchanges between devices

One of the ways your data is protected in COVIDSafe is through the temporary identifier ("tempID") from the COVIDSafe servers. The tempIDs are periodically generated and expire after a certain time. They contain a random unique-identifier. This is used to identify you as an individual user of the app without including any personally identifiable information, such as your phone number, name, postcode or age. This keeps your information safe. The tempID appears completely random to devices that have the COVIDSafe app so they can't tell who you are. Only the National Data Store can recover, from a particular tempID, which user it was issued to.

RSS feeds

[Our feeds](#)

Sign-up for DTA updates

If you would like to receive email notification when we publish news and blogs, please fill in the form.

Email address

First name

Last name

State or territory

[Subscribe](#)

How COVIDSafe exchanges my temporary identifier with nearby devices

Whenever you are in range of another COVIDSafe user, your apps perform a “digital handshake” by exchanging information over Bluetooth. This includes your tempID, and information about phone model and Bluetooth signal strength. More recent versions of COVIDSafe include the time each digital handshake occurs as part of the information exchanged. This allows the server to perform better validation checks. It also means the app can run for up to a week without needing an internet connection, which improves its performance.

When a digital handshake occurs between 2 COVIDSafe users, the information that is exchanged is encrypted so that only the National Data Store can read it. This encryption is like a padlock: anyone can use an open padlock to lock up a box of valuables, but only the trusted person with the key will be able to open it and access what’s inside.



Figure 1: data sent in the digital handshake is now encrypted, so only the COVIDSafe server can read it

The encrypted encounter data your phone stores from other users is uploaded to the National Data Store with your consent if you test positive for COVID-19. It cannot be decrypted by unauthorised third parties.

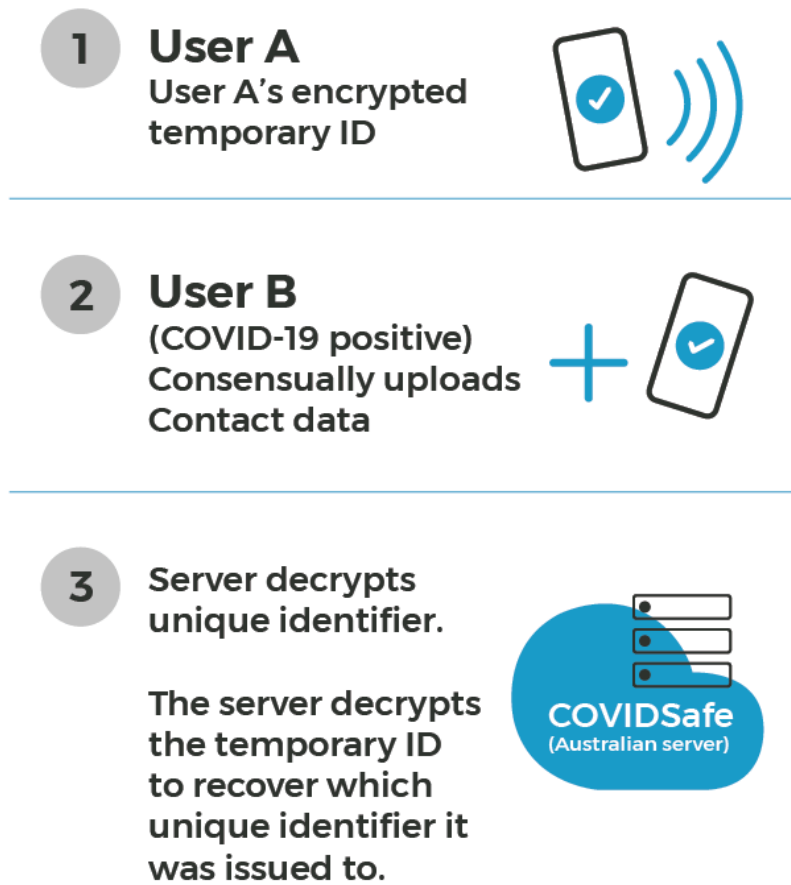


Figure 2: a user's tempID can only be unencrypted by the server.

Improved privacy protections

The data exchanged in the digital handshake now changes every 7.5 minutes instead of every 2 hours. This is a significant improvement to the privacy of users. It reduces the time COVIDSafe sends the same identifier to other app users by up to 93%.

New protections for COVIDSafe data

Working with subject matter experts in industry and academia, we have improved the COVIDSafe code and design. We have enhanced privacy by adding an additional layer of encryption to the Bluetooth exchange.

We also continue to work closely with government, industry, academia and members of the community – including software developers and researchers – to improve the security, privacy and usability of COVIDSafe. We would like to thank everyone for their feedback and recommendations, which continue to inform the development of the app.

For media enquiries email us at media@dta.gov.au

For other enquiries email us at info@dta.gov.au



[Contact us](#) [Join our team](#) [Accessibility](#) [Cookies](#) [Privacy](#)

[Disclaimer and copyright](#)

© Commonwealth of Australia. With the exception of the Commonwealth Coat of Arms and where otherwise noted, this work is licensed under the CC BY 4.0 license.

Social media



**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-11

The following is the annexure marked **FT-11** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains screenshots of the 'Background to COVIDSafe' website as archived by the Internet Archive Wayback Machine on 22 December 2022, which is the most recent capture prior to the site becoming unavailable, and accessed on 27 July 2026 at:

<https://web.archive.org/web/20221222105629/https://covidsafe.gov.au/background.html>

.....
Daniel Davison
Solicitor



Australian Government

[Home](#) [How to use](#) [Technology](#) [Privacy and data](#) [Help topics](#)

Background to COVIDSafe

On this page

- [Overview](#)
- [How COVIDSafe works](#)
- [Close contact information](#)
- [Privacy and security](#)
- [Other COVID-19 mobile services from government](#)
- [Amazon Web Services \(AWS\)](#)
- [More help for COVIDSafe](#)

Overview

The Australian Government developed COVIDSafe to help keep the community safe from coronavirus (COVID-19). Together, let's help stop the spread.

COVIDSafe uses Bluetooth® technology on your mobile phone to look for other devices with COVIDSafe installed. Your phone will take note of contact you've had with other users by securely logging their details.

If you test positive for COVID-19:

- you can consent to the COVIDSafe information securely stored in your phone (called digital handshakes) to be uploaded to the [National COVIDSafe Data Store](#)
- state or territory health officials can then quickly contact people who may have been exposed to the virus

[\[Close all \]](#)

Australia needs COVIDSafe



COVIDSafe helps state and territory health officials to quickly contact people who may have been exposed to COVID-19.

As restrictions are lifted the app helps give us the confidence to know that the virus is not spreading silently in the community.

COVIDSafe supports the current manual process of finding people who have been in close contact with someone with COVID-19.

The more Australians connect to COVIDSafe, the quicker we can find the virus and prevent the spread.

Purpose



COVIDSafe assists state and territory health officials to contact you if you have been in contact with someone with COVID-19. They tell you:

- what to look out for
- whether you need to [quarantine](#)
- how, when and where to [get tested](#)
- how you can [protect yourself and your family and friends](#).

If you test positive for COVID-19, COVIDSafe helps state and territory health officials to notify people you've been in close contact with and advise them about self-quarantine and getting tested.

This will support current manual processes and make it quicker to stop the spread of the virus, particularly as restrictions are eased.

Reasons to use COVIDSafe



Using COVIDSafe means you can:

- receive early notification from a state or territory health official that you may have been exposed to COVID-19
- get tested promptly
- go into quarantine to protect your health and the health of others.

Without the help of technology, finding people who may have been exposed to the virus relies on people:

- being able to recall everyone they have been in close contact with
- knowing their contact details.

In many cases, people won't know the names and contact details of everyone they've been in close contact with (for example, on public transport).

COVIDSafe uses technology to make this process faster and more accurate. We developed it to ensure your information and privacy are strictly protected.

State and territory health officials can only access close contact information from COVIDSafe if a user tests positive for COVID-19 and consents to this information being uploaded. This helps alert those who may need to be tested.

COVIDSafe will never track your location.

App lifecycle



We regularly release COVIDSafe updates, which you can access via your phone's app store or by allowing automatic updates.

COVIDSafe will have a defined end date. The [Privacy Act 1988](#) as amended in 2020 (the Act) calls this the end of the COVIDSafe data period.

The Minister for Health will formally notify the end of the COVIDSafe app data period (section 94Y of the Act):

- when the Minister is satisfied that COVIDSafe is no longer required or no longer likely to be effective in preventing or controlling COVID-19 in Australia
- after consulting the Commonwealth Chief Medical Officer or the Australian Health Protection Principal Committee.

The Act (section 94P) states that after the end of the COVIDSafe data period:

- COVIDSafe must not be available for download
 - COVIDSafe app data must not be collected
 - COVIDSafe app data must be deleted
 - COVIDSafe users should be informed of the above and that they should delete COVIDSafe from their phone.
-

Campaign materials and digital products

You can use [COVIDSafe campaign materials](#) as long as you do not make any changes to the materials. If you have questions about these resources, please contact CoronaComms@health.gov.au

You can use images of the COVIDSafe app, including screenshots, for publications purposes provided you give attribution to the Department of Health.

You cannot use the [Commonwealth coat of arms](#) without written permission.

COVIDSafe in other languages

COVIDSafe is available in 9 languages in addition to English:

- Traditional Chinese
- Simplified Chinese
- Arabic
- Vietnamese
- Korean
- Greek
- Italian
- Punjabi
- Turkish

See how to [use COVIDSafe in a language other than English](#).

Translated information about COVIDSafe is available for you to download and use:

- [User guide to download the COVIDSafe app](#)
- [How to download the COVIDSafe app](#) video
- [COVIDSafe privacy policy](#)
- [Stay COVID free – do the 3](#) poster
- [Stay COVID free – do the 3](#) video.

The [National Coronavirus Helpline](#) can answer questions on COVIDSafe, including troubleshooting during installation, through the [translating and interpreting service](#).

How COVIDSafe works

COVIDSafe operates on your phone as you go about your day. It securely logs the unique identifiers of devices of other COVIDSafe users who have been in close proximity to you. Read more on the [technology behind COVIDSafe](#).

You can voluntarily download the app from the Apple App Store or Google Play. You register to use the app by entering:

- a name (which can be a pseudonym)
- age range
- mobile number
- postcode.

You will receive a confirmation text message to complete the installation. Based on this information, COVIDSafe generates unique identifiers for the app on that phone, which changes regularly to make it more secure.

For COVIDSafe to work, Bluetooth needs to be turned on and the app running in the background on your phone. Other apps can be used at the same time.

COVIDSafe uses Bluetooth to look for other devices that have the app installed. It takes a note of a contact when it occurs, through a digital handshake. It securely logs the other user's unique identifiers, the date, time, Bluetooth signal strength and proximity of the contact on the user's phone, and notes the phone model. This information is then securely encrypted and stored on the phone.

COVIDSafe does not record your location.

COVIDSafe stores contacts on the phone for 21 days. This allows for the 14-day incubation period of the coronavirus, plus the time taken to confirm a positive test result. The rolling 21-day window allows COVIDSafe to continuously note only those user contacts that occur during the coronavirus incubation window. It automatically deletes contacts older than 21 days.

Nobody can access the encrypted information on your phone, including you. If you test positive for COVID-19, you will be asked to consent to upload your digital handshake information to the [National COVIDSafe Data Store](#). The uploaded information enables state and territory health officials to call close contacts to advise them on what to do. State and territory health officials must undertake system training before they can access the [National COVIDSafe Data Store](#).

This cycle continues if a COVIDSafe user who was a close contact later tests positive.

Who can use COVIDSafe



Anyone living in Australia who has a phone that meets the [minimum requirements](#) can download and use COVIDSafe. You need to be connected to Wi-Fi or mobile data to download the app.

Some Australians in rural areas are experiencing difficulties downloading and installing COVIDSafe due to network coverage issues. We advise these people to download and register on the app over the mobile network the next time they are in a coverage area. This might be when they travel into town to purchase groceries or supplies. We have identified a potential solution and are working with the carrier to implement it. We will include the change in a future update.

COVIDSafe is available to:

- users in Australia with Australian or non-Australian Apple App Store and Google Play Store accounts
- people living in Australian External Territories like Norfolk Island
- people with Australian or international mobile phone numbers.

We want to make sure as many people living in Australia as possible can download and use COVIDSafe.

If you tested positive, isolated and recovered

If you have recovered from COVID-19, we still encourage you to use COVIDSafe. We encourage everyone living in Australia to use COVIDSafe regardless of their location or health status.

No extra risk of false positives



There is no extra risk of false positives with COVIDSafe. This is because state and territory health officials verify a person's positive diagnosis before asking them to upload their digital handshake information.

If you test positive



If you test positive for COVID-19, a state or territory health official in your state or territory will contact you. You will be asked to voluntarily upload your digital handshake information to the secure server. The health official will give you a PIN for this upload.

This will help state or territory officials identify people who may have had close contact with you. Uploading your information is a crucial part of alerting others who may be at risk, and could save lives.

For information on what happens if one of your close contacts tests positive, see [if a close contact tests positive](#).

If you refuse to upload information

You do not have to consent to share your COVIDSafe app information if you test positive for COVID-19. But remember that uploading your information could help save lives and keep others in the community safe.

State and territory health officials already require people who test positive for COVID-19 to provide information about their close contacts. COVIDSafe supports manual contact tracing processes. It can provide extra information of contacts that you may not know, such as the person sitting near you on public transport.

Whether or not you consent to the use of your COVIDSafe information, you will still have to go through the existing contact tracing process of recalling all your recent contacts and providing them to your state or territory health officials. The app adds to this process and makes it more effective.

COVIDSafe is community-driven. When app users who test positive for COVID-19 consent to upload their digital handshake information, it helps protect others in the community who have also been exposed.

If a close contact tests positive



Health officials will contact you or your parent/guardian/carer on the mobile number you registered with COVIDSafe to alert you to potential exposure if:

- a person tests positive for COVID-19 and they are a COVIDSafe user
- your device noted that you were in close proximity to them in the last 21 days.

Health officials may discuss the suspected day and time of exposure with the close contact, as per their usual processes. They will not name the person who was infected.

If you believe you have come into contact with a person who has tested positive for COVID-19 but you haven't been contacted, contact your doctor to discuss this and how to get tested.

Close contact information is only available to state and territory health officials after:

- a user is confirmed as COVID-19 positive
- the user consents to securely upload the information stored on their phone

Officials will only call people who were close contacts within the 21 days before the information was uploaded. This early notification allows users to quickly get tested and go into quarantine.

Find out where [you can get tested](#).

Follow the [guidelines on quarantine](#).

Contacting deaf users



State and territory health officials carry out contact tracing. COVIDSafe does not replace their usual contact tracing processes. It supports them.

Please contact the health department in your state or territory for information about their contact tracing processes, including how they support the deaf community and people with differing communication needs.

The Australian Government website www.australia.gov.au has links to COVID-19 advice for all states and territories.

Close contact information

State and territory public health officials only have access to contact information for other COVIDSafe users who have been within approximately 1.5 metres for a period of 1 minute or more.

How COVIDSafe identifies close contact

When 2 or more app users come close to each other their phones exchange Bluetooth® signals and make a series of digital handshakes.

COVIDSafe notes the [encrypted information held on your phone](#) through the strength of Bluetooth® signals. Once the information is uploaded to the [National COVIDSafe Data Store](#), it is then filtered so that state and territory health official can access close contacts.

The proximity for a close contact is approximately 1.5 metres, for a period of 1 minute or more.

To be effective, COVIDSafe should be active on your phone whenever you are coming into contact with people.

How COVIDSafe measures distance and duration of contact

COVIDSafe uses Bluetooth® received signal strength indicator (RSSI) values to measure the signal strength between devices. It uses the calibrated RSSI values to estimate the likelihood of a person being in close contact. Read more on [RSSI values](#).

COVIDSafe collects data that is exchanged between users of the app at a series of intervals. In this way it estimates how long an encounter between 2 users lasted, to determine whether a user was probably exposed to COVID-19.

Contacts are not named

If a state or territory health official tells you that you are a close contact, they will not name the person who tested positive. This is the same as existing contact tracing processes.

COVIDSafe stores close contacts for 21 days

The average incubation period for someone who contracts COVID-19 is typically 5 to 6 days. However, the World Health Organization (WHO) currently estimates that the incubation period can be up to 14 days. These estimates will be refined as more data becomes available.

COVIDSafe's rolling 21-day window allows for the 14-day incubation period, plus the time taken to confirm a positive test result.

The rolling 21-day window allows the app to continuously monitor only those user contacts that occur during the coronavirus incubation window.

COVIDSafe automatically deletes contacts that occurred outside the 21-day window from the user's phone.

Privacy and security

Downloading and using COVIDSafe is voluntary. The app has a range of privacy and security safeguards built in. It uses secure encryption and does not collect data on your location.

You can read an independently developed [Privacy Impact Assessment](#) detailing COVIDSafe's compliance with the Privacy Act 1988 and Australian Privacy Principles. You can also read the [Department of Health's response to the assessment](#).

Information submitted when you register

At registration, you provide a name (which does not have to be your real name), age range, phone number and postcode. The app generates unique identifiers for your mobile phone. The encrypted user ID will be created every 7 days. This will be logged in the National COVIDSafe Data Store (data store), operated by the Department of Health, in case you need to be identified for contact tracing.

COVIDSafe needs a mobile number to activate an account and to allow state or territory health officials to contact you if they need to. The postcode you register with will help identify the relevant state or territory health authority to contact you.

A state or territory health official will contact you if:

- you test positive for COVID-19. If you are a registered COVIDSafe user, the official will ask you to upload the digital handshake information stored on your device. This is voluntary.
- you are a close contact of other COVIDSafe users who test positive for COVID-19.

The name you registered with will be used during the call to verify you are the owner of the mobile number.

Information COVIDSafe collects

COVIDSafe only collects the following information:

- Registration information: name or pseudonym, mobile number, age range and post code. This is stored in the [National COVIDSafe Data Store](#).
- Digital handshake information: unique identifiers, date and time, Bluetooth signal strength, and phone model. This is stored on your phone. If you test positive and upload your information to the [National COVIDSafe Data Store](#), an algorithm uses the Bluetooth® signal strength to determine proximity and duration of contact with other COVIDSafe app users.
- Diagnostic information: the operating system on your phone, the version of COVIDSafe installed on your phone, the language your device is set to, whether your App has recorded any contacts with other COVIDSafe users in the previous seven days, whether your phone has Bluetooth enabled, whether your phone has battery optimisation enabled, and whether your phone has location services enabled.

COVIDSafe does not collect information on your location or your movements.

COVIDSafe collects information needed for health officials to conduct contact tracing. This information includes unique identifiers, date, time, duration and proximity of contacts, and phone model.

All digital handshake information COVIDSafe collects is encrypted and stored on the user's phone. You cannot access this information stored on your phone.

If you delete the app from your phone, this will also delete all the digital handshake information from your phone.

Nobody can access the digital handshake information on your phone, unless you test positive for COVID-19 and you consent to upload the contact information to the [National COVIDSafe Data Store](#).

Diagnostic information is automatically generated by your device and is sent regularly to the data store. An automated system uses this information to decide whether to send you a notification to let you know that something is not working in your app. It will also guide you through the process to fix it. This information is not used for any other purpose.

Only the last check in data sent by an App to the data store will be stored. Historical diagnostic information is not retained.

COVIDSafe cannot track location



COVIDSafe only collects information about interactions with other COVIDSafe users, and diagnostics on how the app is performing on your device. COVIDSafe does not collect or use physical location data (for example, GPS, Wi-Fi fingerprinting and cell ID). It only notes proximity to another COVIDSafe user via Bluetooth®.

It does not record an individual's location or movements. COVIDSafe only records that a close contact occurred to allow state or territory health officials to contact those users to enable them to quickly get tested and go into quarantine.

COVIDSafe cannot be used to enforce quarantine or isolation restrictions or any other laws.

Commonwealth and state or territory law enforcement agencies will not be allowed to access any information from the app, unless investigating misuse of that information itself.

How COVIDSafe stores information



COVIDSafe encrypts the name or pseudonym, verified mobile number, age range and postcode you registered on the [National COVIDSafe Data Store](#), which is hosted in Australia.

The storage system is geo-locked, meaning nobody can take the information out of Australia.

COVIDSafe provides the information as an encrypted hash code. This is the only information shared with other users as part of the Bluetooth® digital handshake.

COVIDSafe stores the digital handshakes it collects on your phone. It encrypts this information and nobody can access or view it, including you.

COVIDSafe automatically deletes digital handshakes that are older than 21 days from your phone.

Digital handshake information only leaves your phone if you test positive for COVID-19 and consent to the upload.

If you consent, the information is then uploaded to the [National COVIDSafe Data Store](#). Only authorised state and territory health officials can access contact information, and only after they have received system training. State and territory health officials can only view close contact information collected by people from their state or territory, who have tested positive for COVID-19.

When accessing and using the uploaded information, health officials must comply with the obligations in part VIIIA of the [Privacy Act 1988](#) and the [Australian Privacy Principles](#). These regulate data protection and information security obligations. The information will only be used to alert individuals if they have come into contact with a person who has tested positive for COVID-19.

Diagnostic information is automatically generated by a user's device and sent daily to the National COVIDSafe Data Store, which calculates the appropriate notification to send to you. All communication is directly between your device and the data store.

Downloading COVIDSafe is voluntary



Using COVIDSafe is entirely voluntary, but it will help save lives.

COVIDSafe does not replace existing contact tracing processes conducted by state and territory public health authorities — it supports them. State and territory public health authorities will continue to ask people who are diagnosed with COVID-19 about their close contacts, whether they use COVIDSafe or not.

You can contact the health department in your state or territory for information about their existing processes. The Australian Government website www.australia.gov.au has links to COVID-19 advice for all of the states and territories.

It is against the law to require another person to download, or operate, the COVIDSafe app.

Downloading the COVIDSafe app is completely voluntary and cannot be forced upon anyone in any way. The [Privacy Act 1988](#) provides for this. The Department of Health and the Prime Minister have also publicly reiterated this.

For this reason, nobody can give incentives for others to download COVIDSafe. They can only recommend and encourage it. The [COVIDSafe privacy policy](#) states “No user should feel pressured to install or continue to use COVIDSafe, or to agree to upload contact data to the data store”.

In particular, a person (including a business or company) cannot:

- refuse entry into, or continue, a contract or arrangement with another person (including a contract of employment) if they don't have the app
- disadvantage an employee if they don't have the app
- refuse to allow another person to enter premises accessible to the public or that the other person has a right to enter if they don't have the app
- refuse to allow another person to participate in an activity if they don't have the app
- refuse to receive goods or services or insist on providing less money for the goods or services if someone doesn't have the app
- refuse to provide goods or services or insist on receiving more money for the goods or services if someone doesn't have the app.

For example, your employer must not require the download or use of the COVIDSafe app as part of your employment, or disadvantage you if you refuse to download the app. An operator of a business open to the public must not refuse entry to you just because you have not downloaded or are not using the app.

If someone tries to force you to use COVIDSafe

The COVIDSafe app enables faster and more comprehensive contact tracing for people exposed to COVID-19 and all Australians are encouraged to download it to help protect themselves, their family and community.

However it is voluntary and you cannot be told it is compulsory.

If your employer or anyone else purports to require you to download or use the COVIDSafe app, or upload your contact information, you can:

- Explain to the person who is telling you to download or use the app or upload your information that:
 - downloading or using the app or uploading information from the app is voluntary
 - the Privacy Act prohibits anyone making another person download or use the app or upload contact information from the app
 - in some circumstances this could amount to a criminal offence.
- Contact the National Coronavirus Helpline on [1800 020 080](tel:1800020080).

If you believe an offence under the Privacy Act has been committed, you can make a complaint to the [Office of the Australian Information Commissioner](#), or the [Australian Federal Police](#).

Penalty for forcing use

Contravening section 94H of the Privacy Act is a criminal offence punishable by a maximum sentence of 5 years' imprisonment, or a fine.

Protections for children



Children can download and use the COVIDSafe app.

The Government expects parents, guardians and carers will provide the same care and guidance to their children with respect to the COVIDSafe app as they do when their children download any other app. It is important for parents to talk to their children about the app and how it works.

When a person under the age of 16 registers the app, it prompts them to confirm they have the consent of their parent, guardian or carer before they proceed.

If a child running COVIDSafe on their device tests positive for COVID-19, the relevant state or territory health official will seek the consent of the child's parent, guardian or carer before the child's information is uploaded to the [National COVIDSafe Data Store](#).

If a state or territory health official contacts a child because they have been in contact with someone who has tested positive for COVID-19, they will ask to speak to the child's parent, guardian or carer. They will then provide the necessary information and advice.

Legislation to protect privacy



The [Privacy Amendment \(Public Health Contact Information\) Act 2020](#) amends the Privacy Act (the Act) to provide stronger privacy protections for COVIDSafe app data. COVIDSafe app data can only be used for specific purposes, and only to the extent required for those purposes.

Under the Act, COVIDSafe app data can only be collected, used or disclosed for the purposes of:

- state and territory health authorities undertaking contact tracing.
- the Department of Health (as the data store administrator):
 - enabling contact tracing by state and territory health authorities.
 - ensuring the proper functioning, integrity or security of the COVIDSafe app or [National COVIDSafe Data Store](#).
 - using COVIDSafe app data to produce de-identified statistical information about the total number of registrations through the COVIDSafe app.
 - using COVIDSafe app data to confirm the correct data is being deleted, if a request has been made to delete the data.
- the Australian Information Commissioner performing functions or exercising powers under the Act.
- investigating or prosecuting a breach of the privacy protections under the Act.

The Act also:

- prohibits anyone from requiring a person to download or use the COVIDSafe app. For example, an employer cannot make downloading or using the COVIDSafe app a condition of employment.
- states the data held in the [National COVIDSafe Data Store](#) and COVIDSafe app data must be kept in Australia.
- requires that the data store administrator delete all COVIDSafe app data held in the [National COVIDSafe Data Store](#) when the COVIDSafe app is no longer required, or is no longer likely to be effective as part of Australia's response to COVID-19. The Minister for Health must determine this following consultation with the Commonwealth Chief Medical Officer or the Australian Health Protection Principal Committee.

Law enforcement agencies or the Australian Information Commissioner can only access COVIDSafe app data to enforce these privacy protections. They cannot use it for any other purpose.

If you think your privacy has been breached, you can make a complaint to the [Office of the Australian Information Commissioner](#) or the [Australian Federal Police](#).

Read the COVIDSafe privacy policy



You can find the COVIDSafe privacy policy:

- [as a web page](#)
- [in 63 languages other than English](#).

Security of COVIDSafe



Protecting the privacy of Australians downloading and using COVIDSafe is a top priority.

Strong cyber security principles underpin COVIDSafe's security design to ensure that your information remains safe. Cyber security experts independently assured these security controls throughout COVIDSafe's development.

COVIDSafe uses Bluetooth® technology on mobile phones to perform a digital handshake. This records close contact with another user who also has the COVIDSafe app installed. The Bluetooth® technology COVIDSafe uses is similar to that used when pairing with other Bluetooth®-enabled devices like headphones or smartwatches.

Your phone's operating system has device-level security controls to keep your information safe. Please keep your smartphone software up to date to ensure you have the latest security controls installed.

All information that COVIDSafe stores (both on your phone and in the [National COVIDSafe Data Store](#)) is encrypted. This provides extra cyber security protection of your information.

We will continue to work with government security agencies, tech experts and the community to maintain and strengthen COVIDSafe's already strong security.

Australian Cyber Security Centre Assessment



The Department of Health is working with the Australian Signals Directorate's (ASD) [Australian Cyber Security Centre \(ACSC\)](#) to conduct testing and assessments of the App and data store to ensure security arrangements are in place and evolving as required. Independent assurance from security experts was a recommendation in the [COVIDSafe Privacy Application Impact Assessment](#).

The ACSC has provided technical cyber security advice and assistance to the Digital Transformation Agency in relation to the security of COVIDSafe and its supporting infrastructure. This advice has been directed at ensuring that COVIDSafe is informed by best practice cyber security principles. The ACSC assesses that COVIDSafe uses and retains only that information necessary to support state and territory public health officials in their contact tracing efforts. COVIDSafe information is stored on mobile phones and in the National Data Store applying better practice encryption and security standards. Information on close contacts is shared with health authorities only after an individual has tested positive for COVID-19 and only after they have provided consent.

The Cyber Security Collaborative Research Centre has provided additional independent review of the COVIDSafe app, which informed ACSC advice to the Digital Transformation Agency.

A number of independent app developers and cyber security experts have provided assurance in relation to the security of COVIDSafe through review of the publicly available mobile application source code. This feedback was provided to the Digital Transformation Agency to inform later releases.

Other COVID-19 mobile services from Government

COVIDSafe is a separate app to the other Australian Government coronavirus apps. Its sole purpose is to improve the ability of state and territory health officials to quickly alert and contain COVID-19 outbreaks in the community.

COVIDSafe is an Australian Government initiative. Contact us if you need assistance: support@covidsafe.gov.au.

Coronavirus Australia app



[Coronavirus Australia](#) is an information service. The Government developed it to ensure the community has access to timely and accurate information about COVID-19.

Coronavirus Australia provides:

- up-to-date information and advice on the virus and Australia's efforts to combat it
- a snapshot of the current official COVID-19 status in Australia
- links to allow users to check symptoms if they are concerned about themselves or others
- relevant contact information
- notifications of urgent updates.

WhatsApp channel



The [Australian Government WhatsApp channel for COVID-19](#) is another way people can access information about COVID-19.

No other COVID-19 contact tracing apps



COVIDSafe is the only contact app that has been developed by the Australian Government Department of Health to ensure your information and privacy are protected.

Other contact apps do not have the support of the Australian Government.

QR code apps for states and territories



States and territories are requiring some businesses to collect personal information about customers and visitors to their premises. Many businesses are already using QR Code apps for this purpose.

The COVIDSafe app does not include QR functionality.

QR code apps assist businesses to comply with record keeping regarding who has attended their premises. The COVIDSafe app has a broader use in supporting the public health response to COVID-19 and in identifying unknown close contacts. The COVIDSafe app is not venue based and does not record location.

The COVIDSafe app and QR code apps are designed to complement the manual contact tracing processes undertaken by state and territory health officials.

The [Safe Work Australia website](#) has further information on what is required of business owners.

Amazon Web Services (AWS)

Amazon Web Services (AWS) has a contract with the Australian Government to provide a secure protected-level cloud service for the storage of encrypted information. Information is uploaded to this storage system once a COVIDSafe user has tested positive for COVID-19 and agreed to the information from the app on their phone being used.

Under the contract, AWS has no access to the encrypted information from COVIDSafe.

Reasons for choosing Amazon Web Services



The Australian Government's Digital Transformation Agency, who developed the COVIDSafe app, had existing contracts with Amazon Web Services (AWS). The Digital Transformation Agency made the COVIDSafe contract as a Statement of Work under the [Amazon Web Services \(AWS\) Whole of Government Arrangement – Standing Offer](#). The [Commonwealth Procurement Rules](#) allow a limited tender when there is:

- genuine urgency (rule 10.3.b)
- continuation of an existing agreement (rule 10.3.e).

The Statement of Work (ID number E104752985) required AWS to provide:

- Activity 1 – AWS Platform Design and Build
- Activity 2 – AWS Mobile Web App Build
- Activity 3 – AWS Admin App Build
- Activity 4 – AWS Project Control.

Using AWS provided the Digital Transformation Agency with hosting, development, and operational support services for COVIDSafe and the [National COVIDSafe Data Store](#). Splitting work packages into parts would have introduced more risk and complexity to the COVIDSafe system.

A change in supplier arrangements would have had risks the Digital Transformation Agency could not accept:

- the app may not have been delivered on time
- the cost would likely be higher, as the work already done by AWS may not have been transferrable to another supplier.

The contract between the Commonwealth and AWS specifies:

- the National COVIDSafe data storage system must use protected certified cloud services
- data held in the National COVIDSafe data storage system must be located in Australia.

While AWS host the data storage system, they do not have access to the [National COVIDSafe Data Store](#).

Information does not go overseas



It is a criminal offence to:

- hold COVIDSafe app information on a database outside Australia
- disclose COVIDSafe app information to a person in any country other than Australia
- use the information for any purpose other than state or territory public health officials undertaking contact tracing.

The Australian Government already uses AWS for many other purposes and requires them to keep Australian data in Australia.

More help for COVIDSafe

Read [Help topics](#) for more information, including:

- [Getting COVIDSafe on your phone](#)
- [Setting up COVIDSafe](#)
- [Battery life and mobile data](#)
- [Bluetooth® settings](#)
- [Removing COVIDSafe](#)
- [Meeting government standards for accessibility](#)
- [COVIDSafe source code](#).

COVIDSAFE

[Home](#) [About](#) [How it works](#) [Privacy policy](#) [Terms of use](#) [COVIDSafe source code](#)
[Help topics](#)

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-12

The following is the annexure marked **FT-12** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains screenshots of the UK-TCoP on the official website at <https://www.gov.uk/guidance/the-technology-code-of-practice>, accessed on 27 July 2026

.....
Daniel Davison
Solicitor

Guidance

The Technology Code of Practice

The Technology Code of Practice is a set of criteria to help government design, build and buy technology.

From: [Government Digital Service](#) and [Central Digital and Data Office](#)

Published: 14 July 2021

Last updated: 7 July 2025 — [See all updates](#)

 [Get emails about this page](#)

Contents

- [Spend controls](#)
- [1. Define user needs](#)
- [2. Make things accessible and inclusive](#)
- [3. Be open and use open source](#)
- [4. Make use of open standards](#)
- [5. Use cloud first](#)
- [6. Make things secure](#)
- [7. Make privacy integral](#)
- [8. Share, reuse and collaborate](#)
- [9. Integrate and adapt technology](#)
- [10. Make better use of data](#)
- [11. Define your purchasing strategy](#)
- [12. Make your technology sustainable](#)
- [13. Meet the Service Standard](#)
- [Contacts](#)

 [Print this page](#)

The Technology Code of Practice (TCoP) is a cross-government agreed standard used for the [Cabinet Office spend control process](#) and the [Local Digital Declaration](#).

You should use the TCoP for all of your technology projects or programmes. Consider each point, align your project or programme with the mandatory points, and follow as many of the remaining points as is practical. You'll get the most benefit by aligning your organisation's technology and business strategies to the Technology Code of Practice.

Each point contains guidance and links to case studies to help you migrate from legacy infrastructure and manage the full lifecycle of your technology.

Related content

Collection

[Cloud technology and the public sector](#)

Spend controls

Use the TCoP during the spend controls process

You must consider all points of the TCoP as part of the [Cabinet Office spend control process](#). If your project or programme needs spend control approval you should contact the GDS Assurance team at digital-spend-assurance@dsit.gov.uk for guidance with the approvals process.

Where legacy technology limits your ability to adhere to the TCoP, you must explain this to the GDS Assurance team.

1. Define user needs

Understand your users and their needs. Develop knowledge of your users and what that means for your technology project or programme.

[Read more about TCoP point 1 - Define user needs.](#)

2. Make things accessible and inclusive

Make sure your technology, infrastructure and systems are accessible and inclusive for all users.

[Read more about TCoP point 2 - Make things accessible.](#)

3. Be open and use open source

Publish your code and use open source software to improve transparency, flexibility and accountability.

[Read more about TCoP point 3 - Be open and use open source.](#)

4. Make use of open standards

Build technology that uses open standards to ensure your technology works and communicates with other technology, and can easily be upgraded and expanded.

[Read more about TCoP point 4 - Make use of open standards.](#)

5. Use cloud first

Consider using public cloud solutions first as stated in the Cloud First policy.

[Read more about TCoP point 5 - Use cloud first.](#)

6. Make things secure

Keep systems and data safe with the appropriate level of security.

[Read more about TCoP point 6 - Make things secure.](#)

7. Make privacy integral

Make sure users rights are protected by integrating privacy as an essential part of your system.

[Read more about TCoP point 7 - Make privacy integral.](#)

8. Share, reuse and collaborate

Avoid duplicating effort and unnecessary costs by collaborating across government and sharing and reusing technology, data, and services.

[Read more about TCoP point 8 - Share, reuse and collaborate.](#)

9. Integrate and adapt technology

Your technology should work with existing technologies, processes and infrastructure in your organisation, and adapt to future demands.

[Read more about TCoP point 9 - Integrate and adapt technology.](#)

10. Make better use of data

Use data more effectively by improving your technology, infrastructure and processes.

[Read more about TCoP point 10 - Make better use of data.](#)

11. Define your purchasing strategy

Your purchasing strategy must show you've considered commercial and technology aspects, and contractual limitations.

[Read more about TCoP point 11 - Define your purchasing strategy.](#)

12. Make your technology sustainable

Increase sustainability throughout the lifecycle of your technology.

[Read more about TCoP point 12 - Make your technology sustainable.](#)

13. Meet the Service Standard

If you're building a service as part of your technology project or programme you will also need to meet the [Service Standard](#)

Contacts

Who to contact for help

GDS Assurance team

digital-spend-assurance@dsit.gov.uk

You can email for help with:

- implementing the Technology Code of Practice
- designing an appropriate strategy for breaking up large systems and services
- evaluating the maturity of the technology market you want to buy from
- identifying opportunities to use common government platforms and components

Crown Commercial Service

info@crowncommercial.gov.uk

You can email for help with buying commodity services through procurement frameworks.

Published 14 July 2021

Last updated 7 July 2025 — [Show all updates](#)



Get emails about this page



Print this page

[↑ Contents](#)

Explore the topic

[Digital accessibility](#)

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-13

The following is the annexure marked **FT-13** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains screenshots of the 'Making source code open and reusable' guidance document accessed on 27 July 2026 at

<https://www.gov.uk/service-manual/technology/making-source-code-open-and-reusable>.

.....
Daniel Davison
Solicitor

Technology

Making source code open and reusable

From: [Technology community \(technical architecture\)](#)

[Give feedback about this page](#)

Contents

- [Making the code open](#)
- [Make your code open from the start](#)
- [How to make existing code open](#)
- [When it's acceptable for code to be closed source](#)
- [You must not store secret keys or credentials in the source code](#)
- [Making configuration code open](#)
- [Making code with a security-enforcing function open](#)
- [Licensing your code](#)
- [Taking responsibility for open source code](#)
- [Tracking changes to your code](#)
- [Dealing with security issues in published code](#)
- [Related guides](#)

When you create new source code, you must make it open so that other developers (including those outside government) can:

- benefit from your work and build on it
- learn from your experiences
- find uses for your code which you had not found

Making the code open

You should make your code publicly available in an open internet source code repository. For example, the Government Digital Service's (GDS's) code is on [GitHub](#). This includes code developed for you by a third party, such as a development agency.

When publishing your code you need to make sure:

- you're clear about who owns the code and how others can use it
- you do not release information that should remain closed - [see when code should be open or closed](#)
- you store it in a repository managed by your department
- any third-party tools you use to host or manage your code follow the National Cyber Security Centre's [cloud security guidance](#)

Make your code open from the start

It's much easier to [write your code in the open](#) from the beginning of a project than it is to open an existing repository later. This is because you can address security and other issues as you go along.

If you do not do this, you'll have to spend a costly period of time at the end of the project checking your code is safe to be released.

Coding in the open from the start means you can:

- plan how you'll avoid publishing sensitive information later in the project
- follow best practices from the beginning, for example keeping good documentation
- set in place processes that will allow you to continuously publish code as it is written
- allow others to identify parts of your code for reuse which you might not have recognised yourself
- allow others to contribute ideas as the project is in progress; for example if they know of existing tools that could help

Contents

- [Making the code open](#)
- [Make your code open from the start](#)
- [How to make existing code open](#)
- [When it's acceptable for code to be closed source](#)
- [You must not store secret keys or credentials in the source code](#)
- [Making configuration code open](#)
- [Making code with a security-enforcing function open](#)
- [Licensing your code](#)
- [Taking responsibility for open source code](#)
- [Tracking changes to your code](#)
- [Dealing with security issues in published code](#)
- [Related guides](#)

How to make existing code open

When you're making existing code open, you must review the code to check for:

- security flaws
- inappropriate content, for example rude messages in comments
- good documentation, including [good commit messages](#)

You should make the code open while preserving the history as this provides [useful documentation](#). If this is not possible, you may release a snapshot, but this should be a last resort.

Once the code is open you should move to a model where you continue development on the open code, but if you plan to continue to develop your code in a closed way you must explain how you are going to keep the open code up to date.

When it's acceptable for code to be closed source

There are very few examples of code that must not be published in the open.

The main reason for code to be closed source is when it relates to policy that has not yet been announced. In this case, you must make the code open as soon as possible after the policy is published.

You may also need to keep some code closed for security reasons, for example code that protects against fraud. Follow the guidance on [code you should keep closed](#) and [security considerations for open code](#).

You must not store secret keys or credentials in the source code

You must store secret keys and credentials separately, for example with a secret management system, and inject them into the code. This protects the keys from being accessed by unauthorised staff, and makes it easy to provision different keys for different environments and rotate keys if needed.

Making configuration code open

You should publish configuration code. For example, [GOV.UK's Puppet code](#) is coded in the open. However, if you publish the exact versions of software used in the stack, it can be easier for attackers to identify out of date software. Whether your code is open or closed, you must have a plan for how to upgrade or patch software you use.

Contents

- [Making the code open](#)
- [Make your code open from the start](#)
- [How to make existing code open](#)
- [When it's acceptable for code to be closed source](#)
- [You must not store secret keys or credentials in the source code](#)
- [Making configuration code open](#)
- [Making code with a security-enforcing function open](#)
- [Licensing your code](#)
- [Taking responsibility for open source code](#)
- [Tracking changes to your code](#)
- [Dealing with security issues in published code](#)
- [Related guides](#)

Making code with a security-enforcing function open

Code that contributes to your service's security does not need to be kept closed.

Many security-enforcing functions, such as cryptographic algorithms, are better when openly examined and understood while the keys are kept private.

Most cryptographic standards are developed in the open by standards authorities. UK public sector services use cryptographic security that's aligned with open, internationally recognised [standards and guidance from the National Cyber Security Centre](#).

Find out more about [security considerations for code that is open](#).

If you're not sure which parts of your code can be published in the open, talk to a third party that you trust. For example, a technical architect in your department or another government department.

You can find a technical architect by joining the [technical architecture community](#).

Licensing your code

You should publish your code under an [Open Source Initiative compatible licence](#). For example, GDS uses the [MIT licence](#).

All code produced by civil servants is automatically covered by [Crown Copyright](#).

Taking responsibility for open source code

When you make your code open, you should:

- [use Semantic Versioning](#) to make it clear when you release an update to your code
- be clear about how you'll communicate with users of your code, for example on support channels and email lists

Encouraging contributions from people who use your code can help make your code more robust, as people will spot bugs and suggest new features. If you would like to encourage contributions, you should:

- include contributing guidelines
- set time aside to maintain your code
- maintain a public issues list

You might also find it useful to read:

- [the GOV.UK Frontend contribution guidelines](#)
- [the GOV.UK style guide for pull requests](#)

Contents

- [Making the code open](#)
- [Make your code open from the start](#)
- [How to make existing code open](#)
- [When it's acceptable for code to be closed source](#)
- [You must not store secret keys or credentials in the source code](#)
- [Making configuration code open](#)
- [Making code with a security-enforcing function open](#)
- [Licensing your code](#)
- [Taking responsibility for open source code](#)
- [Tracking changes to your code](#)
- [Dealing with security issues in published code](#)
- [Related guides](#)

Tracking changes to your code

When your code is open, you must keep track of changes to it using [version control](#).

Services like [GitHub](#) make version control much easier. They allow you to track issues and read documentation alongside your code so you understand what has changed and why.

Dealing with security issues in published code

If you find a security issue in your code after you've published it, you need to be able to [deploy fixes quickly](#) without disclosing too much information about the vulnerability until you've dealt with it.

Fixing security issues in public copies of the code does not work for every team. It's possible to use scripts to switch between private and public copies of the code to manage fixes securely.

You should follow the specific security policies in your team or organisation as well as [general security best practices for dealing with vulnerabilities](#) quickly.

Related guides

You might also find these guides useful:

- [Maintaining version control in coding](#)
- [Deploying software regularly](#)

Published 26 August 2016

Last updated 5 October 2017 — [Show all updates](#)

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-14

The following is the annexure marked **FT-14** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains screenshots of the 'When code should be open or closed' guidance document accessed on 27 July 2026 at <https://www.gov.uk/government/publications/open-source-guidance/when-code-should-be-open-or-closed>.

.....
Daniel Davison
Solicitor



Government
Digital Service



Central Digital
& Data Office

Guidance

When code should be open or closed

Published 27 September 2017

Contents

[Closed code](#)

[Open code](#)



Print this page

You should open all new source code in accordance with [point 3 of the Technology Code of Practice](#).

There are grounds for keeping some code closed. This guide outlines what they are and why you should open configuration and security-enforcing code.

Closed code

You should keep some data and code closed, including:

- keys and credentials
- algorithms used to detect fraud
- unreleased policy

Keys and credentials

You must keep secret data such as keys or credentials closed, as this information could allow someone to gain access to your system.

You must keep code that uses secrets away from the secrets themselves. This includes storing secret keys and credentials separately. You can then open the code while keeping the secrets closed and secure.

For example, you can use a secret management system to store and secure your secrets, but allow applications to use them where necessary. A secret management system makes sure the keys can only be accessed by authorised staff. The system also makes it easier to provide different keys for different environments and rotate keys if needed.

Follow the [guidance on dealing with security vulnerabilities](#) if you accidentally expose a secret.

[Contents](#)

[Closed code](#)

[Open code](#)

 [Print this page](#)

Fraud detection algorithms

You should close any algorithms you use to detect fraud. You should also separate any code using them from the algorithms themselves. The separation will make it easier for you to update the algorithms as you learn more about the attempts to defraud your system.

The Service Manual provides further [guidance on protecting your service against fraud](#).

Unreleased policy

If the code makes clear details of a policy that has not yet been announced, you should keep the code closed until the policy is announced.

However, you must develop the code as if it's already open and continue to [follow good development](#) and [security practices](#). You must open the code as soon as possible after the policy is announced.

Open code

You should open all other code. This includes:

- configuration code
- database schema
- security-enforcing code

The Service Manual contains more [guidance on making code open and reusable](#).

Configuration code

You should open any [configuration code](#) as long as it does not contain keys or credentials. For example, the [GOV.UK Puppet code is open](#).

Whether your configuration code is open or closed, [you must keep your dependencies up to date](#). Potential attackers will know which vulnerabilities you are susceptible to if you do not update your dependencies. This applies even if your code is closed as there are many ways to find out what versions of dependencies you are using without access to the code.

The Service Manual has more [guidance on how to manage software dependencies](#).

Database schema

Unless your database schema contains credentials it is not sensitive and can be open. You should store any credentials separately and keep them closed.

Contents

[Closed code](#)

[Open code](#)

 [Print this page](#)

Security-enforcing code

You should open security-enforcing code. Open code can still be secure. For example, [Keycloak](#), a widely-used identity and access management solution, is Open Source and the [code is available on GitHub](#).

Most cryptographic standards are developed in the open by standards authorities. The US National Institute of Standards and Technology (NIST) concluded a [9-year process from open competition to standardisation](#) for the SHA-3 cryptographic hashing algorithm.

A good analogy is that of a padlock. Everyone knows how a padlock works, but it's still secure because you cannot open it without the key. [Security-enforcing software, such as RSA, works in the same way](#). Good cryptographic algorithms have been reviewed by many professional peers and prove their security through public review.

You should consider using a third-party library for authentication. A third-party library will be more secure and robust than one you might build yourself. It's still secure to open your code when you use a third-party authentication library.

If you're building a service and think your security-enforcing code needs to be closed, you'll have to explain why in your [service assessment](#).

You should also follow [security best practices when coding in the open](#).

[↑ Back to top](#)

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-15

The following is the annexure marked **FT-15** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains screenshots of the 'Security considerations when coding in the open' guidance document accessed on 27 July 2026 at <https://www.gov.uk/government/publications/open-source-guidance/security-considerations-when-coding-in-the-open>.

.....
Daniel Davison
Solicitor



Government
Digital Service



Central Digital
& Data Office

Guidance

Security considerations when coding in the open

Published 27 September 2017

Contents

[Open the code early](#)

[Don't rely on closed code as your only security measure](#)

[Follow good development practices](#)

[Keep keys and credentials closed](#)

[Assume accidental publications are compromised](#)

[Deal with security vulnerabilities](#)



[Print this page](#)

Coding in the open can [create better code, support collaboration, and increase engagement with your users](#).

You should follow the recommendations in this guide and [good security practices](#) to keep your open code secure.

Some code, such as keys and credentials, should be stored separately and remain closed. Follow the [guidance on when to keep code closed](#) if you are unsure what code to open.

Open the code early

You should code in the open from the beginning of your project rather than opening it later. By opening early, you can address security and other issues as you go along and introduce best practices from the start.

Don't rely on closed code as your only security measure

You should use multiple countermeasures to keep your system secure, known as the '[defence in depth](#)' approach. You should not rely on keeping code closed to keep it secure. This is known as [security through obscurity](#), which is considered insufficient by security experts.

Attackers can still learn many details about your code when it is closed. By keeping your code closed, you can also introduce other risks and complications including:

- deprioritisation of code review
- additional costs and complexity of access controls

The technology team at the Ministry of Justice has [explained how it has considered the risks of keeping code closed and why it works in the open](#).

Open code can be just as secure or more secure than closed code. For example, cryptographic algorithms are open and prove their robustness through peer review. You should consider [which code should be opened](#).

Contents

[Open the code early](#)

[Don't rely on closed code as your only security measure](#)

[Follow good development practices](#)

[Keep keys and credentials closed](#)

[Assume accidental publications are compromised](#)

[Deal with security vulnerabilities](#)



[Print this page](#)

Follow good development practices

Good development practices are important when coding in the open. For example, using clear [commit messages](#) and [comprehensive documentation](#) is always important, but becomes more so if people external to your team or organisation will be reading or using the code.

You should review your code to make sure any changes do not introduce security vulnerabilities. For example, GDS teams review code via pull requests and have [documented the review process in a coding style guide](#). Code reviews also help to catch bugs and reduce the risk of committing sensitive data. It's even more important to ensure code reviews are taking place when the code is open.

You must keep your dependencies up to date and have a mechanism for making changes quickly if you need to deal with a mistake or security issue. The Service Manual has more guidance on [managing dependencies](#) and [deploying software regularly](#).

When reviewing code, you should use automated tests and [style enforcement](#).

You could also use security scanning tools. For example, a static analysis tool such as [Brakeman](#).

You can also use tools to attempt to catch accidental disclosure of sensitive data. For example, you can use tools such as:

- [GitRob](#) to review code at a single point in time
- [Talisman](#) to review changes before they are committed

These tools should supplement your manual code review process and not replace it. Be aware the tools can alert mistakenly, known as 'false positives', which need careful management.

Keep keys and credentials closed

You must keep secret data such as keys or credentials closed.

[Read more about how to decide what code must be kept closed](#)

Assume accidental publications are compromised

If you accidentally publish a secret, you must revoke it and immediately provision new keys to the system. Once a secret has been published, you must assume that it is compromised no matter how quickly you are able to remove it as attackers have automated scanning tools that will pick up credential leaks immediately.

This means you must make sure that your system allows for keys and credentials to be changed and rotated easily, and for secrets to be revoked.

Contents

[Open the code early](#)

[Don't rely on closed code as your only security measure](#)

[Follow good development practices](#)

[Keep keys and credentials closed](#)

[Assume accidental publications are compromised](#)

[Deal with security vulnerabilities](#)



[Print this page](#)

Deal with security vulnerabilities

If you identify a vulnerability, you should follow the specific security and mitigation policies in your team or organisation. However, you should also follow general practices for dealing with the issue quickly.

If you discover a vulnerability as part of your usual development and test cycle, or it was reported to you through a private vulnerability disclosure process, the risk of attack is low. You should deal with the vulnerability as a normal bugfix cycle, and release after the code is committed.

If someone has publicly disclosed the vulnerability, you should consider whether you need to make an emergency fix. You should also review the vulnerable parts of the system to check for inconsistencies to determine whether the vulnerability has been exploited.

If you're given private information about a vulnerability that affects others, it might be appropriate to make the fix privately, deploy from a private repository and merge back into the public one when safe to do so. This will avoid putting other teams or systems at risk by leaking the information before it is made public.

You should never close an open repository. Once the code is public, it's likely that users will make their own copies. By closing the code, you may draw attention to the issue and it may not be resolved as quickly.

[↑ Back to top](#)

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-16

The following is the annexure marked **FT-16** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains screenshots of the UK Ministry of Justice 'Why we code in the open' article accessed on 27 July 2026 at

<https://mojdigital.blog.gov.uk/2017/02/21/why-we-code-in-the-open/>.

.....
Daniel Davison
Solicitor

[Blog](#)

Justice Digital, Data and Science

Search blog

Organisations: [Ministry of Justice](#)

This blog post was published under the 2015-2024 Conservative Administration

Why we code in the open

[Dave Rogers](#) and [Steve Marshall](#), 21 February 2017 - [Our services](#)

At the Ministry of Justice, we code in the open, by default. This means whenever we write software, we make [our source code available to anyone and everyone](#).

We are strong advocates of [point 8 of the Digital by Default Service Standard](#):

Make all new source code open and reusable, and publish it under appropriate licences (or provide a convincing explanation as to why this can't be done for specific subsets of the source code).

So our teams have to make a case for not making their code freely available. This approach has resulted in us writing [tens of millions of lines of code, in hundreds of code repositories](#), in the open since 2012.

This is not only the code for our front end systems, but includes the code for our:

- back-end systems
- data handling systems
- services for staff and
- sometimes our security-enforcing systems.

Encouraging good discipline

We expect a high level of quality from all of our software developers, but we have found the quality of code and commit messages is higher when developers are working 'in the open'.

We think this is caused by a developer's contribution being seen by other developers both inside and outside the MoJ. This is a commonly identified psychological effect about the improvement of human behaviour when [we believe we are being observed](#).

Justice Digital

A blog about using digital and technology to transform services in the justice system.

[More about Justice Digital](#)

[Working at Justice Digital](#)

Follow us

[Justice Digital on Twitter](#)

[Justice Digital on LinkedIn](#)

We are hiring
Come and join us >

Categories

Sign up and manage updates

[Email](#)

[Atom](#)

Our Vulnerability Disclosure Policy

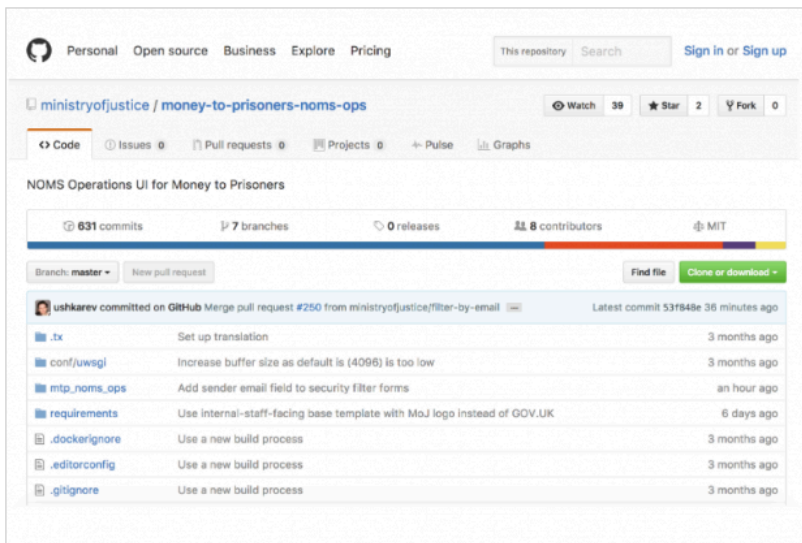
[How we work with the security research community to improve our online security](#)

Increased sharing and collaboration

Coding in the open means people outside our team can use it, and even help to improve it.

When we built [Send Money to a Prisoner](#) it was coded in the open and allowed people outside of government to [add support for different versions of Python](#) (the programming language we built the tools in) and [improve the tools' integrity checks](#).

This made the tool better for us, and more usable for people outside our teams.



It helps us hire great people

Our public code repository is an important part of our recruitment strategy.

Many people who have joined [our team](#) have told us that what they saw in our code repositories was part of attracting them to the role. They can easily see the quality and style of code we produce, the types of technologies we work with, and the kinds of services we deliver.

It's more important to secure data than code

Building technology and making it secure costs money. Whether it's simply the time people spend discussing it, or in the security features or components used.

Keeping code confidential can be complex, leading to additional cost and leaving less money available to use securing the data the service handles.

Open code builds trust in government

Transparency and freedom of information are important priorities at the Ministry of Justice. So being more open about our code, and the processes which lead to coding decisions, are vital parts of building trust in government.

Keeping things confidential

Sometimes software will need to be confidential because it's commercially sensitive or waiting for organisation approval. In most cases it will only need to be confidential temporarily, so we try to make the code open as soon as possible.

A good example of this process is explained [by GDS when opening up the Register to Vote codebase](#).

Doesn't it give attackers an advantage?

Although there's a common concern that coding in the open could give an advantage to an attacker, we believe that only a negligible advantage exists.

In fact there is no evidence to suggest that being open source makes software more susceptible to exploitation.

For example, publishing code in the open, especially when using good security discipline, is no riskier than closed source software where the binaries (the executable version of the source code) are public.

Lots of closed source software such as components, libraries and operating systems can be disassembled to reveal a similar level of detail to source code.

If you look at all the bugs in closed source products, the people that find the bugs don't have the source, they have [disassembly tools], it's out there and it's going to work on open and closed source binaries — get over it.

—Dr. Ian Levy, Technical Director, [NCSC](#), in [an interview with ZDNet](#) in 2013

So how secure is coding in the open?

In the past, there's been a misconception that openly sharing code presents security risks. However, we believe that can be avoided by following best practice, and keeping code separate from configuration and data.

Make things open: it makes them better

As the [tenth GDS design principle](#) says, the more eyes there are on something, the better it gets.

Making our code open makes it more usable, more secure and more accountable.

Would you like to work on things that matter? Find out more about working at [MoJ Digital & Technology](#).

[Subscribe to the blog](#) for updates on our work or follow us on [Twitter](#).

Tags: [coding](#), [open source](#)

← [Family separation: what's GOV got to do with it?](#)

[Working here is quite addictive ...](#) →

Share this page

[X \(formerly Twitter\)](#) [Facebook](#) [LinkedIn](#) [Email](#)



[All GOV.UK blogs](#) [All GOV.UK blog posts](#) [GOV.UK](#) [All departments](#)
[Accessibility statement](#) [Cookies](#)

OGL

All content is available under the [Open Government Licence v3.0](#), except where otherwise stated



© Crown copyright

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-17

The following is the annexure marked **FT-17** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains the official English language version of Regulation (EU) 910/2014, accessed on 27 July 2026 at

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910>.

.....
Daniel Davison
Solicitor

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 23 July 2014
on electronic identification and trust services for electronic transactions in the internal market and
repealing Directive 1999/93/EC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ⁽¹⁾,

Acting in accordance with the ordinary legislative procedure ⁽²⁾,

Whereas:

- (1) Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.
- (2) This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.
- (3) Directive 1999/93/EC of the European Parliament and of the Council ⁽³⁾, dealt with electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. This Regulation enhances and expands the *acquis* of that Directive.
- (4) The Commission communication of 26 August 2010 entitled 'A Digital Agenda for Europe' identified the fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as major obstacles to the virtuous cycle of the digital economy. In its EU Citizenship Report 2010, entitled 'Dismantling the obstacles to EU citizens' rights', the Commission further highlighted the need to solve the main problems that prevent Union citizens from enjoying the benefits of a digital single market and cross-border digital services.
- (5) In its conclusions of 4 February 2011 and of 23 October 2011, the European Council invited the Commission to create a digital single market by 2015, to make rapid progress in key areas of the digital economy and to promote a fully integrated digital single market by facilitating the cross-border use of online services, with particular attention to facilitating secure electronic identification and authentication.

⁽¹⁾ OJ C 351, 15.11.2012, p. 73.

⁽²⁾ Position of the European Parliament of 3 April 2014 (not yet published in the Official Journal) and decision of the Council of 23 July 2014.

⁽³⁾ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, p. 12).

- (6) In its conclusions of 27 May 2011, the Council invited the Commission to contribute to the digital single market by creating appropriate conditions for the mutual recognition of key enablers across borders, such as electronic identification, electronic documents, electronic signatures and electronic delivery services, and for interoperable e-government services across the European Union.
- (7) The European Parliament, in its resolution of 21 September 2010 on completing the internal market for e-commerce ⁽¹⁾, stressed the importance of the security of electronic services, especially of electronic signatures, and of the need to create a public key infrastructure at pan-European level, and called on the Commission to set up a European validation authorities gateway to ensure the cross-border interoperability of electronic signatures and to increase the security of transactions carried out using the internet.
- (8) Directive 2006/123/EC of the European Parliament and of the Council ⁽²⁾ requires Member States to establish 'points of single contact' (PSCs) to ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof can be easily completed, at a distance and by electronic means, through the appropriate PSC with the appropriate authorities. Many online services accessible through PSCs require electronic identification, authentication and signature.
- (9) In most cases, citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognised in other Member States. That electronic barrier excludes service providers from enjoying the full benefits of the internal market. Mutually recognised electronic identification means will facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities.
- (10) Directive 2011/24/EU of the European Parliament and of the Council ⁽³⁾ set up a network of national authorities responsible for e-health. To enhance the safety and the continuity of cross-border healthcare, the network is required to produce guidelines on cross-border access to electronic health data and services, including by supporting 'common identification and authentication measures to facilitate transferability of data in cross-border healthcare'. Mutual recognition of electronic identification and authentication is key to making cross-border healthcare for European citizens a reality. When people travel for treatment, their medical data need to be accessible in the country of treatment. That requires a solid, safe and trusted electronic identification framework.
- (11) This Regulation should be applied in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC of the European Parliament and of the Council ⁽⁴⁾. In this respect, having regard to the principle of mutual recognition established by this Regulation, authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online. Furthermore, requirements under Directive 95/46/EC concerning confidentiality and security of processing should be respected by trust service providers and supervisory bodies.
- (12) One of the objectives of this Regulation is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate, for at least public services. This Regulation does not aim to intervene with regard to electronic identity management systems and related infrastructures established in Member States. The aim of this Regulation is to ensure that for access to cross-border online services offered by Member States, secure electronic identification and authentication is possible.

⁽¹⁾ OJ C 50 E, 21.2.2012, p. 1.

⁽²⁾ Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (OJ L 376, 27.12.2006, p. 36).

⁽³⁾ Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

⁽⁴⁾ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

- (13) Member States should remain free to use or to introduce means for the purposes of electronic identification for accessing online services. They should also be able to decide whether to involve the private sector in the provision of those means. Member States should not be obliged to notify their electronic identification schemes to the Commission. The choice to notify the Commission of all, some or none of the electronic identification schemes used at national level to access at least public online services or specific services is up to Member States.
- (14) Some conditions need to be set out in this Regulation with regard to which electronic identification means have to be recognised and how the electronic identification schemes should be notified. Those conditions should help Member States to build the necessary trust in each other's electronic identification schemes and to mutually recognise electronic identification means falling under their notified schemes. The principle of mutual recognition should apply if the notifying Member State's electronic identification scheme meets the conditions of notification and the notification was published in the *Official Journal of the European Union*. However, the principle of mutual recognition should only relate to authentication for an online service. The access to those online services and their final delivery to the applicant should be closely linked to the right to receive such services under the conditions set out in national legislation.
- (15) The obligation to recognise electronic identification means should relate only to those means the identity assurance level of which corresponds to the level equal to or higher than the level required for the online service in question. In addition, that obligation should only apply when the public sector body in question uses the assurance level 'substantial' or 'high' in relation to accessing that service online. Member States should remain free, in accordance with Union law, to recognise electronic identification means having lower identity assurance levels.
- (16) Assurance levels should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned. The assurance level depends on the degree of confidence that electronic identification means provides in claimed or asserted identity of a person taking into account processes (for example, identity proofing and verification, and authentication), management activities (for example, the entity issuing electronic identification means and the procedure to issue such means) and technical controls implemented. Various technical definitions and descriptions of assurance levels exist as the result of Union-funded Large-Scale Pilots, standardisation and international activities. In particular, the Large-Scale Pilot STORK and ISO 29115 refer, inter alia, to levels 2, 3 and 4, which should be taken into utmost account in establishing minimum technical requirements, standards and procedures for the assurance levels low, substantial and high within the meaning of this Regulation, while ensuring consistent application of this Regulation in particular with regard to assurance level high related to identity proofing for issuing qualified certificates. The requirements established should be technology-neutral. It should be possible to achieve the necessary security requirements through different technologies.
- (17) Member States should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions. The possibility to use such electronic identification means would enable the private sector to rely on electronic identification and authentication already largely used in many Member States at least for public services and to make it easier for businesses and citizens to access their online services across borders. In order to facilitate the use of such electronic identification means across borders by the private sector, the authentication possibility provided by any Member State should be available to private sector relying parties established outside of the territory of that Member State under the same conditions as applied to private sector relying parties established within that Member State. Consequently, with regard to private sector relying parties, the notifying Member State may define terms of access to the authentication means. Such terms of access may inform whether the authentication means related to the notified scheme is presently available to private sector relying parties.
- (18) This Regulation should provide for the liability of the notifying Member State, the party issuing the electronic identification means and the party operating the authentication procedure for failure to comply with the relevant obligations under this Regulation. However, this Regulation should be applied in accordance with national rules on liability. Therefore, it does not affect those national rules on, for example, definition of damages or relevant applicable procedural rules, including the burden of proof.

- (19) The security of electronic identification schemes is key to trustworthy cross-border mutual recognition of electronic identification means. In this context, Member States should cooperate with regard to the security and interoperability of the electronic identification schemes at Union level. Whenever electronic identification schemes require specific hardware or software to be used by relying parties at the national level, cross-border interoperability calls for those Member States not to impose such requirements and related costs on relying parties established outside of their territory. In that case appropriate solutions should be discussed and developed within the scope of the interoperability framework. Nevertheless technical requirements stemming from the inherent specifications of national electronic identification means and likely to affect the holders of such electronic means (e.g. smartcards), are unavoidable.
- (20) Cooperation by Member States should facilitate the technical interoperability of the notified electronic identification schemes with a view to fostering a high level of trust and security appropriate to the degree of risk. The exchange of information and the sharing of best practices between Member States with a view to their mutual recognition should help such cooperation.
- (21) This Regulation should also establish a general legal framework for the use of trust services. However, it should not create a general obligation to use them or to install an access point for all existing trust services. In particular, it should not cover the provision of services used exclusively within closed systems between a defined set of participants, which have no effect on third parties. For example, systems set up in businesses or public administrations to manage internal procedures making use of trust services should not be subject to the requirements of this Regulation. Only trust services provided to the public having effects on third parties should meet the requirements laid down in the Regulation. Neither should this Regulation cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form laid down by national or Union law. In addition, it should not affect national form requirements pertaining to public registers, in particular commercial and land registers.
- (22) In order to contribute to their general cross-border use, it should be possible to use trust services as evidence in legal proceedings in all Member States. It is for the national law to define the legal effect of trust services, except if otherwise provided in this Regulation.
- (23) To the extent that this Regulation creates an obligation to recognise a trust service, such a trust service may only be rejected if the addressee of the obligation is unable to read or verify it due to technical reasons lying outside the immediate control of the addressee. However, that obligation should not in itself require a public body to obtain the hardware and software necessary for the technical readability of all existing trust services.
- (24) Member States may maintain or introduce national provisions, in conformity with Union law, relating to trust services as far as those services are not fully harmonised by this Regulation. However, trust services that comply with this Regulation should circulate freely in the internal market.
- (25) Member States should remain free to define other types of trust services in addition to those making part of the closed list of trust services provided for in this Regulation, for the purpose of recognition at national level as qualified trust services.
- (26) Because of the pace of technological change, this Regulation should adopt an approach which is open to innovation.
- (27) This Regulation should be technology-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met.

- (28) To enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, the notions of qualified trust services and qualified trust service provider should be introduced with a view to indicating requirements and obligations that ensure high-level security of whatever qualified trust services and products are used or provided.
- (29) In line with the obligations under the United Nations Convention on the Rights of Persons with Disabilities, approved by Council Decision 2010/48/EC ⁽¹⁾, in particular Article 9 of the Convention, persons with disabilities should be able to use trust services and end-user products used in the provision of those services on an equal basis with other consumers. Therefore, where feasible, trust services provided and end-user products used in the provision of those services should be made accessible for persons with disabilities. The feasibility assessment should include, inter alia, technical and economic considerations.
- (30) Member States should designate a supervisory body or supervisory bodies to carry out the supervisory activities under this Regulation. Member States should also be able to decide, upon a mutual agreement with another Member State, to designate a supervisory body in the territory of that other Member State.
- (31) Supervisory bodies should cooperate with data protection authorities, for example, by informing them about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached. The provision of information should in particular cover security incidents and personal data breaches.
- (32) It should be incumbent on all trust service providers to apply good security practice appropriate to the risks related to their activities so as to boost users' trust in the single market.
- (33) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Union or national law.
- (34) All Member States should follow common essential supervision requirements to ensure a comparable security level of qualified trust services. To ease the consistent application of those requirements across the Union, Member States should adopt comparable procedures and should exchange information on their supervision activities and best practices in the field.
- (35) All trust service providers should be subject to the requirements of this Regulation, in particular those on security and liability to ensure due diligence, transparency and accountability of their operations and services. However, taking into account the type of services provided by trust service providers, it is appropriate to distinguish as far as those requirements are concerned between qualified and non-qualified trust service providers.
- (36) Establishing a supervisory regime for all trust service providers should ensure a level playing field for the security and accountability of their operations and services, thus contributing to the protection of users and to the functioning of the internal market. Non-qualified trust service providers should be subject to a light touch and reactive *ex post* supervisory activities justified by the nature of their services and operations. The supervisory body should therefore have no general obligation to supervise non-qualified service providers. The supervisory body should only take action when it is informed (for example, by the non-qualified trust service provider itself, by another supervisory body, by a notification from a user or a business partner or on the basis of its own investigation) that a non-qualified trust service provider does not comply with the requirements of this Regulation.

⁽¹⁾ Council Decision 2010/48/EC of 26 November 2009 concerning the conclusion, by the European Community, of the United Nations Convention on the Rights of Persons with Disabilities (OJ L 23, 27.1.2010, p. 35).

- (37) This Regulation should provide for the liability of all trust service providers. In particular, it establishes the liability regime under which all trust service providers should be liable for damage caused to any natural or legal person due to failure to comply with the obligations under this Regulation. In order to facilitate the assessment of financial risk that trust service providers might have to bear or that they should cover by insurance policies, this Regulation allows trust service providers to set limitations, under certain conditions, on the use of the services they provide and not to be liable for damages arising from the use of services exceeding such limitations. Customers should be duly informed about the limitations in advance. Those limitations should be recognisable by a third party, for example by including information about the limitations in the terms and conditions of the service provided or through other recognisable means. For the purposes of giving effect to those principles, this Regulation should be applied in accordance with national rules on liability. Therefore, this Regulation does not affect those national rules on, for example, definition of damages, intention, negligence, or relevant applicable procedural rules.
- (38) Notification of security breaches and security risk assessments is essential with a view to providing adequate information to concerned parties in the event of a breach of security or loss of integrity.
- (39) To enable the Commission and the Member States to assess the effectiveness of the breach notification mechanism introduced by this Regulation, supervisory bodies should be requested to provide summary information to the Commission and to European Union Agency for Network and Information Security (ENISA).
- (40) To enable the Commission and the Member States to assess the effectiveness of the enhanced supervision mechanism introduced by this Regulation, supervisory bodies should be requested to report on their activities. This would be instrumental in facilitating the exchange of good practice between supervisory bodies and would ensure the verification of the consistent and efficient implementation of the essential supervision requirements in all Member States.
- (41) To ensure sustainability and durability of qualified trust services and to boost users' confidence in the continuity of qualified trust services, supervisory bodies should verify the existence and the correct application of provisions on termination plans in cases where qualified trust service providers cease their activities.
- (42) To facilitate the supervision of qualified trust service providers, for example, when a provider is providing its services in the territory of another Member State and is not subject to supervision there, or when the computers of a provider are located in the territory of a Member State other than the one where it is established, a mutual assistance system between supervisory bodies in the Member States should be established.
- (43) In order to ensure the compliance of qualified trust service providers and the services they provide with the requirements set out in this Regulation, a conformity assessment should be carried out by a conformity assessment body and the resulting conformity assessment reports should be submitted by the qualified trust service providers to the supervisory body. Whenever the supervisory body requires a qualified trust service provider to submit an ad hoc conformity assessment report, the supervisory body should respect, in particular, the principles of good administration, including the obligation to give reasons for its decisions, as well as the principle of proportionality. Therefore, the supervisory body should duly justify its decision to require an ad hoc conformity assessment.
- (44) This Regulation aims to ensure a coherent framework with a view to providing a high level of security and legal certainty of trust services. In this regard, when addressing the conformity assessment of products and services, the Commission should, where appropriate, seek synergies with existing relevant European and international schemes such as the Regulation (EC) No 765/2008 of the European Parliament and of the Council ⁽¹⁾ which sets out the requirements for accreditation of conformity assessment bodies and market surveillance of products.

⁽¹⁾ Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

- (45) In order to allow an efficient initiation process, which should lead to the inclusion of qualified trust service providers and the qualified trust services they provide into trusted lists, preliminary interactions between prospective qualified trust service providers and the competent supervisory body should be encouraged with a view to facilitating the due diligence leading to the provisioning of qualified trust services.
- (46) Trusted lists are essential elements in the building of trust among market operators as they indicate the qualified status of the service provider at the time of supervision.
- (47) Confidence in and convenience of online services are essential for users to fully benefit and consciously rely on electronic services. To this end, an EU trust mark should be created to identify the qualified trust services provided by qualified trust service providers. Such an EU trust mark for qualified trust services would clearly differentiate qualified trust services from other trust services thus contributing to transparency in the market. The use of an EU trust mark by qualified trust service providers should be voluntary and should not lead to any requirement other than those provided for in this Regulation.
- (48) While a high level of security is needed to ensure mutual recognition of electronic signatures, in specific cases, such as in the context of Commission Decision 2009/767/EC ⁽¹⁾, electronic signatures with a lower security assurance should also be accepted.
- (49) This Regulation should establish the principle that an electronic signature should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic signature. However, it is for national law to define the legal effect of electronic signatures, except for the requirements provided for in this Regulation according to which a qualified electronic signature should have the equivalent legal effect of a handwritten signature.
- (50) As competent authorities in the Member States currently use different formats of advanced electronic signatures to sign their documents electronically, it is necessary to ensure that at least a number of advanced electronic signature formats can be technically supported by Member States when they receive documents signed electronically. Similarly, when competent authorities in the Member States use advanced electronic seals, it would be necessary to ensure that they support at least a number of advanced electronic seal formats.
- (51) It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device.
- (52) The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply.

⁽¹⁾ Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (OJ L 274, 20.10.2009, p. 36).

- (53) The suspension of qualified certificates is an established operational practice of trust service providers in a number of Member States, which is different from revocation and entails the temporary loss of validity of a certificate. Legal certainty calls for the suspension status of a certificate to always be clearly indicated. To that end, trust service providers should have the responsibility to clearly indicate the status of the certificate and, if suspended, the precise period of time during which the certificate has been suspended. This Regulation should not impose the use of suspension on trust service providers or Member States, but should provide for transparency rules when and where such a practice is available.
- (54) Cross-border interoperability and recognition of qualified certificates is a precondition for cross-border recognition of qualified electronic signatures. Therefore, qualified certificates should not be subject to any mandatory requirements exceeding the requirements laid down in this Regulation. However, at national level, the inclusion of specific attributes, such as unique identifiers, in qualified certificates should be allowed, provided that such specific attributes do not hamper cross-border interoperability and recognition of qualified certificates and electronic signatures.
- (55) IT security certification based on international standards such as ISO 15408 and related evaluation methods and mutual recognition arrangements is an important tool for verifying the security of qualified electronic signature creation devices and should be promoted. However, innovative solutions and services such as mobile signing and cloud signing rely on technical and organisational solutions for qualified electronic signature creation devices for which security standards may not yet be available or for which the first IT security certification is ongoing. The level of security of such qualified electronic signature creation devices could be evaluated by using alternative processes only where such security standards are not available or where the first IT security certification is ongoing. Those processes should be comparable to the standards for IT security certification insofar as their security levels are equivalent. Those processes could be facilitated by a peer review.
- (56) This Regulation should lay down requirements for qualified electronic signature creation devices to ensure the functionality of advanced electronic signatures. This Regulation should not cover the entire system environment in which such devices operate. Therefore, the scope of the certification of qualified signature creation devices should be limited to the hardware and system software used to manage and protect the signature creation data created, stored or processed in the signature creation device. As detailed in relevant standards, the scope of the certification obligation should exclude signature creation applications.
- (57) To ensure legal certainty as regards the validity of the signature, it is essential to specify the components of a qualified electronic signature, which should be assessed by the relying party carrying out the validation. Moreover, specifying the requirements for qualified trust service providers that can provide a qualified validation service to relying parties unwilling or unable to carry out the validation of qualified electronic signatures themselves, should stimulate the private and public sector to invest in such services. Both elements should make qualified electronic signature validation easy and convenient for all parties at Union level.
- (58) When a transaction requires a qualified electronic seal from a legal person, a qualified electronic signature from the authorised representative of the legal person should be equally acceptable.
- (59) Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity.
- (60) Trust service providers issuing qualified certificates for electronic seals should implement the necessary measures in order to be able to establish the identity of the natural person representing the legal person to whom the qualified certificate for the electronic seal is provided, when such identification is necessary at national level in the context of judicial or administrative proceedings.

- (61) This Regulation should ensure the long-term preservation of information, in order to ensure the legal validity of electronic signatures and electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes.
- (62) In order to ensure the security of qualified electronic time stamps, this Regulation should require the use of an advanced electronic seal or an advanced electronic signature or of other equivalent methods. It is foreseeable that innovation may lead to new technologies that may ensure an equivalent level of security for time stamps. Whenever a method other than an advanced electronic seal or an advanced electronic signature is used, it should be up to the qualified trust service provider to demonstrate, in the conformity assessment report, that such a method ensures an equivalent level of security and complies with the obligations set out in this Regulation.
- (63) Electronic documents are important for further development of cross-border electronic transactions in the internal market. This Regulation should establish the principle that an electronic document should not be denied legal effect on the grounds that it is in an electronic form in order to ensure that an electronic transaction will not be rejected only on the grounds that a document is in electronic form.
- (64) When addressing formats of advanced electronic signatures and seals, the Commission should build on existing practices, standards and legislation, in particular Commission Decision 2011/130/EU ⁽¹⁾.
- (65) In addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers.
- (66) It is essential to provide for a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services. That framework could also open new market opportunities for Union trust service providers to offer new pan-European electronic registered delivery services.
- (67) Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated. The provision and the use of website authentication services are entirely voluntary. However, in order for website authentication to become a means to boosting trust, providing a better experience for the user and furthering growth in the internal market, this Regulation should lay down minimal security and liability obligations for the providers and their services. To that end, the results of existing industry-led initiatives, for example the Certification Authorities/Browsers Forum — CA/B Forum, have been taken into account. In addition, this Regulation should not impede the use of other means or methods to authenticate a website not falling under this Regulation nor should it prevent third country providers of website authentication services from providing their services to customers in the Union. However, a third country provider should only have its website authentication services recognised as qualified in accordance with this Regulation, if an international agreement between the Union and the country of establishment of the provider has been concluded.
- (68) The concept of 'legal persons', according to the provisions of the Treaty on the Functioning of the European Union (TFEU) on establishment, leaves operators free to choose the legal form which they deem suitable for carrying out their activity. Accordingly, 'legal persons', within the meaning of the TFEU, means all entities constituted under, or governed by, the law of a Member State, irrespective of their legal form.
- (69) The Union institutions, bodies, offices and agencies are encouraged to recognise electronic identification and trust services covered by this Regulation for the purpose of administrative cooperation capitalising, in particular, on existing good practices and the results of ongoing projects in the areas covered by this Regulation.

⁽¹⁾ Commission Decision 2011/130/EU of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (OJ L 53, 26.2.2011, p. 66).

- (70) In order to complement certain detailed technical aspects of this Regulation in a flexible and rapid manner, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of criteria to be met by the bodies responsible for the certification of qualified electronic signature creation devices. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.
- (71) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission, in particular for specifying reference numbers of standards the use of which would raise a presumption of compliance with certain requirements laid down in this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ⁽¹⁾.
- (72) When adopting delegated or implementing acts, the Commission should take due account of the standards and technical specifications drawn up by European and international standardisation organisations and bodies, in particular the European Committee for Standardisation (CEN), the European Telecommunications Standards Institute (ETSI), the International Organisation for Standardisation (ISO) and the International Telecommunication Union (ITU), with a view to ensuring a high level of security and interoperability of electronic identification and trust services.
- (73) For reasons of legal certainty and clarity, Directive 1999/93/EC should be repealed.
- (74) To ensure legal certainty for market operators already using qualified certificates issued to natural persons in compliance with Directive 1999/93/EC, it is necessary to provide for a sufficient period of time for transitional purposes. Similarly, transitional measures should be established for secure signature creation devices, the conformity of which has been determined in accordance with Directive 1999/93/EC, as well as for certification service providers issuing qualified certificates before 1 July 2016. Finally, it is also necessary to provide the Commission with the means to adopt the implementing acts and delegated acts before that date.
- (75) The application dates set out in this Regulation do not affect existing obligations that Member States already have under Union law, in particular under Directive 2006/123/EC.
- (76) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of the scale of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.
- (77) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council ⁽²⁾ and delivered an opinion on 27 September 2012 ⁽³⁾,

⁽¹⁾ Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

⁽²⁾ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

⁽³⁾ OJ C 28, 30.1.2013, p. 6.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services this Regulation:

- (a) lays down the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;
- (b) lays down rules for trust services, in particular for electronic transactions; and
- (c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

Article 2

Scope

1. This Regulation applies to electronic identification schemes that have been notified by a Member State, and to trust service providers that are established in the Union.
2. This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.
3. This Regulation does not affect national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form.

Article 3

Definitions

For the purposes of this Regulation, the following definitions apply:

- (1) 'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;
- (2) 'electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;
- (3) 'person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;
- (4) 'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;

- (5) 'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;
- (6) 'relying party' means a natural or legal person that relies upon an electronic identification or a trust service;
- (7) 'public sector body' means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;
- (8) 'body governed by public law' means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council ⁽¹⁾;
- (9) 'signatory' means a natural person who creates an electronic signature;
- (10) 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
- (11) 'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26;
- (12) 'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;
- (13) 'electronic signature creation data' means unique data which is used by the signatory to create an electronic signature;
- (14) 'certificate for electronic signature' means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;
- (15) 'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;
- (16) 'trust service' means an electronic service normally provided for remuneration which consists of:
- (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
 - (b) the creation, verification and validation of certificates for website authentication; or
 - (c) the preservation of electronic signatures, seals or certificates related to those services;
- (17) 'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation;

⁽¹⁾ Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).

- (18) 'conformity assessment body' means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;
- (19) 'trust service provider' means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;
- (20) 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;
- (21) 'product' means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services;
- (22) 'electronic signature creation device' means configured software or hardware used to create an electronic signature;
- (23) 'qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II;
- (24) 'creator of a seal' means a legal person who creates an electronic seal;
- (25) 'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;
- (26) 'advanced electronic seal' means an electronic seal, which meets the requirements set out in Article 36;
- (27) 'qualified electronic seal' means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;
- (28) 'electronic seal creation data' means unique data, which is used by the creator of the electronic seal to create an electronic seal;
- (29) 'certificate for electronic seal' means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;
- (30) 'qualified certificate for electronic seal' means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;
- (31) 'electronic seal creation device' means configured software or hardware used to create an electronic seal;
- (32) 'qualified electronic seal creation device' means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II;
- (33) 'electronic time stamp' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;
- (34) 'qualified electronic time stamp' means an electronic time stamp which meets the requirements laid down in Article 42;

- (35) 'electronic document' means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;
- (36) 'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;
- (37) 'qualified electronic registered delivery service' means an electronic registered delivery service which meets the requirements laid down in Article 44;
- (38) 'certificate for website authentication' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;
- (39) 'qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;
- (40) 'validation data' means data that is used to validate an electronic signature or an electronic seal;
- (41) 'validation' means the process of verifying and confirming that an electronic signature or a seal is valid.

Article 4

Internal market principle

1. There shall be no restriction on the provision of trust services in the territory of a Member State by a trust service provider established in another Member State for reasons that fall within the fields covered by this Regulation.
2. Products and trust services that comply with this Regulation shall be permitted to circulate freely in the internal market.

Article 5

Data processing and protection

1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC.
2. Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.

CHAPTER II

ELECTRONIC IDENTIFICATION

Article 6

Mutual recognition

1. When an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online, provided that the following conditions are met:
 - (a) the electronic identification means is issued under an electronic identification scheme that is included in the list published by the Commission pursuant to Article 9;

- (b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high;
- (c) the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online.

Such recognition shall take place no later than 12 months after the Commission publishes the list referred to in point (a) of the first subparagraph.

2. An electronic identification means which is issued under an electronic identification scheme included in the list published by the Commission pursuant to Article 9 and which corresponds to the assurance level low may be recognised by public sector bodies for the purposes of cross-border authentication for the service provided online by those bodies.

Article 7

Eligibility for notification of electronic identification schemes

An electronic identification scheme shall be eligible for notification pursuant to Article 9(1) provided that all of the following conditions are met:

- (a) the electronic identification means under the electronic identification scheme are issued:
 - (i) by the notifying Member State;
 - (ii) under a mandate from the notifying Member State; or
 - (iii) independently of the notifying Member State and are recognised by that Member State;
- (b) the electronic identification means under the electronic identification scheme can be used to access at least one service which is provided by a public sector body and which requires electronic identification in the notifying Member State;
- (c) the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the assurance levels set out in the implementing act referred to in Article 8(3);
- (d) the notifying Member State ensures that the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued;
- (e) the party issuing the electronic identification means under that scheme ensures that the electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3);
- (f) the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form.

For relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication. The cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body.

Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes;

- (g) at least six months prior to the notification pursuant to Article 9(1), the notifying Member State provides the other Member States for the purposes of the obligation under Article 12(5) a description of that scheme in accordance with the procedural arrangements established by the implementing acts referred to in Article 12(7);
- (h) the electronic identification scheme meets the requirements set out in the implementing act referred to in Article 12(8).

Article 8

Assurance levels of electronic identification schemes

1. An electronic identification scheme notified pursuant to Article 9(1) shall specify assurance levels low, substantial and/or high for electronic identification means issued under that scheme.
2. The assurance levels low, substantial and high shall meet respectively the following criteria:
 - (a) assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;
 - (b) assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;
 - (c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.
3. By 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means for the purposes of paragraph 1.

Those minimum technical specifications, standards and procedures shall be set out by reference to the reliability and quality of the following elements:

- (a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means;

- (b) the procedure for the issuance of the requested electronic identification means;
- (c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party;
- (d) the entity issuing the electronic identification means;
- (e) any other body involved in the application for the issuance of the electronic identification means; and
- (f) the technical and security specifications of the issued electronic identification means.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 9

Notification

1. The notifying Member State shall notify to the Commission the following information and, without undue delay, any subsequent changes thereto:

- (a) a description of the electronic identification scheme, including its assurance levels and the issuer or issuers of electronic identification means under the scheme;
- (b) the applicable supervisory regime and information on the liability regime with respect to the following:
 - (i) the party issuing the electronic identification means; and
 - (ii) the party operating the authentication procedure;
- (c) the authority or authorities responsible for the electronic identification scheme;
- (d) information on the entity or entities which manage the registration of the unique person identification data;
- (e) a description of how the requirements set out in the implementing acts referred to in Article 12(8) are met;
- (f) a description of the authentication referred to in point (f) of Article 7;
- (g) arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned.

2. One year from the date of application of the implementing acts referred to in Articles 8(3) and 12(8), the Commission shall publish in the *Official Journal of the European Union* a list of the electronic identification schemes which were notified pursuant to paragraph 1 of this Article and the basic information thereon.

3. If the Commission receives a notification after the expiry of the period referred to in paragraph 2, it shall publish in the *Official Journal of the European Union* the amendments to the list referred to in paragraph 2 within two months from the date of receipt of that notification.

4. A Member State may submit to the Commission a request to remove an electronic identification scheme notified by that Member State from the list referred to in paragraph 2. The Commission shall publish in the *Official Journal of the European Union* the corresponding amendments to the list within one month from the date of receipt of the Member State's request.

5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of notifications under paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 10

Security breach

1. Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.

2. When the breach or compromise referred to in paragraph 1 is remedied, the notifying Member State shall re-establish the cross-border authentication and shall inform other Member States and the Commission without undue delay.

3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme.

The Commission shall publish in the *Official Journal of the European Union* the corresponding amendments to the list referred to in Article 9(2) without undue delay.

Article 11

Liability

1. The notifying Member State shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations under points (d) and (f) of Article 7 in a cross-border transaction.

2. The party issuing the electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligation referred to in point (e) of Article 7 in a cross-border transaction.

3. The party operating the authentication procedure shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to ensure the correct operation of the authentication referred to in point (f) of Article 7 in a cross-border transaction.

4. Paragraphs 1, 2 and 3 shall be applied in accordance with national rules on liability.

5. Paragraphs 1, 2 and 3 are without prejudice to the liability under national law of parties to a transaction in which electronic identification means falling under the electronic identification scheme notified pursuant to Article 9(1) are used.

Article 12

Cooperation and interoperability

1. The national electronic identification schemes notified pursuant to Article 9(1) shall be interoperable.

2. For the purposes of paragraph 1, an interoperability framework shall be established.

3. The interoperability framework shall meet the following criteria:

- (a) it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State;
- (b) it follows European and international standards, where possible;
- (c) it facilitates the implementation of the principle of privacy by design; and
- (d) it ensures that personal data is processed in accordance with Directive 95/46/EC.

4. The interoperability framework shall consist of:

- (a) a reference to minimum technical requirements related to the assurance levels under Article 8;
- (b) a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8;
- (c) a reference to minimum technical requirements for interoperability;
- (d) a reference to a minimum set of person identification data uniquely representing a natural or legal person, which is available from electronic identification schemes;
- (e) rules of procedure;
- (f) arrangements for dispute resolution; and
- (g) common operational security standards.

5. Member States shall cooperate with regard to the following:

- (a) the interoperability of the electronic identification schemes notified pursuant to Article 9(1) and the electronic identification schemes which Member States intend to notify; and
- (b) the security of the electronic identification schemes.

6. The cooperation between Member States shall consist of:

- (a) the exchange of information, experience and good practice as regards electronic identification schemes and in particular technical requirements related to interoperability and assurance levels;
- (b) the exchange of information, experience and good practice as regards working with assurance levels of electronic identification schemes under Article 8;
- (c) peer review of electronic identification schemes falling under this Regulation; and
- (d) examination of relevant developments in the electronic identification sector.

7. By 18 March 2015, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in paragraphs 5 and 6 with a view to fostering a high level of trust and security appropriate to the degree of risk.

8. By 18 September 2015, for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1, the Commission shall, subject to the criteria set out in paragraph 3 and taking into account the results of the cooperation between Member States, adopt implementing acts on the interoperability framework as set out in paragraph 4.

9. The implementing acts referred to in paragraphs 7 and 8 of this Article shall be adopted in accordance with the examination procedure referred to in Article 48(2).

CHAPTER III

TRUST SERVICES

SECTION 1

General provisions

Article 13

Liability and burden of proof

1. Without prejudice to paragraph 2, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation.

The burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph.

The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.

2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.

3. Paragraphs 1 and 2 shall be applied in accordance with national rules on liability.

Article 14

International aspects

1. Trust services provided by trust service providers established in a third country shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU.

2. Agreements referred to in paragraph 1 shall ensure, in particular, that:
 - (a) the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country or international organisations with which the agreement is concluded, and by the trust services they provide;
 - (b) the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or international organisation with which the agreement is concluded.

Article 15

Accessibility for persons with disabilities

Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.

Article 16

Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Regulation. The penalties provided for shall be effective, proportionate and dissuasive.

SECTION 2

Supervision

Article 17

Supervisory body

1. Member States shall designate a supervisory body established in their territory or, upon mutual agreement with another Member State, a supervisory body established in that other Member State. That body shall be responsible for supervisory tasks in the designating Member State.

Supervisory bodies shall be given the necessary powers and adequate resources for the exercise of their tasks.

2. Member States shall notify to the Commission the names and the addresses of their respective designated supervisory bodies.

3. The role of the supervisory body shall be the following:

- (a) to supervise qualified trust service providers established in the territory of the designating Member State to ensure, through *ex ante* and *ex post* supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation;
- (b) to take action if necessary, in relation to non-qualified trust service providers established in the territory of the designating Member State, through *ex post* supervisory activities, when informed that those non-qualified trust service providers or the trust services they provide allegedly do not meet the requirements laid down in this Regulation.

4. For the purposes of paragraph 3 and subject to the limitations provided therein, the tasks of the supervisory body shall include in particular:

- (a) to cooperate with other supervisory bodies and provide them with assistance in accordance with Article 18;
- (b) to analyse the conformity assessment reports referred to in Articles 20(1) and 21(1);
- (c) to inform other supervisory bodies and the public about breaches of security or loss of integrity in accordance with Article 19(2);
- (d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article;
- (e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2);
- (f) to cooperate with the data protection authorities, in particular, by informing them without undue delay, about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached;
- (g) to grant qualified status to trust service providers and to the services they provide and to withdraw this status in accordance with Articles 20 and 21;
- (h) to inform the body responsible for the national trusted list referred to in Article 22(3) about its decisions to grant or to withdraw qualified status, unless that body is also the supervisory body;
- (i) to verify the existence and correct application of provisions on termination plans in cases where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with point (h) of Article 24(2);
- (j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation.

5. Member States may require the supervisory body to establish, maintain and update a trust infrastructure in accordance with the conditions under national law.

6. By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year's main activities together with a summary of breach notifications received from trust service providers in accordance with Article 19(2).

7. The Commission shall make the annual report referred to in paragraph 6 available to Member States.

8. The Commission may, by means of implementing acts, define the formats and procedures for the report referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

*Article 18***Mutual assistance**

1. Supervisory bodies shall cooperate with a view to exchanging good practice.

A supervisory body shall, upon receipt of a justified request from another supervisory body, provide that body with assistance so that the activities of supervisory bodies can be carried out in a consistent manner. Mutual assistance may cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21.

2. A supervisory body to which a request for assistance is addressed may refuse that request on any of the following grounds:

- (a) the supervisory body is not competent to provide the requested assistance;

- (b) the requested assistance is not proportionate to supervisory activities of the supervisory body carried out in accordance with Article 17;

- (c) providing the requested assistance would be incompatible with this Regulation.

3. Where appropriate, Member States may authorise their respective supervisory bodies to carry out joint investigations in which staff from other Member States' supervisory bodies is involved. The arrangements and procedures for such joint actions shall be agreed upon and established by the Member States concerned in accordance with their national law.

*Article 19***Security requirements applicable to trust service providers**

1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

2. Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.

The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest.

3. The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers.

4. The Commission may, by means of implementing acts,:

(a) further specify the measures referred to in paragraph 1; and

(b) define the formats and procedures, including deadlines, applicable for the purpose of paragraph 2.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 3

Qualified trust services

Article 20

Supervision of qualified trust service providers

1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.

2. Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall inform the data protection authorities of the results of its audits.

3. Where the supervisory body requires the qualified trust service provider to remedy any failure to fulfil requirements under this Regulation and where that provider does not act accordingly, and if applicable within a time limit set by the supervisory body, the supervisory body, taking into account, in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the affected service it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1). The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.

4. The Commission may, by means of implementing acts, establish reference number of the following standards:

(a) accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1;

(b) auditing rules under which conformity assessment bodies will carry out their conformity assessment of the qualified trust service providers as referred to in paragraph 1.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

*Article 21***Initiation of a qualified trust service**

1. Where trust service providers, without qualified status, intend to start providing qualified trust services, they shall submit to the supervisory body a notification of their intention together with a conformity assessment report issued by a conformity assessment body.

2. The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.

If the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements referred to in the first subparagraph, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article.

If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.

3. Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists referred to in Article 22(1).

4. The Commission may, by means of implementing acts, define the formats and procedures for the purpose of paragraphs 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

*Article 22***Trusted lists**

1. Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

2. Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing.

3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto.

4. The Commission shall make available to the public, through a secure channel, the information referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing.

5. By 18 September 2015 the Commission shall, by means of implementing acts, specify the information referred to in paragraph 1 and define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

*Article 23***EU trust mark for qualified trust services**

1. After the qualified status referred to in the second subparagraph of Article 21(2) has been indicated in the trusted list referred to in Article 22(1), qualified trust service providers may use the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide.
2. When using the EU trust mark for the qualified trust services referred to in paragraph 1, qualified trust service providers shall ensure that a link to the relevant trusted list is made available on their website.
3. By 1 July 2015 the Commission shall, by means of implementing acts, provide for specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

*Article 24***Requirements for qualified trust service providers**

1. When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.

The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:

- (a) by the physical presence of the natural person or of an authorised representative of the legal person; or
- (b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or
- (c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or
- (d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.

2. A qualified trust service provider providing qualified trust services shall:

- (a) inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities;
- (b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;
- (c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;

- (d) before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;
- (e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;
- (f) use trustworthy systems to store data provided to it, in a verifiable form so that:
 - (i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,
 - (ii) only authorised persons can make entries and changes to the stored data,
 - (iii) the data can be checked for authenticity;
- (g) take appropriate measures against forgery and theft of data;
- (h) record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;
- (i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);
- (j) ensure lawful processing of personal data in accordance with Directive 95/46/EC;
- (k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.

3. If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.

4. With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.

5. The Commission may, by means of implementing acts, establish reference numbers of standards for trustworthy systems and products, which comply with the requirements under points (e) and (f) of paragraph 2 of this Article. Compliance with the requirements laid down in this Article shall be presumed where trustworthy systems and products meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 4

Electronic signatures

Article 25

Legal effects of electronic signatures

1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.
2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.
3. A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.

Article 26

Requirements for advanced electronic signatures

An advanced electronic signature shall meet the following requirements:

- (a) it is uniquely linked to the signatory;
- (b) it is capable of identifying the signatory;
- (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
- (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Article 27

Electronic signatures in public services

1. If a Member State requires an advanced electronic signature to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures, advanced electronic signatures based on a qualified certificate for electronic signatures, and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.
2. If a Member State requires an advanced electronic signature based on a qualified certificate to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures based on a qualified certificate and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.
3. Member States shall not request for cross-border use in an online service offered by a public sector body an electronic signature at a higher security level than the qualified electronic signature.
4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic signatures. Compliance with the requirements for advanced electronic signatures referred to in paragraphs 1 and 2 of this Article and in Article 26 shall be presumed when an advanced electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

5. By 18 September 2015, and taking into account existing practices, standards and Union legal acts, the Commission shall, by means of implementing acts, define reference formats of advanced electronic signatures or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 28

Qualified certificates for electronic signatures

1. Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I.
2. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.
3. Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.
4. If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.
5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature:
 - (a) if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;
 - (b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.
6. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 29

Requirements for qualified electronic signature creation devices

1. Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.
2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 30

Certification of qualified electronic signature creation devices

1. Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.

2. Member States shall notify to the Commission the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.

3. The certification referred to in paragraph 1 shall be based on one of the following:

- (a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph; or
- (b) a process other than the process referred to in point (a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the Commission. That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing.

The Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1 of this Article.

Article 31

Publication of a list of certified qualified electronic signature creation devices

1. Member States shall notify to the Commission without undue delay and no later than one month after the certification is concluded, information on qualified electronic signature creation devices that have been certified by the bodies referred to in Article 30(1). They shall also notify to the Commission, without undue delay and no later than one month after the certification is cancelled, information on electronic signature creation devices that are no longer certified.

2. On the basis of the information received, the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices.

3. The Commission may, by means of implementing acts, define formats and procedures applicable for the purpose of paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 32

Requirements for the validation of qualified electronic signatures

1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:

- (a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;
- (b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;
- (c) the signature validation data corresponds to the data provided to the relying party;

- (d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;
- (e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;
- (f) the electronic signature was created by a qualified electronic signature creation device;
- (g) the integrity of the signed data has not been compromised;
- (h) the requirements provided for in Article 26 were met at the time of signing.

2. The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

3. The Commission may, by means of implementing acts, establish reference numbers of standards for the validation of qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation of qualified electronic signatures meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 33

Qualified validation service for qualified electronic signatures

1. A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who:

- (a) provides validation in compliance with Article 32(1); and
- (b) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified validation service referred to in paragraph 1. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation service for a qualified electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 34

Qualified preservation service for qualified electronic signatures

1. A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for the qualified preservation service for qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 5

Electronic seals

Article 35

Legal effects of electronic seals

1. An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.
2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.
3. A qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States.

Article 36

Requirements for advanced electronic seals

An advanced electronic seal shall meet the following requirements:

- (a) it is uniquely linked to the creator of the seal;
- (b) it is capable of identifying the creator of the seal;
- (c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and
- (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

Article 37

Electronic seals in public services

1. If a Member State requires an advanced electronic seal in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals, advanced electronic seals based on a qualified certificate for electronic seals and qualified electronic seals at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.
2. If a Member State requires an advanced electronic seal based on a qualified certificate in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals based on a qualified certificate and qualified electronic seal at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.
3. Member States shall not request for the cross-border use in an online service offered by a public sector body an electronic seal at a higher security level than the qualified electronic seal.
4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic seals. Compliance with the requirements for advanced electronic seals referred to in paragraphs 1 and 2 of this Article and Article 36 shall be presumed when an advanced electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

5. By 18 September 2015, and taking into account existing practices, standards and legal acts of the Union, the Commission shall, by means of implementing acts, define reference formats of advanced electronic seals or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 38

Qualified certificates for electronic seals

1. Qualified certificates for electronic seals shall meet the requirements laid down in Annex III.
2. Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.
3. Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic seals.
4. If a qualified certificate for an electronic seal has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.
5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of qualified certificates for electronic seals:
 - (a) if a qualified certificate for electronic seal has been temporarily suspended, that certificate shall lose its validity for the period of suspension;
 - (b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.
6. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic seals. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 39

Qualified electronic seal creation devices

1. Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.
2. Article 30 shall apply mutatis mutandis to the certification of qualified electronic seal creation devices.
3. Article 31 shall apply mutatis mutandis to the publication of a list of certified qualified electronic seal creation devices.

Article 40

Validation and preservation of qualified electronic seals

Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.

SECTION 6

Electronic time stamps

Article 41

Legal effect of electronic time stamps

1. An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.
2. A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.
3. A qualified electronic time stamp issued in one Member State shall be recognised as a qualified electronic time stamp in all Member States.

Article 42

Requirements for qualified electronic time stamps

1. A qualified electronic time stamp shall meet the following requirements:
 - (a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
 - (b) it is based on an accurate time source linked to Coordinated Universal Time; and
 - (c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.
2. The Commission may, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for accurate time sources. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accurate time source meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 7

Electronic registered delivery services

Article 43

Legal effect of an electronic registered delivery service

1. Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.
2. Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

*Article 44***Requirements for qualified electronic registered delivery services**

1. Qualified electronic registered delivery services shall meet the following requirements:
 - (a) they are provided by one or more qualified trust service provider(s);
 - (b) they ensure with a high level of confidence the identification of the sender;
 - (c) they ensure the identification of the addressee before the delivery of the data;
 - (d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;
 - (e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;
 - (f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.

In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

*SECTION 8***Website authentication***Article 45***Requirements for qualified certificates for website authentication**

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV.
2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for website authentication. Compliance with the requirements laid down in Annex IV shall be presumed where a qualified certificate for website authentication meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

*CHAPTER IV***ELECTRONIC DOCUMENTS***Article 46***Legal effects of electronic documents**

An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

CHAPTER V

DELEGATIONS OF POWER AND IMPLEMENTING PROVISIONS*Article 47***Exercise of the delegation**

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Article 30(4) shall be conferred on the Commission for an indeterminate period of time from 17 September 2014.
3. The delegation of power referred to in Article 30(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
5. A delegated act adopted pursuant to Article 30(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

*Article 48***Committee procedure**

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

CHAPTER VI

FINAL PROVISIONS*Article 49***Review**

The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council no later than 1 July 2020. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this Regulation or its specific provisions, including Article 6, point (f) of Article 7 and Articles 34, 43, 44 and 45, taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments.

The report referred to in the first paragraph shall be accompanied, where appropriate, by legislative proposals.

In addition, the Commission shall submit a report to the European Parliament and the Council every four years after the report referred to in the first paragraph on the progress towards achieving the objectives of this Regulation.

*Article 50***Repeal**

1. Directive 1999/93/EC is repealed with effect from 1 July 2016.
2. References to the repealed Directive shall be construed as references to this Regulation.

*Article 51***Transitional measures**

1. Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall be considered as qualified electronic signature creation devices under this Regulation.
2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall be considered as qualified certificates for electronic signatures under this Regulation until they expire.
3. A certification-service-provider issuing qualified certificates under Directive 1999/93/EC shall submit a conformity assessment report to the supervisory body as soon as possible but not later than 1 July 2017. Until the submission of such a conformity assessment report and the completion of its assessment by the supervisory body, that certification-service-provider shall be considered as qualified trust service provider under this Regulation.
4. If a certification-service-provider issuing qualified certificates under Directive 1999/93/EC does not submit a conformity assessment report to the supervisory body within the time limit referred to in paragraph 3, that certification-service-provider shall not be considered as qualified trust service provider under this Regulation from 2 July 2017.

*Article 52***Entry into force**

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.
2. This Regulation shall apply from 1 July 2016, except for the following:
 - (a) Articles 8(3), 9(5), 12(2) to (9), 17(8), 19(4), 20(4), 21(4), 22(5), 23(3), 24(5), 27(4) and (5), 28(6), 29(2), 30(3) and (4), 31(3), 32(3), 33(2), 34(2), 37(4) and (5), 38(6), 42(2), 44(2), 45(2), and Articles 47 and 48 shall apply from 17 September 2014;
 - (b) Article 7, Article 8(1) and (2), Articles 9, 10, 11 and Article 12(1) shall apply from the date of application of the implementing acts referred to in Articles 8(3) and 12(8);
 - (c) Article 6 shall apply from three years as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8).
3. Where the notified electronic identification scheme is included in the list published by the Commission pursuant to Article 9 before the date referred to in point (c) of paragraph 2 of this Article, the recognition of the electronic identification means under that scheme pursuant to Article 6 shall take place no later than 12 months after the publication of that scheme but not before the date referred to in point (c) of paragraph 2 of this Article.

4. Notwithstanding point (c) of paragraph 2 of this Article, a Member State may decide that electronic identification means under electronic identification scheme notified pursuant to Article 9(1) by another Member State are recognised in the first Member State as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8). Member States concerned shall inform the Commission. The Commission shall make this information public.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 23 July 2014.

For the Parliament

The President

M. SCHULZ

For the Council

The President

S. GOZI

ANNEX I

REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SIGNATURES

Qualified certificates for electronic signatures shall contain:

- (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;
- (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:
 - for a legal person: the name and, where applicable, registration number as stated in the official records,
 - for a natural person: the person's name;
- (c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;
- (d) electronic signature validation data that corresponds to the electronic signature creation data;
- (e) details of the beginning and end of the certificate's period of validity;
- (f) the certificate identity code, which must be unique for the qualified trust service provider;
- (g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
- (h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;
- (i) the location of the services that can be used to enquire about the validity status of the qualified certificate;
- (j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

ANNEX II

REQUIREMENTS FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES

1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:
 - (a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;
 - (b) the electronic signature creation data used for electronic signature creation can practically occur only once;
 - (c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;
 - (d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.
 2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.
 3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.
 4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:
 - (a) the security of the duplicated datasets must be at the same level as for the original datasets;
 - (b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.
-

ANNEX III

REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SEALS

Qualified certificates for electronic seals shall contain:

- (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal;
 - (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:
 - for a legal person: the name and, where applicable, registration number as stated in the official records,
 - for a natural person: the person's name;
 - (c) at least the name of the creator of the seal and, where applicable, registration number as stated in the official records;
 - (d) electronic seal validation data, which corresponds to the electronic seal creation data;
 - (e) details of the beginning and end of the certificate's period of validity;
 - (f) the certificate identity code, which must be unique for the qualified trust service provider;
 - (g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
 - (h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;
 - (i) the location of the services that can be used to enquire as to the validity status of the qualified certificate;
 - (j) where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing.
-

ANNEX IV

REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR WEBSITE AUTHENTICATION

Qualified certificates for website authentication shall contain:

- (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;
 - (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:
 - for a legal person: the name and, where applicable, registration number as stated in the official records,
 - for a natural person: the person's name;
 - (c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym. If a pseudonym is used, it shall be clearly indicated;

for legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records;
 - (d) elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;
 - (e) the domain name(s) operated by the natural or legal person to whom the certificate is issued;
 - (f) details of the beginning and end of the certificate's period of validity;
 - (g) the certificate identity code, which must be unique for the qualified trust service provider;
 - (h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
 - (i) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (h) is available free of charge;
 - (j) the location of the certificate validity status services that can be used to enquire as to the validity status of the qualified certificate.
-

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-18

The following is the annexure marked **FT-18** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains the official English language version of Regulation (EU) 2024/1183, accessed on 27 July 2026 at

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401183.

.....
Daniel Davison
Solicitor



2024/1183

30.4.2024

REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 11 April 2024

amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ⁽¹⁾,

Having regard to the opinion of the Committee of the Regions ⁽²⁾,

Acting in accordance with the ordinary legislative procedure ⁽³⁾,

Whereas:

- (1) The Commission Communication of 19 February 2020 entitled ‘Shaping Europe’s Digital Future’ announces a revision of Regulation (EU) No 910/2014 of the European Parliament and of the Council ⁽⁴⁾ to improve its effectiveness, extend its benefits to the private sector and promote trusted digital identities for all Europeans.
- (2) In its conclusions of 1-2 October 2020, the European Council called on the Commission to propose the development of a Union-wide framework for secure public electronic identification, including interoperable digital signatures, to provide people with control over their online identity and data as well as to enable access to public, private and cross-border digital services.
- (3) The Digital Decade Policy Programme 2030, established by Decision (EU) 2022/2481 of the European Parliament and of the Council ⁽⁵⁾, sets the objectives and digital targets of a Union framework which, by 2030, are intended to lead to wide deployment of a trusted, voluntary, user-controlled digital identity that is recognised throughout the Union and allows every user to control their data in online interactions.
- (4) The ‘European Declaration on Digital Rights and Principles for the Digital Decade’ proclaimed by the European Parliament, the Council and the Commission ⁽⁶⁾ (the ‘Declaration’), underlines everyone’s right to access digital technologies, products and services that are safe, secure, and privacy-protective by design. This includes ensuring that all people living in the Union are offered an accessible, secure and trusted digital identity that enables access to a broad range of online and offline services, protected against cybersecurity risks and cybercrime including data breaches and identity theft or manipulation. The Declaration also states that everyone has the right to the protection of their personal data. That right encompasses the control on how the data is used and with whom it is shared.

⁽¹⁾ OJ C 105, 4.3.2022, p. 81.

⁽²⁾ OJ C 61, 4.2.2022, p. 42.

⁽³⁾ Position of the European Parliament of 29 February 2024 (not yet published in the Official Journal) and decision of the Council of 26 March 2024.

⁽⁴⁾ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

⁽⁵⁾ Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (OJ L 323, 19.12.2022, p. 4).

⁽⁶⁾ OJ C 23, 23.1.2023, p. 1.

- (5) Union citizens and residents in the Union should have the right to a digital identity that is under their sole control and that enables them to exercise their rights in the digital environment and to participate in the digital economy. To achieve that aim, a European digital identity framework should be established allowing Union citizens and residents in the Union to access public and private online and offline services throughout the Union.
- (6) A harmonised digital identity framework should contribute to the creation of a more digitally integrated Union by reducing digital barriers between Member States and by empowering Union citizens and residents in the Union to enjoy the benefits of digitalisation, while increasing transparency and the protection of their rights.
- (7) A more harmonised approach to electronic identification should reduce the risks and costs of the current fragmentation due to the use of divergent national solutions or, in some Member States, the absence of such electronic identification solutions. Such an approach should strengthen the internal market by allowing Union citizens, residents in the Union, as defined by national law, and businesses to identify themselves and to provide authentication of their identity online and offline in a safe, trustworthy, user-friendly, convenient, accessible and harmonised way, across the Union. The European Digital Identity Wallet should provide natural and legal persons across the Union with a harmonised electronic identification means enabling authentication and the sharing of data linked to their identity. Everyone should be able to access public and private services securely, relying on an improved ecosystem for trust services and on verified proofs of identity and electronic attestations of attributes, such as academic qualifications, including university degrees, or other educational or professional entitlements. The European Digital Identity Framework is intended to achieve a shift from the reliance on national digital identity solutions only, to the provision of electronic attestations of attributes valid and legally recognised across the Union. Providers of electronic attestations of attributes should benefit from a clear and uniform set of rules, while public administrations should be able to rely on electronic documents in a given format.
- (8) Several Member States have implemented and use electronic identification means that are accepted by service providers in the Union. Additionally, investments have been made in both national and cross-border solutions on the basis of Regulation (EU) No 910/2014, including the interoperability of notified electronic identification schemes pursuant to that Regulation. In order to ensure the complementarity and fast adoption of European Digital Identity Wallets by current users of notified electronic identification means and to minimise the impact on existing service providers, European Digital Identity Wallets are expected to benefit from building on the experience gained with existing electronic identification means and from the infrastructure of notified electronic identification schemes deployed at Union and national level.
- (9) Regulation (EU) 2016/679 of the European Parliament and of the Council⁽⁷⁾ and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council⁽⁸⁾ apply to all personal data processing activities under Regulation (EU) No 910/2014. The solutions under the interoperability framework provided in this Regulation also comply with those rules. Union data protection law provides for data protection principles, such as the data minimisation and purpose limitation principle and obligations, such as data protection by design and by default.
- (10) To support the competitiveness of Union businesses, both online and offline service providers should be able to rely on digital identity solutions recognised across the Union, irrespective of the Member State in which those solutions are provided, thus benefiting from a harmonised Union approach to trust, security and interoperability. Both users and service providers should be able to benefit from the same legal value provided to electronic attestations of attributes across the Union. A harmonised digital identity framework is intended to create economic value by providing easier access to goods and services and by significantly reducing operational costs linked to electronic identification and authentication procedures, for instance during the onboarding of new customers, by reducing the potential for cybercrime, such as identity theft, data theft and online fraud, thus promoting efficiency gains and the secure digital transformation of the Union's micro, small and medium-sized enterprises (SMEs).

⁽⁷⁾ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

⁽⁸⁾ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

- (11) European Digital Identity Wallets should facilitate the application of the ‘once only’ principle, thus reducing the administrative burden on and supporting cross-border mobility of Union citizens and residents in the Union and businesses across the Union and fostering the development of interoperable e-government services across the Union.
- (12) Regulation (EU) 2016/679, Regulation (EU) 2018/1725 of the European Parliament and of the Council⁽⁹⁾ and Directive 2002/58/EC apply to the processing of personal data in the implementation of this Regulation. Therefore, this Regulation should lay down specific safeguards to prevent providers of electronic identification means and electronic attestation of attributes from combining personal data obtained when providing other services with the personal data processed to provide the services falling within the scope of this Regulation. Personal data related to the provision of European Digital Identity Wallets should be kept logically separate from any other data held by the provider of the European Digital Identity Wallet. This Regulation should not prevent providers of European Digital Identity Wallets from applying additional technical measures that contribute to the protection of personal data, such as physical separation of personal data related to the provision of European Digital Identity Wallets from any other data held by the provider. Without prejudice to Regulation (EU) 2016/679, this Regulation further specifies the application of principles of purpose limitation, data minimisation, and data protection by design and by default.
- (13) European Digital Identity Wallets should have the function of a common dashboard embedded into the design, in order to ensure a higher degree of transparency, privacy and control of the users over their personal data. That function should provide an easy, user-friendly interface with an overview of all relying parties with whom the user shares data, including attributes, and the type of data shared with each relying party. It should allow users to track all transactions executed through the European Digital Identity Wallet with at least the following data: the time and date of the transaction, the counterpart identification, the personal data requested and the data shared. That information should be stored even if the transaction was not concluded. It should not be possible to repudiate the authenticity of the information contained in the transaction history. Such a function should be active by default. It should allow users easily to request the immediate erasure by a relying party of personal data pursuant Article 17 of Regulation (EU) 2016/679 and easily to report the relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for personal data is received, directly via the European Digital Identity Wallet.
- (14) Member States should integrate different privacy-preserving technologies, such as zero knowledge proof, into the European Digital Identity Wallet. Those cryptographic methods should allow a relying party to validate whether a given statement based on the person’s identification data and attestation of attributes is true, without revealing any data on which that statement is based, thereby preserving the privacy of the user.
- (15) This Regulation sets out the harmonised conditions for the establishment of a framework for European Digital Identity Wallets to be provided by Member States. All Union citizens, and residents in the Union as defined by national law, should be empowered to securely request, select, combine, store, delete, share and present data related to their identity and request the erasure of their personal data in a user-friendly and convenient way, under the sole control of the user, while enabling selective disclosure of personal data. This Regulation reflects shared European values and respects fundamental rights, legal safeguards and liability, thus protecting democratic societies, Union citizens and residents in the Union. Technologies used to achieve those objectives should be developed aiming towards the highest level of security, privacy, user convenience, accessibility, wide usability and seamless interoperability. Member States should ensure equal access to electronic identification to all their citizens and residents. Member States should not, directly or indirectly, limit access to public or private services to natural or legal persons not opting to use European Digital Identity Wallets and should make available appropriate alternative solutions.

⁽⁹⁾ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

- (16) Member States should rely on the possibilities offered by this Regulation to provide, under their responsibility, European Digital Identity Wallets for use by the natural and legal persons residing on their territory. To offer Member States flexibility and leverage the state-of-the-art technology, this Regulation should enable provision of European Digital Identity Wallets directly by a Member State, under a mandate from a Member State, or independently of a Member State, but recognised by that Member State.
- (17) For the purposes of registration, relying parties should provide the information necessary to allow for their electronic identification and authentication towards European Digital Identity Wallets. When declaring their intended use of the European Digital Identity Wallet, relying parties should provide information regarding the data that they will request, if any, in order to provide their services and the reason for the request. Relying party registration facilitates the verification by Member States with regard to the lawfulness of the activities of the relying parties in accordance with Union law. The obligation to register provided for in this Regulation should be without prejudice to obligations laid down in other Union or national law, such as the information to be provided to the data subjects pursuant to the Regulation (EU) 2016/679. Relying parties should comply with the safeguards offered by Articles 35 and 36 of that Regulation, in particular by performing data protection impact assessments and by consulting the competent data protection authorities prior to data processing where data protection impact assessments indicate that the processing would result in a high risk. Such safeguards should support the lawful processing of personal data by relying parties, in particular with regard to special categories of data, such as health data. The registration of relying parties is intended to enhance transparency and trust in the use of European Digital Identity Wallets. Registration should be cost-effective and proportionate to the related risks in order to ensure uptake by service providers. In that context, registration should provide for the use of automated procedures, including the reliance on and the use of existing registers by Member States, and should not entail a pre-authorisation process. The registration process should enable a variety of use-cases that can differ in terms of mode of operation, whether online or in offline mode, or in terms of the requirement to authenticate devices for the purposes of interfacing with the European Digital Identity Wallet. Registration should apply exclusively to relying parties providing services by means of digital interaction.
- (18) Safeguarding Union citizens and residents in the Union against the unauthorised or fraudulent use of European Digital Identity Wallets is of high importance for ensuring trust in and for the wide uptake of European Digital Identity Wallets. Users should be provided with effective protection against such misuse. In particular, when facts that form the basis for fraudulent or otherwise illegal use of a European Digital Identity Wallet are established by a national judicial authority in the context of another procedure, supervisory bodies that are responsible for European Digital Identity Wallet issuers should, upon notification, take the necessary measures to ensure that the registration of the relying party and the inclusion of relying parties in the authentication mechanism are withdrawn or suspended until the notifying authority confirms that the irregularities identified have been remedied.
- (19) All European Digital Identity Wallets should enable users to electronically identify themselves and authenticate online and in offline mode across borders to access a wide range of public and private services. Without prejudice to Member States' prerogatives as regards the identification of their citizens and residents, European Digital Identity Wallets can also serve the institutional needs of public administrations, international organisations and the Union's institutions, bodies, offices and agencies. Authentication in offline mode would be important in many sectors, including in the health sector where services are often provided through face-to-face interaction and ePrescriptions should be able to rely on QR-codes or similar technologies to verify authenticity. Relying on the assurance level high with regard to electronic identification schemes European Digital Identity Wallets should benefit from the potential offered by tamper-proof solutions such as secure elements, to comply with the security requirements under this Regulation. European Digital Identity Wallets should also allow users to create and use qualified electronic signatures and seals which are accepted across the Union. Once on-boarded to a European Digital Identity Wallet, natural persons should be able to use it to sign with qualified electronic signatures, by default and free of charge, without having to go through any additional administrative procedures. Users should be able to sign or seal self-claimed assertions or attributes. To achieve simplification and cost-reduction benefits for persons and businesses across the Union, including by enabling powers of representation and e-mandates, Member States should provide European Digital Identity Wallets that rely on common standards and technical specifications to ensure seamless interoperability and to adequately increase IT security, strengthen robustness against cyber-attacks and thus significantly reduce the potential risks of ongoing digitalisation for Union citizens, residents in the Union and undertakings. Only Member States' competent authorities can provide a high level of confidence in establishing the

identity of a person and therefore provide assurance that the person claiming or asserting a particular identity is in fact the person he or she claims to be. It is therefore necessary for the provision of European Digital Identity Wallets to rely on the legal identity of Union citizens, residents in the Union or legal persons. Reliance on the legal identity should not hinder European Digital Identity Wallet users to access services under a pseudonym, where there is no legal requirement for legal identity for authentication. Trust in European Digital Identity Wallets would be enhanced if issuing and managing parties are required to implement appropriate technical and organisational measures to ensure the highest level of security that is commensurate to the risks raised for the rights and freedoms of the natural persons, in accordance with Regulation (EU) 2016/679.

- (20) The use of a qualified electronic signature should be free of charge to all natural persons for non-professional purposes. It should be possible for Member States to provide for measures to prevent the use of qualified electronic signatures for professional purposes by natural persons free-of-charge, while ensuring that any such measures are proportionate to identified risks and are justified.

- (21) It is beneficial to facilitate the uptake and use of European Digital Identity Wallets by seamlessly integrating them with the ecosystem of public and private digital services already implemented at national, local or regional level. To achieve that goal, it should be possible for Member States to provide for legal and organisational measures in order to increase flexibility for providers of European Digital Identity Wallets and to allow for additional functionalities of European Digital Identity Wallets to those provided for in this Regulation, including by enhanced interoperability with existing national electronic identification means. Such additional functionalities should by no means be to the detriment of providing core functions of European Digital Identity Wallets provided for in this Regulation or promote existing national solutions over European Digital Identity Wallets. Since they go beyond this Regulation, such additional functionalities do not benefit from the provisions on cross-border reliance on European Digital Identity Wallets set out in this Regulation.

- (22) European Digital Identity Wallets should include a functionality to generate user-chosen and managed pseudonyms, to authenticate when accessing online services.

- (23) In order to achieve a high level of security and trustworthiness, this Regulation establishes the requirements for European Digital Identity Wallets. The conformity of European Digital Identity Wallets with those requirements should be certified by accredited conformity assessment bodies designated by Member States.

- (24) In order to avoid divergent approaches and harmonise the implementation of the requirements laid down by this Regulation, the Commission should, for the purpose of certifying European Digital Identity Wallets, adopt implementing acts to establish a list of reference standards and, where necessary, to establish specifications and procedures for the purpose of expressing detailed technical specifications of those requirements. To the extent that the certification of the conformity of European Digital Identity Wallets with relevant cybersecurity requirements is not covered by existing cybersecurity certification schemes that are referred to in this Regulation, and as regards non-cybersecurity requirements relevant to European Digital Identity Wallets, Member States should establish national certification schemes pursuant to the harmonised requirements set out in and adopted pursuant to this Regulation. Member States should transmit their draft national certification schemes to the European Digital Identity Cooperation Group, which should be able to issue opinions and recommendations.

- (25) Certification of conformity with the cybersecurity requirements established in this Regulation should, where available, rely on the relevant European cybersecurity certifications schemes established pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council⁽¹⁰⁾, which establishes a voluntary European cybersecurity certification framework for ICT products, processes and services.

⁽¹⁰⁾ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

- (26) In order to continuously assess and mitigate risks linked to security, certified European Digital Identity Wallets should be subject to regular vulnerability assessments aiming to detect any vulnerability in the certified product-related components, certified process-related components and certified service-related components of the European Digital Identity Wallet.
- (27) By protecting users and companies from cybersecurity risks, the essential cybersecurity requirements laid down in this Regulation also contribute to enhancing the protection of personal data and privacy of individuals. Synergies on both standardisation and certification on cybersecurity aspects should be considered through the cooperation between the Commission, the European Standardisation Organizations, the European Union Agency for Cybersecurity (ENISA), the European Data Protection Board established by Regulation (EU) 2016/679 and the national data protection supervisory authorities.
- (28) The onboarding of Union citizens and residents in the Union to the European Digital Identity Wallet should be facilitated by relying on electronic identification means issued at assurance level high. Electronic identification means issued at assurance level substantial should be relied upon only where harmonised technical specifications and procedures using electronic identification means issued at assurance level substantial in combination with supplementary means of identity verification will allow the fulfilment of the requirements set out in this Regulation as regards assurance level high. Such supplementary means should be reliable and easy to use and could be built on the possibility to use remote onboarding procedures, qualified certificates supported by qualified electronic signatures, qualified electronic attestation of attributes or a combination thereof. To ensure sufficient uptake of European Digital Identity Wallets, harmonised technical specifications and procedures for the onboarding of users by using electronic identification means, including those issued at assurance level substantial, should be set out in implementing acts.
- (29) The objective of this Regulation is to provide the user with a fully mobile, secure and user-friendly European Digital Identity Wallet. As a transitional measure until the availability of certified tamper-proof solutions, such as secure elements within the users' devices, European Digital Identity Wallets should be able to rely upon certified external secure elements for the protection of the cryptographic material and other sensitive data or upon notified electronic identification means at assurance level high in order to demonstrate compliance with the relevant requirements of this Regulation as regards the assurance level of the European Digital Identity Wallet. This Regulation should be without prejudice to national conditions with regard to the issuance and use of a certified external secure element where the transitional measure is dependent on it.
- (30) European Digital Identity Wallets should ensure the highest level of data protection and security for the purposes of electronic identification and authentication to facilitate access to public and private services, irrespective of whether such data is stored locally or on cloud-based solutions, taking due account of the different levels of risk.
- (31) European Digital Identity Wallets should be secure-by-design and should implement advanced security features to protect against identity and other data theft, denial of service and any other cyber threat. Such security should include state-of-the-art encryption and storage methods that are accessible only to, and decryptable only by, the user and that rely on end-to-end encrypted communication with other European Digital Identity Wallets and relying parties. Additionally, European Digital Identity Wallets should require secure, explicit and active user confirmation for the operations performed via European Digital Identity Wallets.
- (32) The use, free of charge, of European Digital Identity Wallets should not result in the processing of data beyond data that is necessary for the provision of European Digital Identity Wallet services. This Regulation should not allow the processing of personal data stored in or resulting from the use of the European Digital Identity Wallet by the provider of the European Digital Identity Wallet for purposes other than the provision of European Digital Identity Wallet services. To ensure privacy, European Digital Identity Wallet providers should ensure unobservability by not collecting data and not having insight into the transactions of the users of the European Digital Identity Wallet. Such unobservability means that the providers are not able to see the details of the transactions made by the user. However, in specific cases, on the basis of explicit prior consent by the user in each of those specific cases, and fully in accordance with Regulation (EU) 2016/679, providers of European Digital Identity Wallets could be granted

access to the information necessary for the provision of a particular service related to European Digital Identity Wallets.

- (33) The transparency of European Digital Identity Wallets and the accountability of their providers are key elements to creating social trust and trigger acceptance of the framework. The functioning of European Digital Identity Wallets should therefore be transparent and, in particular, allow for verifiable processing of personal data. To achieve this, Member States should disclose the source code of the user application software components of European Digital Identity Wallets, including those that are related to processing of personal data and data of legal persons. The publication of this source code under an open-source licence should enable society, including users and developers, to understand its operation, audit and review the code. This would increase users' trust in the ecosystem and contribute to the security of European Digital Identity Wallets by enabling anyone to report vulnerabilities and errors in the code. Overall, this should provide suppliers with an incentive to deliver and maintain a highly secure product. However, in certain cases, the disclosure of the source code for the libraries used, communication channel or other elements that are not hosted on the user device, could be limited by Member States, for duly justified reasons, especially for the purpose of public security.
- (34) The use of European Digital Identity Wallets as well as the discontinuation of their use should be the exclusive right and choice of users. Member States should develop simple and secure procedures for the users to request immediate revocation of validity of European Digital Identity Wallets, including in the case of loss or theft. Upon the death of the user or the cessation of activity by a legal person, a mechanism should be established to enable the authority responsible for settling the succession of the natural person or assets of the legal person to request the immediate revocation of European Digital Identity Wallets.
- (35) In order to promote the uptake of European Digital Identity Wallets and the wider use of digital identities, Member States should not only promote the benefits of the relevant services, but should also, in cooperation with the private sector, researchers and academia, develop training programmes aiming to strengthen the digital skills of their citizens and residents, in particular for vulnerable groups such as persons with disabilities and older persons. Member States should also raise awareness of the benefits and risks of European Digital Identity Wallets by means of communication campaigns.
- (36) To ensure that the European Digital Identity Framework is open to innovation, technological development and future-proof, Member States are encouraged, jointly, to set up sandboxes to test innovative solutions in a controlled and secure environment in particular to improve the functionality, protection of personal data, security and interoperability of the solutions and to inform future updates of technical references and legal requirements. That environment should foster the inclusion of SMEs, start-ups and individual innovators and researchers, as well as relevant industry stakeholders. Such initiatives should contribute to and strengthen the regulatory compliance and technical robustness of European Digital Identity Wallets to be provided to Union citizens and residents in the Union, thus preventing the development of solutions that do not comply with Union law on data protection or that are open to security vulnerabilities.
- (37) Regulation (EU) 2019/1157 of the European Parliament and of the Council ⁽¹¹⁾ strengthens the security of identity cards with enhanced security features by August 2021. Member States should consider the feasibility of notifying them under electronic identification schemes to extend the cross-border availability of electronic identification means.
- (38) The process of notification of electronic identification schemes should be simplified and accelerated to promote access to convenient, trusted, secure and innovative authentication and identification solutions and, where relevant, to encourage private identity providers to offer electronic identification schemes to Member State's authorities for notification as national electronic identification schemes under Regulation (EU) No 910/2014.

⁽¹¹⁾ Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement (OJ L 188, 12.7.2019, p. 67).

- (39) Streamlining of the current notification and peer-review procedures will prevent heterogeneous approaches to the assessment of various notified electronic identification schemes and facilitate trust-building between Member States. New, simplified, mechanisms are intended to foster Member States' cooperation on the security and interoperability of their notified electronic identification schemes.
- (40) Member States should benefit from new, flexible tools to ensure compliance with the requirements of this Regulation and of the relevant implementing acts adopted pursuant thereto. This Regulation should allow Member States to use reports and assessments, performed by accredited conformity assessment bodies, as provided for in the context of certification schemes to be established at Union level under Regulation (EU) 2019/881, to support their claims on the alignment of the schemes or of parts thereof with Regulation (EU) No 910/2014.
- (41) Public service providers use the person identification data available from electronic identification means pursuant to Regulation (EU) No 910/2014 to match the electronic identity of the users from other Member States with the person identification data provided to those users in the Member State performing the cross-border identity matching process. However, in many cases, despite the use of the minimum data set provided under the notified electronic identification schemes, ensuring accurate identity matching when Member States act as relying parties requires additional information about the user and specific complementary unique identification procedures to be performed at national level. To further support the usability of electronic identification means, provide better online public services and increase legal certainty in relation to the electronic identity of the users, Regulation (EU) No 910/2014 should require Member States to take specific online measures to ensure unequivocal identity matching when users intend to access online cross-border public services.
- (42) When developing European Digital Identity Wallets, it is essential to take into consideration the needs of users. Meaningful use cases and online services relying on European Digital Identity Wallets should be available. For the convenience of users and in order to ensure cross-border availability of such services, it is important to undertake actions in order to facilitate a similar approach to design, development and implementation of online services in all Member States. Non-binding guidelines on how to design, develop and implement online services relying on European Digital Identity Wallets have the potential of becoming a useful tool to achieve that goal. Such guidelines should be prepared taking into account the interoperability framework of the Union. Member States should have a leading role when it comes to adopting those guidelines.
- (43) In accordance with Directive (EU) 2019/882 of the European Parliament and of the Council⁽¹²⁾, persons with disabilities should be able to use European Digital Identity Wallets, trust services and end-user products used in the provision of those services on an equal basis with other users.
- (44) In order to ensure effective enforcement of this Regulation, a minimum for the maximum of administrative fines for both qualified and non-qualified trust service providers should be established. Member States should provide for effective, proportionate and dissuasive penalties. When determining the penalties, the size of the affected entities, their business models and the severity of the infringements should be duly taken into consideration.
- (45) Member States should lay down rules on penalties for infringements such as direct or indirect practices leading to confusion between non-qualified and qualified trust services or to the abusive use of the EU trust mark by non-qualified trust service providers. The EU trust mark should not be used under conditions which, directly or indirectly, lead to the perception that any non-qualified trust services offered by those providers are qualified.
- (46) This Regulation should not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form laid down by Union or national law. In addition, it should not affect national form requirements pertaining to public registers, in particular commercial and land registers.

⁽¹²⁾ Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

- (47) The provision and use of trust services and the benefits brought in terms of convenience and legal certainty in the context of cross-border transactions, in particular when qualified trust services are used, are becoming increasingly important for international trade and cooperation. International partners of the Union are establishing trust frameworks inspired by Regulation (EU) No 910/2014. In order to facilitate the recognition of qualified trust services and of their providers, the Commission may adopt implementing acts to set the conditions under which trust frameworks of third countries could be considered equivalent to the trust framework for qualified trust services and providers thereof in this Regulation. Such an approach should complement the possibility for the mutual recognition of trust services and providers thereof established in the Union and in third countries in accordance with Article 218 of the Treaty on the Functioning of the European Union (TFEU). When setting out the conditions under which the trust frameworks of third countries could be considered to be equivalent to the trust framework for qualified trust services and providers thereof under Regulation (EU) No 910/2014, compliance with the relevant provisions in the Directive (EU) 2022/2555 of the European Parliament and of the Council⁽¹³⁾ and Regulation (EU) 2016/679 should be ensured, as well as the use of trusted lists as essential elements to build trust.
- (48) This Regulation should foster choice and the possibility of switching between European Digital Identity Wallets where a Member State has endorsed more than one European Digital Identity Wallet solution on its territory. In order to avoid lock-in effects in such situations, where technically feasible, the providers of European Digital Identity Wallets should ensure the effective portability of data at the request of European Digital Identity Wallet users, and should not be allowed to use contractual, economic or technical barriers to prevent or to discourage effective switching between different European Digital Identity Wallets.
- (49) To ensure the proper functioning of European Digital Identity Wallets, European Digital Identity Wallet providers need effective interoperability and fair, reasonable and non-discriminatory conditions for the European Digital Identity Wallets to access specific hardware and software features of mobile devices. Those components could include, in particular, near field communication antennas and secure elements, including universal integrated circuit cards, embedded secure elements, microSD cards and Bluetooth Low Energy. Access to those components could be under the control of mobile network operators and equipment manufacturers. Therefore, where needed to provide the services of European Digital Identity Wallets, original equipment manufacturers of mobile devices or providers of electronic communication services should not refuse access to such components. In addition, the undertakings that are designated as gatekeepers for core platform services as listed by the Commission pursuant to Regulation (EU) 2022/1925 of the European Parliament and of the Council⁽¹⁴⁾ should remain subject to the specific provisions of that Regulation, building on Article 6(7) thereof.
- (50) In order to streamline the cybersecurity obligations imposed on trust service providers, as well as to enable those providers and their respective competent authorities to benefit from the legal framework established by Directive (EU) 2022/2555, trust services are required to take appropriate technical and organisational measures pursuant to that Directive, such as measures addressing system failures, human error, malicious actions or natural phenomena in order to manage the risks posed to the security of network and information systems which those providers use in the provision of their services as well as to notify significant incidents and cyber threats in accordance with that Directive. With regard to the reporting of incidents, trust service providers should notify any incidents having a significant impact on the provision of their services, including such caused by theft or loss of devices, network cable damage or incidents that occur in the context of the identification of persons. The cybersecurity risk management requirements and reporting obligations under Directive (EU) 2022/2555 should be considered to be complementary to the requirements imposed on trust service providers under this Regulation. Where appropriate, established national practices or guidance in relation to the implementation of security and reporting requirements and supervision of compliance with such requirements under Regulation (EU) No 910/2014 should continue to be applied by the competent authorities designated under Directive (EU) 2022/2555. This Regulation does not affect the obligation to notify personal data breaches pursuant to Regulation (EU) 2016/679.

⁽¹³⁾ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

⁽¹⁴⁾ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, p. 1).

- (51) Due consideration should be given to ensure effective cooperation between the supervisory bodies designated pursuant to Article 46b of Regulation (EU) No 910/2014 and the competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555. Where such a supervisory body is different from such a competent authority, they should cooperate closely, in a timely manner by exchanging the relevant information in order to ensure effective supervision and compliance of trust service providers with the requirements set out in Regulation (EU) No 910/2014 and in Directive (EU) 2022/2555. In particular, supervisory bodies designated pursuant to Regulation (EU) No 910/2014 should be entitled to request competent authorities designated or established pursuant Directive (EU) 2022/2555 to provide relevant information needed to grant the qualified status and to carry out supervisory actions to verify compliance of the trust service providers with the relevant requirements under Directive (EU) 2022/2555 or to require them to remedy non-compliance.
- (52) It is essential to provide for a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services. That framework could also open new market opportunities for Union trust service providers to offer new Union-wide electronic registered delivery services. In order to ensure that data using a qualified electronic registered delivery service is delivered to the correct addressee, qualified electronic registered delivery services should ensure complete certainty the identification of the addressee while a high level of confidence would suffice as regards the identification of the sender. Providers of qualified electronic registered delivery services should be encouraged by Member States to make their services interoperable with qualified electronic registered delivery services provided by other qualified trust service providers in order to easily transfer electronic registered data between two or more qualified trust service providers and to promote fair practices in the internal market.
- (53) In most cases, Union citizens and residents in the Union are unable to exchange digital information relating to their identity, such as their address, age, professional qualifications, driving licence and other permits and payment data, across borders, securely and with a high level of data protection.
- (54) It should be possible to issue and handle trustworthy electronic attributes and contribute to reducing administrative burden, empowering Union citizens and residents in the Union to use them in their private and public transactions. Union citizens and residents in the Union should be able, for instance, to demonstrate ownership of a valid driving licence issued by an authority in one Member State, which can be verified and relied upon by the relevant authorities in other Member States, to rely on their social security credentials or on future digital travel documents in a cross border context.
- (55) Any service provider that issues attested attributes in electronic form such as diplomas, licences, birth certificates or powers and mandates to represent or act on behalf of natural or legal persons should be considered to be a trust service provider of electronic attestation of attributes. An electronic attestation of attributes should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic attestation of attributes. General requirements should be laid down to ensure that a qualified electronic attestation of attributes has the equivalent legal effect of lawfully issued attestations in paper form. However, those requirements should apply without prejudice to Union or national law defining additional sector-specific requirements as regards form with underlying legal effects and, in particular, the cross-border recognition of qualified electronic attestation of attributes, where appropriate.
- (56) The wide availability and usability of European Digital Identity Wallets should enhance their acceptance and trust in them both by private individuals and by private service providers. Therefore, private relying parties providing services, for example in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, telecommunications or education, should accept the use of European Digital Identity Wallets for the provision of services where strong user authentication for online identification is required by Union or national law or by contractual obligation. Any request by the relying party for information from the user of a European Digital Identity Wallet should be necessary for, and proportionate to, the intended use in a given case, should be in line with the principle of data minimisation and should ensure transparency as regards which data is shared and for what purposes. To facilitate the use and acceptance of European Digital Identity Wallets, widely accepted industry standards and specifications should be taken into account in their deployment.

- (57) Where very large online platforms within the meaning of Article 33(1) of Regulation (EU) 2022/2065 of the European Parliament and of the Council ⁽¹⁵⁾ require users to be authenticated in order to access online services, those platforms should be required to accept the use of European Digital Identity Wallets upon the voluntary request of the user. Users should be under no obligation to use a European Digital Identity Wallet to access private services and should not be restricted or hindered in their access to services on the grounds that they do not use a European Digital Identity Wallet. However, if users wish to do so, very large online platforms should accept them for that purpose, while respecting the principle of data minimisation and the right of the users to use freely chosen pseudonyms. Given the importance of very large online platforms, due to their reach, in particular as expressed in number of recipients of the service and economic transactions, the obligation to accept European Digital Identity Wallets is necessary to increase the protection of users from fraud and to secure a high level of data protection.
- (58) Codes of conduct at Union level should be developed in order to contribute to the widespread availability and usability of electronic identification means, including European Digital Identity Wallets within the scope of this Regulation. The codes of conduct should facilitate broad acceptance of electronic identification means including European Digital Identity Wallets by those service providers which do not qualify as very large platforms and which rely on third party electronic identification services for user authentication.
- (59) Selective disclosure is a concept empowering the owner of data to disclose only certain parts of a larger data set, in order for the receiving entity to obtain only such information as is necessary for the provision of a service requested by a user. The European Digital Identity Wallet should technically enable the selective disclosure of attributes to relying parties. It should be technically possible for the user to selectively disclose attributes, including from multiple, distinct electronic attestations, and to combine and present them seamlessly to relying parties. This feature should become a basic design feature of European Digital Identity Wallets, thereby reinforcing convenience and the protection of personal data, including data minimisation.
- (60) Unless specific rules of Union or national law require users to identify themselves, accessing services by using a pseudonym should not be prohibited.
- (61) Attributes provided by the qualified trust service providers as part of the qualified attestation of attributes should be verified against authentic sources either directly by the qualified trust service provider or by means of designated intermediaries recognised at national level in accordance with Union or national law for the purpose of secure exchange of attested attributes between identity or attestation of attributes' service providers and relying parties. Member States should establish appropriate mechanisms at national level to ensure that qualified trust service providers issuing qualified electronic attestation of attributes are able, on the basis of the consent of the person to whom the attestation is issued, to verify the authenticity of the attributes relying on authentic sources. It should be possible for appropriate mechanisms to include the use of specific intermediaries or technical solutions in accordance with national law allowing access to authentic sources. Ensuring the availability of a mechanism that allows the verification of attributes against authentic sources is intended to facilitate the compliance of the qualified trust service providers of qualified electronic attestation of attributes with their obligations under Regulation (EU) No 910/2014. A new annex to that Regulation should contain a list of categories of attributes with regard to which Member States are to ensure that measures are taken to allow qualified providers of electronic attestations of attributes to verify by electronic means, at the request of the user, their authenticity against the relevant authentic source.
- (62) Secure electronic identification and the provision of attestation of attributes should offer additional flexibility and solutions for the financial services sector to allow the identification of customers and the exchange of specific attributes necessary to comply with, for example, customer due diligence requirements under a future Regulation establishing the Anti Money Laundering Authority, with suitability requirements stemming from investor protection law, or to support the fulfilment of strong customer authentication requirements for online identification for the purposes of account login and of initiation of transactions in the field of payment services.
- (63) The legal effect of an electronic signature is not to be challenged on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic signature. However, it is for national law to establish the legal effect of electronic signatures, except for the requirements provided for in this Regulation according to which the legal effect of a qualified electronic signature is to be considered to be equivalent to that of

⁽¹⁵⁾ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1).

a handwritten signature. In determining the legal effects of electronic signatures, Member States should take into account the principle of proportionality between the legal value of a document to be signed and the level of security and cost that an electronic signature requires. To increase the accessibility and use of electronic signatures, Member States are encouraged to consider the use of advanced electronic signatures in the day-to-day transactions for which they provide a sufficient level of security and confidence.

- (64) In order to ensure the consistency of certification practices across the Union, the Commission should issue guidelines on the certification and recertification of qualified electronic signature creation devices and of qualified electronic seal creation devices, including their validity and limitations in time. This Regulation does not prevent the public or private bodies that have certified qualified electronic signature creation devices from temporarily re-certifying such devices for a short certification period on the basis of the results of the previous certification process, where such re-certification cannot be performed within the legally set time frame for a reason other than a breach or security incident, without prejudice to the obligation to conduct a vulnerability assessment and without prejudice to the applicable certification practice.
- (65) The issuance of certificates for website authentication is intended to provide users with assurance with a high level of confidence in the identity of the entity standing behind the website, irrespective of the platform used to display that identity. Those certificates should contribute to the building of trust in conducting business online, as users would have confidence in a website that has been authenticated. The use of such certificates by websites should be voluntary. In order for website authentication to become a means by which to increase trust, to provide a better experience for the user and to foster growth in the internal market, this Regulation lays down a trust framework including minimal security and liability obligations for the providers of qualified certificates for website authentication and requirements for the issuance of those certificates. National trusted lists should confirm the qualified status of website authentication services and of their trust service providers, including their full compliance with the requirements of this Regulation with regard to the issuance of qualified certificates for website authentication. The recognition of qualified certificates for website authentication means that the providers of web-browsers should not deny the authenticity of qualified certificates for website authentication for the sole purpose of attesting the link between the website domain name and the natural or legal person to whom the certificate is issued or confirming the identity of that person. Providers of web-browsers should display the certified identity data and the other attested attributes to the end-user in a user-friendly manner in the browser environment, by technical means of their choice. To that end, providers of web-browsers should ensure support and interoperability with qualified certificates for website authentication issued in full compliance with this Regulation. The obligation of recognition and interoperability of and support for qualified certificates for website authentication does not affect the freedom of providers of web-browsers to ensure web security, domain authentication and the encryption of web traffic in a manner and by means of technology that they consider to be the most appropriate. In order to contribute to the online security of end-users, providers of web-browsers should, in exceptional circumstances, be able to take precautionary measures that are both necessary and proportionate in reaction to substantiated concerns regarding security breaches or the loss of integrity of an identified certificate or set of certificates. Where they take such precautionary measures, providers of web-browsers should notify, without undue delay, the Commission, the national supervisory body, the entity to which the certificate was issued and the qualified trust service provider that issued that certificate or set of certificates, of any concern with regard to such a security breach or loss of integrity as well as the measures taken relating to the single certificate or set of certificates. Those measures should be without prejudice to the obligation of the providers of web-browsers to recognise qualified website authentication certificates in accordance with the national trusted lists. To further protect Union citizens and residents in the Union and promote the use of qualified certificates for website authentication, public authorities in Member States should consider incorporating qualified certificates for website authentication in their websites. The measures provided for by this Regulation that aim to bring increased coherence between Member States' divergent approaches and practices relating to supervisory procedures are intended to contribute to improved trust and confidence in the security, quality and availability of qualified certificates for website authentication.
- (66) Many Member States have introduced national requirements for services providing secure and trustworthy electronic archiving in order to allow for the long-term preservation of electronic data and electronic documents, and associated trust services. To ensure legal certainty, trust and harmonisation across Member States, a legal framework for qualified electronic archiving services should be established, inspired by the framework of the other trust services set out in this Regulation. The legal framework for qualified electronic archiving services should offer trust service providers and users an efficient toolbox that includes functional requirements for the electronic archiving service, as well as clear legal effects when a qualified electronic archiving service is used. Those provisions should apply to electronic data and electronic documents created in electronic form as well as paper documents that have been scanned and digitised. When required, those provisions should permit the preserved electronic data and electronic

documents to be ported on different media or formats for the purpose of extending their durability and legibility beyond the technological validity period, while preventing loss and alteration to the extent possible. When electronic data and electronic documents submitted to the electronic archiving service contain one or more qualified electronic signatures or qualified electronic seals, the service should use procedures and technologies capable of extending their trustworthiness for the preservation period of such data, possibly relying on the use of other qualified trust services established by this Regulation. In order to create preservation evidence where electronic signatures, electronic seals or electronic timestamps are used, qualified trust services should be used. To the extent that electronic archiving services are not harmonised by this Regulation, it should be possible for Member States to maintain or introduce national provisions, in accordance with Union law, relating to those services, such as specific provisions for services integrated in an organisation and only used for the internal archives of that organisation. This Regulation should not distinguish between electronic data and electronic documents created in electronic form and physical documents that have been digitised.

- (67) The activities of national archives and memory institutions, in their capacity as organisations dedicated to preserving the documentary heritage in the public interest, are usually regulated in national law and they do not necessarily provide trust services within the meaning of this Regulation. In so far such institutions do not provide such trust services, this Regulation is without prejudice to their operation.
- (68) Electronic ledgers are a sequence of electronic data records which should ensure their integrity and the accuracy of their chronological ordering. Electronic ledgers should establish a chronological sequence of data records. In conjunction with other technologies, they should contribute to solutions for more efficient and transformative public services such as e-voting, cross-border cooperation of customs authorities, cross-border cooperation of academic institutions and the recording of ownership for real estate in decentralised land registries. Qualified electronic ledgers should establish a legal presumption for the unique and accurate sequential chronological ordering and integrity of the data records in the ledger. Due to their specificities, such as the sequential chronological ordering of data records, electronic ledgers should be distinguished from other trust services such as electronic time stamps and electronic registered delivery services. To ensure legal certainty and promote innovation, a Union-wide legal framework that provides for the cross-border recognition of trust services for the recording of data in electronic ledgers should be established. This should sufficiently prevent the same digital asset from being copied and sold more than once to different parties. The process of creating and updating an electronic ledger depends on the type of ledger used, namely whether it is centralised or distributed. This Regulation should ensure technological neutrality, namely neither favouring, nor discriminating against, any technology used to implement the new trust service for electronic ledgers. In addition, sustainability indicators with regard to any adverse impacts on the climate or other environment-related adverse impacts should be taken into account by the Commission, using adequate methodologies, when preparing the implementing acts specifying the requirements for qualified electronic ledgers.
- (69) The role of trust service providers for electronic ledgers should be to ascertain the sequential recording of data into the ledger. This Regulation is without prejudice to any legal obligations of users of electronic ledgers under Union or national law. For instance, use cases that involve the processing of personal data should comply with Regulation (EU) 2016/679 and use cases that relate to financial services should comply with the relevant Union financial services law.
- (70) In order to avoid the fragmentation of and barriers in the internal market, due to diverging standards and technical restrictions, and to ensure a coordinated process to avoid affecting the implementation of the European Digital Identity Framework, a process for close and structured cooperation between the Commission, Member States, civil society, academia and the private sector is needed. To achieve that objective, Member States and the Commission should cooperate within the framework set out in the Commission Recommendation (EU) 2021/946⁽¹⁶⁾ to identify a common Union toolbox for the European Digital Identity Framework. In that context, Member States should agree on a comprehensive technical architecture and reference framework, a set of common standards and technical references including recognised existing standards and a set of guidelines and descriptions of best practices covering at least all functionalities and interoperability of European Digital Identity Wallets, including eSignatures and of the qualified trust service providers for electronic attestation of attributes as laid out in this Regulation. In that context, Member States should also agree on common elements with regard to a business model and fee structure for

⁽¹⁶⁾ Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework (OJ L 210, 14.6.2021, p. 51).

European Digital Identity Wallets, in order to facilitate take up, in particular by SMEs, in a cross-border context. The content of the toolbox should evolve in parallel with and reflect the outcome of the discussion and the process of adoption of the European Digital Identity Framework.

- (71) This Regulation provides for a harmonised level of quality, trustworthiness and security of qualified trust services, regardless of where the operations are conducted. Thus, a qualified trust service provider should be allowed to outsource its operations related to the provision of a qualified trust service in a third country, where that third country provides adequate guarantees, ensuring that supervisory activities and audits can be enforced as if they were carried out in the Union. When the compliance with this Regulation cannot be fully assured, the supervisory bodies should be able to adopt proportionate and justified measures including the withdrawal of the qualified status of the trust service provided.
- (72) To ensure legal certainty as regards the validity of advanced electronic signatures based on qualified certificates, it is essential that the assessment by the relying party carrying out the validation of that advanced electronic signature based on qualified certificates be specified.
- (73) Trust service providers should use cryptographic methods reflecting current best practices and trustworthy implementations of those algorithms in order to ensure security and reliability of their trust services.
- (74) This Regulation lays down an obligation for qualified trust service providers to verify the identity of a natural or legal person to whom the qualified certificate or the qualified electronic attestation of attribute is issued based on various harmonised methods across the Union. To ensure that qualified certificates and qualified electronic attestations of attributes are issued to the person to whom they belong and that they attest the correct and unique set of data representing the identity of that person, qualified trust service providers issuing qualified certificates or issuing qualified electronic attestations of attributes should, at the moment of the issuance of those certificates and attestations, ensure with complete certainty the identification of that person. Moreover, in addition to the mandatory verification of the identity of the person, if applicable for the issuance of qualified certificates and when issuing a qualified electronic attestation of attributes, qualified trust service providers should ensure with complete certainty the correctness and accuracy of the attested attributes of the person to whom the qualified certificate or the qualified electronic attestation of attributes is issued. Those obligations of result and complete certainty in verifying the attested data should be supported by appropriate means, including by using one or, where required, a combination of specific methods provided for in this Regulation. It should be possible to combine those methods to provide an appropriate basis for the verification of the identity of the person to whom the qualified certificate or a qualified electronic attestation of attributes is issued. It should be possible for such a combination to include reliance on electronic identification means which meet the requirements of assurance level substantial in combination with other means of identity verification. Such electronic identification would allow the fulfilment of the harmonised requirements set out in this Regulation as regards assurance level high as part of additional harmonised remote procedures, ensuring identification with a high level of confidence. Those methods should include the possibility for the qualified trust service provider issuing a qualified electronic attestation of attributes to verify the attributes to be attested by electronic means at the request of the user, in accordance with Union or national law, including against authentic sources.
- (75) To keep this Regulation in line with global developments and to follow the best practices on the internal market, the delegated and implementing acts adopted by the Commission should be reviewed and if necessary updated on a regular basis. The assessment of the necessity of those updates should take into account new technologies, practices, standards or technical specifications.
- (76) Since the objectives of this Regulation, namely the development of the Union-wide European Digital Identity Framework and of a trust service framework, cannot be sufficiently achieved by the Member States but can rather, by reason of their scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.
- (77) The European Data Protection Supervisor has been consulted pursuant to Article 42(1) of Regulation (EU) 2018/1725.

(78) Regulation (EU) No 910/2014 should therefore be amended accordingly,

HAVE ADOPTED THIS REGULATION:

Article 1

Amendments to Regulation (EU) No 910/2014

Regulation (EU) No 910/2014 is amended as follows:

(1) Article 1 is replaced by the following:

‘Article 1

Subject matter

This Regulation aims to ensure the proper functioning of the internal market and the provision of an adequate level of security of electronic identification means and trust services used across the Union, in order to enable and facilitate the exercise by natural and legal persons of the right to participate in digital society safely and to access online public and private services throughout the Union. For those purposes, this Regulation:

- (a) lays down the conditions under which Member States are to recognise natural and legal persons’ electronic identification means falling under a notified electronic identification scheme of another Member State and provide and recognise European Digital Identity Wallets;
- (b) lays down rules for trust services, in particular for electronic transactions;
- (c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, certificate services for website authentication, electronic archiving, electronic attestation of attributes, electronic signature creation devices, electronic seal creation devices, and electronic ledgers.’;

(2) Article 2 is amended as follows:

(a) paragraph 1 is replaced by the following:

‘1. This Regulation applies to electronic identification schemes notified by a Member State, to European Digital Identity Wallets provided by a Member State and to trust service providers established in the Union.’;

(b) paragraph 3 is replaced by the following:

‘3. This Regulation does not affect Union or national law related to the conclusion and validity of contracts, other legal or procedural obligations relating to form, or sector-specific requirements relating to form.

4. This Regulation is without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council (*).

(*) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).’;

(3) Article 3 is amended as follows:

(a) points (1) to (5) are replaced by the following:

‘(1) “electronic identification” means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person;

- (2) “electronic identification means” means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service;
 - (3) “person identification data” means a set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person.
 - (4) “electronic identification scheme” means a system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing other natural persons or legal persons;
 - (5) “authentication” means an electronic process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form;’
- (b) the following point is inserted:
- ‘(5a) “user” means a natural or legal person, or a natural person representing another natural person or a legal person, that uses trust services or electronic identification means provided in accordance with this Regulation;’
- (c) point (6) is replaced by the following:
- ‘(6) “relying party” means a natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service;’
- (d) point (16) is replaced by the following:
- ‘(16) “trust service” means an electronic service normally provided for remuneration which consists of any of the following:
 - (a) the issuance of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services;
 - (b) the validation of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services;
 - (c) the creation of electronic signatures or electronic seals;
 - (d) the validation of electronic signatures or electronic seals;
 - (e) the preservation of electronic signatures, electronic seals, certificates for electronic signatures or certificates for electronic seals;
 - (f) the management of remote electronic signature creation devices or remote electronic seal creation devices;
 - (g) the issuance of electronic attestations of attributes;
 - (h) the validation of electronic attestation of attributes;
 - (i) the creation of electronic timestamps;
 - (j) the validation of electronic timestamps;
 - (k) the provision of electronic registered delivery services;
 - (l) the validation of data transmitted through electronic registered delivery services and related evidence;
 - (m) the electronic archiving of electronic data and electronic documents;

- (n) the recording of electronic data in an electronic ledger;;
- (e) point (18) is replaced by the following:
 - ‘(18) “conformity assessment body” means a conformity assessment body as defined in Article 2, point 13, of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides, or as competent to carry out certification of European Digital Identity Wallets or electronic identification means;’;
- (f) point (21) is replaced by the following:
 - ‘(21) “product” means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of electronic identification and trust services;’;
- (g) the following points are inserted:
 - ‘(23a) “remote qualified electronic signature creation device” means a qualified electronic signature creation device that is managed by a qualified trust service provider in accordance with Article 29a on behalf of a signatory;
 - ‘(23b) “remote qualified electronic seal creation device” means a qualified electronic seal creation device that is managed by a qualified trust service provider in accordance with Article 39a on behalf of a seal creator;’;
- (h) point (38) is replaced by the following:
 - ‘(38) “certificate for website authentication” means an electronic attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;’;
- (i) point (41) is replaced by the following:
 - ‘(41) “validation” means the process of verifying and confirming that data in electronic form are valid in accordance with this Regulation;’;
- (j) the following points are added:
 - ‘(42) “European Digital Identity Wallet” means an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals;
 - (43) “attribute” means a characteristic, quality, right or permission of a natural or legal person or of an object;
 - (44) “electronic attestation of attributes” means an attestation in electronic form that allows attributes to be authenticated;
 - (45) “qualified electronic attestation of attributes” means an electronic attestation of attributes which is issued by a qualified trust service provider and meets the requirements laid down in Annex V;
 - (46) “electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source” means an electronic attestation of attributes issued by a public sector body that is responsible for an authentic source or by a public sector body that is designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45f and with Annex VII;
 - (47) “authentic source” means a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice;

- (48) “electronic archiving” means a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to ensure their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period;
- (49) “qualified electronic archiving service” means an electronic archiving service which is provided by a qualified trust service provider and which meets the requirements laid down in Article 45j;
- (50) “EU Digital Identity Wallet Trust Mark” means a verifiable, simple and recognisable indication which is communicated in a clear manner that a European Digital Identity Wallet has been provided in accordance with this Regulation;
- (51) “strong user authentication” means an authentication based on the use of at least two authentication factors from different categories of either knowledge, something only the user knows, possession, something only the user possesses or inherence, something the user is, that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;
- (52) “electronic ledger” means a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records;
- (53) “qualified electronic ledger” means an electronic ledger which is provided by a qualified trust service provider and which meets the requirements laid down in Article 45l;
- (54) “personal data” means any information as defined in Article 4, point (1), of Regulation (EU) 2016/679;
- (55) “identity matching” means a process where person identification data, or electronic identification means are matched with or linked to an existing account belonging to the same person;
- (56) “data record” means electronic data recorded with related meta-data supporting the processing of the data;
- (57) “offline mode” means, as regards the use of European Digital Identity Wallets, an interaction between a user and a third party at a physical location using close proximity technologies, whereby the European Digital Identity Wallet is not required to access remote systems via electronic communication networks for the purpose of the interaction.’;

- (4) Article 5 is replaced by the following:

‘Article 5

Pseudonyms in electronic transaction

Without prejudice to specific rules of Union or national law requiring users to identify themselves or to the legal effect given to pseudonyms under national law, the use of pseudonyms that are chosen by the user shall not be prohibited.’;

- (5) in Chapter II, the following section is inserted:

‘SECTION 1

EUROPEAN DIGITAL IDENTITY WALLET

Article 5a

European Digital Identity Wallets

1. For the purpose of ensuring that all natural and legal persons in the Union have secure, trusted and seamless cross-border access to public and private services, while having full control over their data, each Member State shall provide at least one European Digital Identity Wallet within 24 months of the date of entry into force of the implementing acts referred to in paragraph 23 of this Article and in Article 5c(6).

2. European Digital Identity Wallets shall be provided in one or more of the following ways:

- (a) directly by a Member State;
- (b) under a mandate from a Member State;
- (c) independently of a Member State but recognised by that Member State.

3. The source code of the application software components of European Digital Identity Wallets shall be open-source licensed. Member States may provide that, for duly justified reasons, the source code of specific components other than those installed on user devices shall not be disclosed.

4. European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to:

- (a) securely request, obtain, select, combine, store, delete, share and present, under the sole control of the user, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, in offline mode, in order to access public and private services, while ensuring that selective disclosure of data is possible;
- (b) generate pseudonyms and store them encrypted and locally within the European Digital Identity Wallet;
- (c) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets;
- (d) access a log of all transactions carried out through the European Digital Identity Wallet via a common dashboard enabling the user to:
 - (i) view an up-to-date list of relying parties with which the user has established a connection and, where applicable, all data exchanged;
 - (ii) easily request the erasure by a relying party of personal data pursuant to Article 17 of the Regulation (EU) 2016/679;
 - (iii) easily report a relying party to the competent national data protection authority, where an allegedly unlawful or suspicious request for data is received;
- (e) sign by means of qualified electronic signatures or seal by means of qualified electronic seals;
- (f) download, to the extent technically feasible, the user's data, electronic attestation of attributes and configurations;
- (g) exercise the user's rights to data portability.

5. European Digital Identity Wallets shall, in particular:

- (a) support common protocols and interfaces:
 - (i) for issuance of person identification data, qualified and non-qualified electronic attestations of attributes or qualified and non-qualified certificates to the European Digital Identity Wallet;
 - (ii) for relying parties to request and validate person identification data and electronic attestations of attributes;
 - (iii) for the sharing and presentation to relying parties of person identification data, electronic attestation of attributes or of selectively disclosed related data online and, where appropriate, in offline mode;

- (iv) for the user to allow interaction with the European Digital Identity Wallet and display an EU Digital Identity Wallet Trust Mark;
 - (v) to securely onboard the user by using an electronic identification means in accordance with Article 5a(24);
 - (vi) for interaction between two persons' European Digital Identity Wallets for the purpose of receiving, validating and sharing person identification data and electronic attestations of attributes in a secure manner;
 - (vii) for authenticating and identifying relying parties by implementing authentication mechanisms in accordance with Article 5b;
 - (viii) for relying parties to verify the authenticity and validity of European Digital Identity Wallets;
 - (ix) for requesting a relying party the erasure of personal data pursuant to Article 17 of Regulation (EU) 2016/679;
 - (x) for reporting a relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for data is received;
 - (xi) for the creation of qualified electronic signatures or electronic seals by means of qualified electronic signature or electronic seal creation devices;
- (b) not provide any information to trust service providers of electronic attestations of attributes about the use of those electronic attestations;
- (c) ensure that the relying parties can be authenticated and identified by implementing authentication mechanisms in accordance with Article 5b;
- (d) meet the requirements set out in Article 8 with regard to assurance level high, in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication;
- (e) in the case of the electronic attestation of attributes with embedded disclosure policies, implement the appropriate mechanism to inform the user that the relying party or the user of the European Digital Identity Wallet requesting that electronic attestation of attributes has the permission to access such attestation;
- (f) ensure that the person identification data, which is available from the electronic identification scheme under which the European Digital Identity Wallet is provided, uniquely represents the natural person, legal person or the natural person representing the natural or legal person, and is associated with that European Digital Identity Wallet;
- (g) offer all natural persons the ability to sign by means of qualified electronic signatures by default and free of charge.

Notwithstanding point (g) of the first subparagraph, Member States may provide for proportionate measures to ensure that the use of qualified electronic signatures free-of-charge by natural persons is limited to non-professional purposes.

6. Member State shall inform users, without delay, of any security breach that could have entirely or partially compromised their European Digital Identity Wallet or its contents, in particular if their European Digital Identity Wallet has been suspended or revoked pursuant to Article 5e.

7. Without prejudice to Article 5f, Member States may provide, in accordance with national law, for additional functionalities of European Digital Identity Wallets, including interoperability with existing national electronic identification means. Those additional functionalities shall comply with this Article.

8. Member States shall provide validation mechanisms free-of-charge, in order to:
- (a) ensure that the authenticity and validity of European Digital Identity Wallets can be verified;
 - (b) allow users to verify the authenticity and validity of the identity of relying parties registered in accordance with Article 5b.
9. Member States shall ensure that the validity of the European Digital Identity Wallet can be revoked in the following circumstances:
- (a) upon the explicit request of the user;
 - (b) where the security of the European Digital Identity Wallet has been compromised;
 - (c) upon the death of the user or cease of activity of the legal person.
10. Providers of European Digital Identity Wallets shall ensure that users can easily request technical support and report technical problems or any other incidents having a negative impact on the use of European Digital Identity Wallets.
11. European Digital Identity Wallets shall be provided under an electronic identification scheme with assurance level high.
12. European Digital Identity Wallets shall ensure security-by-design.
13. The issuance, use and revocation of the European Digital Identity Wallets shall be free of charge to all natural persons.
14. Users shall have full control of the use of and of the data in their European Digital Identity Wallet. The provider of the European Digital Identity Wallet shall neither collect information about the use of the European Digital Identity Wallet which is not necessary for the provision of European Digital Identity Wallet services, nor combine person identification data or any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by that provider or from third-party services which are not necessary for the provision of European Digital Identity Wallet services, unless the user has expressly requested otherwise. Personal data relating to the provision of the European Digital Identity Wallet shall be kept logically separate from any other data held by the provider of the European Digital Identity Wallet. If the European Digital Identity Wallet is provided by private parties in accordance with paragraph 2, points (b) and (c), of this Article, the provisions of Article 45h(3) shall apply *mutatis mutandis*.
15. The use of European Digital Identity Wallets shall be voluntary. Access to public and private services, access to the labour market and freedom to conduct business shall not in any way be restricted or made disadvantageous to natural or legal persons that do not use European Digital Identity Wallets. It shall remain possible to access public and private services by other existing identification and authentication means.
16. The technical framework of the European Digital Identity Wallet shall:
- (a) not allow providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, to obtain data that allows transactions or user behaviour to be tracked, linked or correlated, or knowledge of transactions or user behaviour to be otherwise obtained, unless explicitly authorised by the user;
 - (b) enable privacy preserving techniques which ensure unlikability, where the attestation of attributes does not require the identification of the user.
17. Any processing of personal data carried out by the Member States or on their behalf by bodies or parties responsible for the provision of European Digital Identity Wallets as electronic identification means shall be carried out in accordance with appropriate and effective data protection measures. Compliance of such processing with Regulation (EU) 2016/679 shall be demonstrated. Member States may introduce national provisions to further specify the application of such measures.

18. Member States shall, without undue delay, notify the Commission of information about:
- (a) the body responsible for establishing and maintaining the list of registered relying parties that rely on European Digital Identity Wallets in accordance with Article 5b(5) and the location of that list;
 - (b) the bodies responsible for the provision of European Digital Identity Wallets in accordance with Article 5a(1);
 - (c) the bodies responsible for ensuring that the person identification data is associated with the European Digital Identity Wallet in accordance with Article 5a(5), point (f);
 - (d) the mechanism allowing for the validation of the person identification data referred to in Article 5a(5), point (f), and of the identity of the relying parties;
 - (e) the mechanism by which to validate the authenticity and validity of European Digital Identity Wallets.

The Commission shall make available the information notified pursuant to the first subparagraph to the public through a secure channel, in electronically signed or sealed form suitable for automated processing.

19. Without prejudice to paragraph 22 of this Article, Article 11 shall apply *mutatis mutandis* to the European Digital Identity Wallet.

20. Article 24(2), points (b), and (d) to (h), shall apply *mutatis mutandis* to providers of European Digital Identity Wallets.

21. European Digital Identity Wallets shall be made accessible for use, by persons with disabilities, on an equal basis with other users, in accordance with Directive (EU) 2019/882 of the European Parliament and of the Council (*).

22. For the purposes of the provision of European Digital Identity Wallets, European Digital Identity Wallets and the electronic identification schemes under which they are provided shall not be subject to the requirements laid down in Articles 7, 9, 10, 12 and 12a.

23. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraphs 4, 5, 8 and 18 of this Article on the implementation of the European Digital Identity Wallet. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

24. The Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures in order to facilitate the onboarding of users to the European Digital Identity Wallet either by electronic identification means conforming to assurance level high or by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures that together meet the requirements of assurance level high. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 5b

European Digital Identity Wallet-Relying Parties

1. Where a relying party intends to rely upon European Digital Identity Wallets for the provision of public or private services by means of digital interaction, the relying party shall register in the Member State where it is established.

2. The registration process shall be cost-effective and proportionate-to-risk. The relying party shall provide at least:

- (a) the information necessary to authenticate to European Digital Identity Wallets, which as a minimum includes:
 - (i) the Member State in which the relying party is established; and

- (ii) the name of the relying party and, where applicable, its registration number as stated in an official record together with identification data of that official record;
 - (b) the contact details of the relying party;
 - (c) the intended use of European Digital Identity Wallets, including an indication of the data to be requested by the relying party from users.
3. Relying parties shall not request users to provide any data other than that indicated pursuant to paragraph 2, point (c).
4. Paragraphs 1 and 2 shall be without prejudice to Union or national law that is applicable to the provision of specific services.
5. Member States shall make the information referred to in paragraph 2 publicly available online in electronically signed or sealed form suitable for automated processing.
6. Relying parties registered in accordance with this Article shall inform Member States without delay about any changes to the information provided in the registration pursuant to paragraph 2.
7. Member States shall provide a common mechanism for allowing the identification and authentication of relying parties, as referred to in Article 5a(5), point (c).
8. Where relying parties intend to rely upon European Digital Identity Wallets, they shall identify themselves to the user.
9. Relying parties shall be responsible for carrying out the procedure for authenticating and validating person identification data and electronic attestation of attributes requested from European Digital Identity Wallets. Relying parties shall not refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.
10. Intermediaries acting on behalf of relying parties shall be deemed to be relying parties and shall not store data about the content of the transaction.
11. By 21 November 2024, the Commission shall establish technical specifications and procedures for the requirements referred to in paragraphs 2, 5 and 6 to 9 of this Article by means of implementing acts on the implementation of European Digital Identity Wallets as referred to in Article 5a(23). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 5c

Certification of European Digital Identity Wallets

1. The conformity of European Digital Identity Wallets and the electronic identification scheme under which they are provided with the requirements laid down in Article 5a(4), (5), (8), the requirement for logical separation laid down in Article 5a(14) and, where applicable, with the standards and technical specifications referred to in Article 5a(24), shall be certified by conformity assessment bodies designated by Member States.
2. Certification of the conformity of European Digital Identity Wallets with requirements referred to in paragraph 1 of this Article, or parts thereof, that are relevant for cybersecurity shall be carried out in accordance with European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council (**) and referred to in the implementing acts referred to in paragraph 6 of this Article.
3. For requirements referred to in paragraph 1 of this Article that are not relevant for cybersecurity, and, for requirements referred to in paragraph 1 of this Article that are relevant for cybersecurity, to the extent that cybersecurity certification schemes as referred to in paragraph 2 of this Article do not, or only partially, cover those cybersecurity requirements, also for those requirements, Member States shall establish national certification schemes following the requirements set out in the implementing acts referred to in paragraph 6 of this Article. Member States shall transmit their draft national certification schemes to the European Digital Identity Cooperation Group established pursuant to Article 46e(1) (the "Cooperation Group"). The Cooperation Group may issue opinions and recommendations.

4. Certification pursuant to paragraph 1 shall be valid for up to five years, provided that a vulnerability assessment is carried out every two years. Where a vulnerability is identified and not remedied in a timely manner, certification shall be cancelled.

5. Compliance with the requirements set out in Article 5a of this Regulation related to the personal data processing operations may be certified pursuant to Regulation(EU) 2016/679.

6. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the certification of European Digital Identity Wallets referred to in paragraph 1, 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

7. Member States shall communicate to the Commission the names and addresses of the conformity assessment bodies referred to in paragraph 1. The Commission shall make that information available to all Member States.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 establishing specific criteria to be met by the designated conformity assessment bodies referred to in paragraph 1 of this Article.

Article 5d

Publication of a list of certified European Digital Identity Wallets

1. Member States shall inform the Commission and the Cooperation Group established pursuant to Article 46e(1) without undue delay of European Digital Identity Wallets that have been provided pursuant to Article 5a and certified by the conformity assessment bodies referred to in Article 5c(1). They shall inform the Commission and the Cooperation Group established pursuant to Article 46e(1), without undue delay if a certification is cancelled and shall state the reasons for the cancellation.

2. Without prejudice to Article 5a(18), the information provided by Member States referred to in paragraph 1 of this Article shall include at least:

- (a) the certificate and certification assessment report of the certified European Digital Identity Wallet;
- (b) a description of the electronic identification scheme under which the European Digital Identity Wallet is provided;
- (c) the applicable supervisory regime and information on the liability regime with respect to the party providing the European Digital Identity Wallet;
- (d) the authority or authorities responsible for the electronic identification scheme;
- (e) arrangements for suspension or revocation of the electronic identification scheme or authentication or of the compromised parts concerned.

3. On the basis of the information received pursuant to paragraph 1, the Commission shall establish, publish in the *Official Journal of the European Union* and maintain in a machine-readable form a list of certified European Digital Identity Wallets.

4. A Member State may submit a request to the Commission to remove a European Digital Identity Wallet and the electronic identification scheme under which it is provided from the list referred to in paragraph 3.

5. Where there are changes to the information provided pursuant to paragraph 1, the Member State shall provide the Commission with updated information.

6. The Commission shall keep the list referred to in paragraph 3 updated by publishing in the *Official Journal of the European Union* the corresponding amendments to the list within one month of receipt of a request pursuant to paragraph 4 or of updated information pursuant to paragraph 5.

7. By 21 November 2024, the Commission shall establish the formats and procedures applicable for the purposes of paragraphs 1, 4 and 5 of this Article by means of implementing acts on the implementation of European Digital Identity Wallets as referred to in Article 5a(23). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 5e

Security breach of European Digital Identity Wallets

1. Where European Digital Identity Wallets provided pursuant to Article 5a, the validation mechanisms referred to in Article 5a(8) or the electronic identification scheme under which the European Digital Identity Wallets are provided are breached or partly compromised in a manner that affects their reliability or the reliability of other European Digital Identity Wallets, the Member State that provided the European Digital Identity Wallets shall, without undue delay, suspend the provision and the use of European Digital Identity Wallets.

Where justified by the severity of the security breach or compromise referred to in the first subparagraph, the Member State shall withdraw European Digital Identity Wallets without undue delay.

The Member State shall inform the users affected, the single points of contact designated pursuant to Article 46c(1), the relying parties and the Commission accordingly.

2. If the security breach or compromise referred to in paragraph 1, first subparagraph, of this Article is not remedied within three months of the suspension, the Member State that provided the European Digital Identity Wallets shall withdraw European Digital Identity Wallets and revoke their validity. The Member State shall inform the users affected, the single points of contact designated pursuant to Article 46c(1), the relying parties and the Commission of the withdrawal accordingly.

3. Where the security breach or compromise referred to in paragraph 1, first subparagraph, of this Article is remedied, the providing Member State shall re-establish the provision and the use of European Digital Identity Wallets and inform the affected users and relying parties, the single points of contact designated pursuant to Article 46c(1) and the Commission without undue delay.

4. The Commission shall publish in the *Official Journal of the European Union* the corresponding amendments to the list referred to in Article 5d without undue delay.

5. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the measures referred to in paragraphs 1, 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 5f

Cross-border reliance on European Digital Identity Wallets

1. Where Member States require electronic identification and authentication to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets that are provided in accordance with this Regulation.

2. Where private relying parties that provide services, with the exception of microenterprises and small enterprises as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC (**), are required by Union or national law to use strong user authentication for online identification or where strong user authentication for online identification is required by contractual obligation, including in the areas of transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, those private relying parties shall, no later than 36 months from the date of entry into force of the implementing acts referred to in Article 5a(23) and Article 5c(6) and only upon the voluntary request of the user, also accept European Digital Identity Wallets that are provided in accordance with this Regulation.

3. Where providers of very large online platforms as referred to in Article 33 of Regulation (EU) 2022/2065 of the European Parliament and of the Council (****) require user authentication for access to online services, they shall also accept and facilitate the use of European Digital Identity Wallets that are provided in accordance with this Regulation for user authentication only upon the voluntary request of the user and in respect of the minimum data necessary for the specific online service for which authentication is requested.

4. In cooperation with Member States, the Commission shall facilitate the development of codes of conduct in close collaboration with all relevant stakeholders, including civil society, in order to contribute to the wide availability and usability of European Digital Identity Wallets within the scope of this Regulation, and to encourage service providers to complete the development of codes of conduct.

5. Within 24 months after deployment of the European Digital Identity Wallets, the Commission shall assess the demand for, and the availability and usability of, European Digital Identity Wallets, taking into account criteria such as user take-up, cross-border presence of service providers, technological developments, evolution in usage patterns and consumer demand.

(*) Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

(**) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

(***) Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

(****) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1).';

(6) the following heading is inserted before Article 6:

‘SECTION 2

ELECTRONIC IDENTIFICATION SCHEMES’;

(7) in Article 7, point (g) is replaced by the following:

‘(g) at least six months prior to notification pursuant to Article 9(1), the notifying Member State provides the other Member States, for the purposes of Article 12(5), with a description of that scheme in accordance with the procedural arrangements established by the implementing acts adopted pursuant to Article 12(6);’;

(8) in Article 8(3), the first subparagraph is replaced by the following:

‘3 By 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means.’;

(9) in Article 9, paragraphs 2 and 3 are replaced by the following:

‘2. The Commission shall, without undue delay, publish in the *Official Journal of the European Union* a list of the electronic identification schemes which were notified pursuant to paragraph 1 together with basic information about those schemes.

3. The Commission shall publish in the *Official Journal of the European Union* the amendments to the list referred to in paragraph 2 within one month of the date of receipt of that notification.’;

(10) in Article 10, the title is replaced by the following:

‘Security breach of electronic identification schemes’;

(11) the following article is inserted:

'Article 11a

Cross-border identity matching

1. When acting as relying parties for cross-border services, Member States shall ensure unequivocal identity matching for natural persons using notified electronic identification means or European Digital Identity Wallets.
2. Member States shall provide for technical and organisational measures to ensure a high level of protection of personal data used for identity matching and to prevent the profiling of users.
3. By 21 November 2024, the Commission shall establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraph 1 of this Article by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).;

(12) Article 12 is amended as follows:

(a) the title is replaced by the following:

'Interoperability';

(b) paragraph 3 is amended as follows:

(i) point (c) is replaced by the following:

'(c) it facilitates the implementation of privacy and security by design;';

(ii) point (d) is deleted;

(c) in paragraph 4, point (d) is replaced by the following:

'(d) a reference to a minimum set of person identification data necessary to uniquely represent a natural or legal person, or a natural person representing another natural person or a legal person, which is available from electronic identification schemes;';

(d) paragraphs 5 and 6 are replaced by the following:

'5. Member States shall carry out peer reviews of the electronic identification schemes that fall within the scope of this Regulation and that are to be notified pursuant to Article 9(1), point (a).

6. By 18 March 2025, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements for the peer reviews referred to in paragraph 5 of this Article with a view to fostering a high level of trust and security appropriate to the degree of risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).;

(e) paragraph 7 is deleted;

(f) paragraph 8 is replaced by the following:

'8. By 18 September 2025, for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1 of this Article, the Commission shall, subject to the criteria set out in paragraph 3 of this Article and taking into account the results of the cooperation between Member States, adopt implementing acts on the interoperability framework as set out in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).;

(13) the following articles are inserted in Chapter II:

Article 12a

Certification of electronic identification schemes

1. The conformity of electronic identification schemes to be notified with the cybersecurity requirements laid down in this Regulation, including conformity with the cybersecurity relevant requirements set out in Article 8(2) regarding the assurance levels of electronic identification schemes, shall be certified by conformity assessment bodies designated by Member States.
2. Certification pursuant to paragraph 1 of this Article shall be carried out under a relevant cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 or parts thereof, insofar as the cybersecurity certificate or parts thereof cover those cybersecurity requirements.
3. Certification pursuant to paragraph 1 shall be valid for up to five years, provided that a vulnerability assessment is carried out every two years. Where a vulnerability is identified and not remedied within three months of such identification, certification shall be cancelled.
4. Notwithstanding paragraph 2, Member States may request, in accordance with that paragraph, additional information from a notifying Member State about electronic identification schemes or part thereof certified.
5. The peer review of electronic identification schemes referred to in Article 12(5) shall not apply to electronic identification schemes or parts of such schemes certified in accordance with paragraph 1 of this Article. Member States may use a certificate or a statement of conformity, issued in accordance with a relevant certification scheme or parts of such schemes, with the non-cybersecurity-related requirements set out in Article 8(2) regarding the assurance level of electronic identification schemes.
6. Member States shall communicate to the Commission the names and addresses of the conformity assessment bodies referred to in paragraph 1. The Commission shall make that information available to all Member States.

Article 12b

Access to hardware and software features

Where providers of European Digital Identity Wallets and issuers of notified electronic identification means that act in a commercial or professional capacity and use core platform services as defined in Article 2, point (2), of Regulation (EU) 2022/1925 of the European Parliament and of the Council (*) for the purpose or in the course of providing European Digital Identity Wallet services and electronic identification means to end-users are business users as defined in Article 2, point (21), of that Regulation, gatekeepers shall in particular allow them effective interoperability with, and, for the purposes of interoperability, access to, the same operating system, hardware or software features. Such effective interoperability and access shall be allowed free of charge and regardless of whether the hardware or software features are part of the operating system, are available to, or are used by, that gatekeeper when providing such services, within the meaning of Article 6(7) of Regulation (EU) 2022/1925. This Article is without prejudice to Article 5a(14) of this Regulation.

(*) Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, p. 1).;

(14) in Article 13, paragraph 1 is replaced by the following:

- ‘1. Notwithstanding paragraph 2 of this Article and without prejudice to Regulation (EU) 2016/679, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation. Any natural or legal person who has suffered material or non-material damage as a result of an infringement of this Regulation by a trust service provider shall have the right to seek compensation in accordance with Union and national law.

The burden of proving the intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph.

The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.;

(15) Articles 14, 15 and 16 are replaced by the following:

Article 14

International aspects

1. Trust services provided by trust service providers established in a third country or by an international organisation shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union, where the trust services originating from the third country or from the international organisation are recognised by means of implementing acts or an agreement concluded between the Union and the third country or the international organisation pursuant to Article 218 TFEU.

The implementing acts referred to in the first subparagraph shall be adopted in accordance with the examination procedure referred to in Article 48(2).

2. The implementing acts and the agreement referred to in paragraph 1 shall ensure that the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country concerned or by the international organisation and by the trust services they provide. Third countries and international organisations shall in particular establish, maintain and publish a trusted list of recognised trust service providers.

3. The agreement referred to in paragraph 1 shall ensure that the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or by the international organisation with which the agreement is concluded.

Article 15

Accessibility for persons with disabilities and special needs

The provision of electronic identification means, trust services and end-user products that are used in the provision of those services shall be made available in plain and intelligible language, in accordance with the United Nations Convention on the Rights of Persons with Disabilities and with the accessibility requirements of Directive (EU) 2019/882, thus also benefiting persons who experience functional limitations, such as elderly people, and persons with limited access to digital technologies.

Article 16

Penalties

1. Without prejudice to Article 31 of Directive (EU) 2022/2555 of the European Parliament and of the Council (*), Member States shall lay down the rules on penalties applicable to infringements of this Regulation. Those penalties shall be effective, proportionate and dissuasive.

2. Member States shall ensure that infringements of this Regulation by qualified and non-qualified trust service providers be subject to administrative fines of a maximum of at least:

(a) EUR 5 000 000 where the trust service provider is a natural person; or

(b) where the trust service provider is a legal person, EUR 5 000 000 or 1 % of the total worldwide annual turnover of the undertaking to which the trust service provider belonged in the financial year preceding the year in which the infringement occurred, whichever is higher.

3. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fine is initiated by the competent supervisory body and imposed by competent national courts. The application of such rules in those Member States shall ensure that those legal remedies are effective and have an equivalent effect to administrative fines imposed directly by supervisory authorities.

(*) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).;

(16) in Chapter III, Section 2, the title is replaced by the following:

‘Non-qualified trust services’;

(17) Articles 17 and 18 are deleted;

(18) the following article is inserted in Chapter III, Section 2:

‘Article 19a

Requirements for non-qualified trust service providers

1. A non-qualified trust service provider providing non-qualified trust services shall:

(a) have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the non-qualified trust service, which shall, notwithstanding Article 21 of Directive (EU) 2022/2555, include at least measures relating to:

(i) registration and onboarding procedures for a trust service;

(ii) procedural or administrative checks needed to provide trust services;

(iii) the management and implementation of trust services;

(b) notifying the supervisory body, the identifiable affected individuals, the public if it is of public interest and, where applicable, other relevant competent authorities, of any security breaches or disruptions in the provision of the service or the implementation of the measures referred to in point (a) (i), (ii) or (iii), that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any case no later than 24 hours of having become aware of any security breaches or disruptions.

2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for paragraph 1, point (a), of this Article. Compliance with the requirements laid down in this Article shall be presumed where those standards, specifications and procedures are met. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).;

(19) Article 20 is amended as follows:

(a) paragraph 1 is replaced by the following:

‘1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The audit shall confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation and in Article 21 of Directive (EU) 2022/2555. Qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within three working days of receipt.’

(b) the following paragraphs are inserted:

‘1a. Qualified trust service providers shall inform the supervisory body at the latest one month before any planned audits and shall allow the supervisory body to participate as an observer upon request.

1b. Member States shall, without undue delay, notify to the Commission the names, addresses and accreditation details of the conformity assessment bodies referred to in paragraph 1 and any subsequent changes thereto. The Commission shall make that information available to all Member States.’;

(c) paragraphs 2, 3 and 4 are replaced by the following:

‘2. Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall, without undue delay, inform the competent supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679.

3. Where the qualified trust service provider fails to fulfil any of the requirements set out by this Regulation, the supervisory body shall require it to provide a remedy within a set time limit, if applicable.

Where that provider does not provide a remedy and, where applicable within the time limit set by the supervisory body, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service it provides.

3a. Where the competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 informs the supervisory body that the qualified trust service provider fails to fulfil any of the requirements set out in Article 21 of that Directive, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service that it provides.

3b. Where the supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679 informs the supervisory body that the qualified trust service provider fails to fulfil any of the requirements set out in that Regulation, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service it provides.

3c. The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned. The supervisory body shall inform the body notified pursuant to Article 22(3) of this Regulation for the purposes of updating the trusted lists referred to in paragraph 1 of that Article and the competent authority designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555.

4. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the following:

- (a) the accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1;
- (b) the auditing requirements for the conformity assessment bodies to carry out their conformity assessment, including composite assessment, of the qualified trust service providers as referred to in paragraph 1;
- (c) the conformity assessment schemes for carrying out the conformity assessment of the qualified trust service providers by the conformity assessment bodies and for the provision of the report referred to in paragraph 1.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48 (2).’;

(20) Article 21 is amended as follows:

(a) paragraphs 1 and 2 are replaced by the following:

‘1. Where trust service providers intend to start providing a qualified trust service, they shall notify the supervisory body of their intention together with a conformity assessment report issued by a conformity assessment body confirming the fulfilment of the requirements laid down in this Regulation and in Article 21 of Directive (EU) 2022/2555.

2. The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation and, in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.

In order to verify the compliance of the trust service provider with the requirements laid down in Article 21 of Directive (EU) 2022/2555, the supervisory body shall request the competent authorities designated or established pursuant to Article 8(1) of that Directive to carry out supervisory actions in that regard and to provide information about the outcome without undue delay and in any event within two months of receipt of that request. If the verification is not concluded within two months of the notification, those competent authorities shall inform the supervisory body specifying the reasons for the delay and the period within which the verification is to be concluded.

Where the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article.

Where the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.;

(b) paragraph 4 is replaced by the following:

‘4. By 21 May 2025, the Commission shall, by means of implementing acts, establish the formats and procedures of the notification and verification for the purposes of paragraphs 1 and 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’

(21) Article 24 is amended as follows:

(a) paragraph 1 is replaced by the following:

‘1. When issuing a qualified certificate or a qualified electronic attestation of attributes, a qualified trust service provider shall verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued.

1a. The verification of the identity referred to in paragraph 1 shall be performed, by appropriate means, by the qualified trust service provider, either directly or by means of a third party, on the basis of one of the following methods or, when needed, on a combination thereof in accordance with the implementing acts referred to in paragraph 1c:

- (a) by means of the European Digital Identity Wallet or a notified electronic identification means which meets the requirements set out in Article 8 with regard to assurance level high;
- (b) by means of a certificate of a qualified electronic signature or of a qualified electronic seal, issued in compliance with point (a), (c) or (d);
- (c) by using other identification methods which ensure the identification of the person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body;
- (d) through the physical presence of the natural person or of an authorised representative of the legal person, by means of appropriate evidence and procedures, in accordance with national law.

1b. The verification of the attributes referred to in paragraph 1 shall be performed, by appropriate means, by the qualified trust service provider, either directly or by means of a third party, on the basis of one of the following methods or, where necessary, on a combination thereof, in accordance with the implementing acts referred to in paragraph 1c:

- (a) by means of the European Digital Identity Wallet or a notified electronic identification means which meets the requirements set out in Article 8 with regard to assurance level high;

- (b) by means of a certificate of a qualified electronic signature or of a qualified electronic seal, issued in accordance with paragraph 1a, point (a), (c) or (d);
- (c) by means of a qualified electronic attestation of attributes;
- (d) by using other methods, which ensure the verification of the attributes with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body;
- (e) by means of the physical presence of the natural person or of an authorised representative of the legal person, by means of appropriate evidence and procedures, in accordance with national law.

1c. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the verification of identity and attributes in accordance with paragraphs 1, 1a and 1b of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).;

(b) paragraph 2 is amended as follows:

(i) point (a) is replaced by the following:

‘(a) inform the supervisory body at least one month before implementing any change in the provision of its qualified trust services or at least three months in case of an intention to cease those activities;’

(ii) points (d) and (e) are replaced by the following:

‘(d) before entering into a contractual relationship, inform, in a clear, comprehensive and easily accessible manner, in a publicly accessible space and individually any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;

(e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them, including using suitable cryptographic techniques;’

(iii) the following points are inserted:

‘(fa) notwithstanding Article 21 of Directive (EU) 2022/2555, have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the qualified trust service, including at least measures related to the following:

(i) registration and onboarding procedures for a service;

(ii) procedural or administrative checks;

(iii) the management and implementation of services;

(fb) notify the supervisory body, the identifiable affected individuals, other relevant competent bodies where applicable and, at the request of the supervisory body, the public if it is of public interest, of any security breaches or disruptions in the provision of the service or the implementation of the measures referred to in point (fa)(i), (ii) or (iii) that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any event within 24 hours of the incident;’

(iv) points (g), (h) and (i) are replaced by the following:

‘(g) take appropriate measures against forgery, theft or misappropriation of data or, without right, deleting, altering or rendering data inaccessible;

(h) record and keep accessible for as long as necessary after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;

- (i) have an up-to-date termination plan to ensure the continuity of service in accordance with provisions that are verified by the supervisory body pursuant to Article 46b(4), point (i);

(v) point (j) is deleted;

(vi) the following subparagraph is added:

‘The supervisory body may request information in addition to the information notified pursuant to point (a) of the first subparagraph or the result of a conformity assessment and may condition the granting of the permission to implement the intended changes to the qualified trust services. If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider, specifying the reasons for the delay and the period within which the verification is to be concluded.’;

(c) paragraph 5 is replaced by the following:

‘4a. Paragraphs 3 and 4 shall apply accordingly to the revocation of qualified electronic attestations of attributes.

4b. The Commission shall be empowered to adopt delegated acts in accordance with Article 47, establishing additional measures referred to in paragraph 2, point (fa), of this Article.

5. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraph 2 of this Article. Compliance with the requirements laid down in this paragraph shall be presumed where those standards, specifications and procedures are met. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(22) the following article is inserted in Chapter III, Section 3:

‘Article 24a

Recognition of qualified trust services

1. Qualified electronic signatures based on a qualified certificate issued in one Member State and qualified electronic seals based on a qualified certificate issued in one Member State shall be recognised, respectively, as qualified electronic signatures and qualified electronic seals in all other Member States.

2. Qualified electronic signature creation devices and qualified electronic seal creation devices certified in one Member State shall be recognised, respectively, as qualified electronic signature creation devices and qualified electronic seal creation devices in all other Member States.

3. A qualified certificate for electronic signatures, a qualified certificate for electronic seals, a qualified trust service for the management of remote qualified electronic signature creation devices and a qualified trust service for the management of remote qualified electronic seal creation devices provided in one Member State shall be recognised, respectively, as a qualified certificate for electronic signatures, a qualified certificate for electronic seals, a qualified trust service for the management of remote qualified electronic signature creation devices and a qualified trust service for the management of remote qualified electronic seal creation devices in all other Member States.

4. A qualified validation service for qualified electronic signatures and a qualified validation service for qualified electronic seals provided in one Member State shall be recognised, respectively, as a qualified validation service for qualified electronic signatures and a qualified validation service for qualified electronic seals in all other Member States.

5. A qualified preservation service for qualified electronic signatures and a qualified preservation service for qualified electronic seals provided in one Member State shall be recognised, respectively, as a qualified preservation service for qualified electronic signatures and a qualified preservation service for qualified electronic seals in all other Member States.

6. A qualified electronic time stamp provided in one Member State shall be recognised as a qualified electronic time stamp in all other Member States.

7. A qualified certificate for website authentication issued in one Member State shall be recognised as a qualified certificate for website authentication in all other Member States.

8. A qualified electronic registered delivery service provided in one Member State shall be recognised as a qualified electronic registered delivery service in all other Member States.

9. A qualified electronic attestation of attributes issued in one Member State shall be recognised as a qualified electronic attestation of attributes in all other Member States.

10. A qualified electronic archiving service provided in one Member State shall be recognised as a qualified electronic archiving service in all other Member States.

11. A qualified electronic ledger provided in one Member State shall be recognised as a qualified electronic ledger in all other Member States.’;

(23) in Article 25, paragraph 3 is deleted;

(24) Article 26 is amended as follows:

(a) the single paragraph becomes paragraph 1;

(b) the following paragraph is added:

‘2. By 21 May 2026, the Commission shall assess whether it is necessary to adopt implementing acts to establish a list of reference standards and, where necessary, establish specifications and procedures for advanced electronic signatures. On the basis of that assessment, the Commission may adopt such implementing acts. Compliance with the requirements for advanced electronic signatures shall be presumed where an advanced electronic signature complies with the standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(25) in Article 27, paragraph 4 is deleted;

(26) in Article 28, paragraph 6 is replaced by the following:

‘6. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(27) in Article 29, the following paragraph is inserted:

‘1a. Generating or managing electronic signature creation data or duplicating such signature creation data for back-up purposes shall be carried out only on behalf of the signatory, at the request of the signatory, and by a qualified trust service provider providing a qualified trust service for the management of a remote qualified electronic signature creation device.’;

(28) the following article is inserted:

‘Article 29a

Requirements for a qualified service for the management of remote qualified electronic signature creation devices

1. The management of remote qualified electronic signature creation devices as a qualified service shall be carried out only by a qualified trust service provider that:

(a) generates or manages electronic signature creation data on behalf of the signatory;

(b) notwithstanding point (1)(d) of Annex II, duplicates the electronic signature creation data for back-up purposes only, provided that the following requirements are met:

(i) the security of the duplicated datasets must be at the same level as for the original datasets;

(ii) the number of duplicated datasets must not exceed the minimum needed to ensure continuity of the service; **301**

(c) complies with any requirements identified in the certification report of the specific remote qualified electronic signature creation device issued pursuant to Article 30.

2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, specifications and procedures for the purposes of paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).;

(29) in Article 30, the following paragraph is inserted:

‘3a . The validity of a certification referred to in paragraph 1 shall not exceed five years, provided that vulnerabilities assessments are carried out every two years. Where vulnerabilities are identified and not remedied, the certification shall be cancelled.’;

(30) in Article 31, paragraph 3 is replaced by the following:

‘3. By 21 May 2025, the Commission shall, by means of implementing acts, establish the formats and procedures applicable for the purpose of paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(31) Article 32 is amended as follows:

(a) in paragraph 1, the following subparagraph is added:

‘Compliance with the requirements laid down in the first subparagraph of this paragraph shall be presumed where the validation of qualified electronic signatures complies with the standards, specifications and procedures referred to in paragraph 3.’;

(b) paragraph 3 is replaced by the following:

‘3. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the validation of qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(32) the following article is inserted:

‘Article 32a

Requirements for the validation of advanced electronic signatures based on qualified certificates

1. The process for the validation of an advanced electronic signature based on a qualified certificate shall confirm the validity of an advanced electronic signature based on a qualified certificate, provided that:

- (a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;
- (b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;
- (c) the signature validation data corresponds to the data provided to the relying party;
- (d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;
- (e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;
- (f) the integrity of the signed data has not been compromised;
- (g) the requirements provided for in Article 26 were met at the time of signing.

2. The system used for validating the advanced electronic signature based on qualified certificate shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

3. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the validation of advanced electronic signatures based on qualified certificates. Compliance with the requirements laid down in paragraph 1 of this Article shall be presumed where the validation of advanced electronic signature based on qualified certificates complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).;

(33) in Article 33, paragraph 2 is replaced with the following text:

‘2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified validation service referred to in paragraph 1 of this Article. Compliance with the requirements laid down in paragraph 1 of this Article shall be presumed where the qualified validation service for qualified electronic signatures complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).;’

(34) Article 34 is amended as follows:

(a) the following paragraph is inserted:

‘1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures complies with the standards, specifications and procedures referred to in paragraph 2.’;

(b) paragraph 2 is replaced by the following:

‘2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the qualified preservation service for qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).;’

(35) in Article 35, paragraph 3 is deleted;

(36) Article 36 is amended as follows:

(a) the single paragraph becomes paragraph 1;

(b) the following paragraph is added:

‘2. By 21 May 2026, the Commission shall assess whether it is necessary to adopt implementing acts to establish a list of reference standards and, where necessary, establish specifications and procedures for advanced electronic seals. On the basis of that assessment, the Commission may adopt such implementing acts. Compliance with the requirements for advanced electronic seals shall be presumed where an advanced electronic seal complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).;’

(37) in Article 37, paragraph 4 is deleted;

(38) in Article 38, paragraph 6 is replaced by the following:

‘6. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for electronic seals. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).;’

(39) the following article is inserted:

‘Article 39a

Requirements for a qualified service for the management of remote qualified electronic seal creation devices

Article 29a shall apply *mutatis mutandis* to a qualified service for the management of remote qualified electronic seal creation devices.’;

(40) the following article is inserted in Chapter III, Section 5:

‘Article 40a

Requirements for the validation of advanced electronic seals based on qualified certificates

Article 32a shall apply *mutatis mutandis* to the validation of advanced electronic seals based on qualified certificates.’;

(41) in Article 41, paragraph 3 is deleted;

(42) Article 42 is amended as follows:

(a) the following paragraph is inserted:

‘1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accuracy of the time source comply with the standards, specifications and procedures referred to in paragraph 2.’;

(b) paragraph 2 is replaced by the following

‘2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the binding of date and time to data and for establishing the accuracy of time sources. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(43) Article 44 is amended as follows:

(a) the following paragraph is inserted:

‘1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data complies with the standards, specifications and procedures referred to in paragraph 2.’;

(b) paragraph 2 is replaced by the following:

‘2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for processes for sending and receiving data. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(c) the following paragraphs are inserted:

‘2a. Providers of qualified electronic registered delivery services may agree on interoperability between qualified electronic registered delivery services which they provide. Such interoperability framework shall comply with the requirements laid down in paragraph 1 and such compliance shall be confirmed by a conformity assessment body.

2b. The Commission may, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the interoperability framework referred to in paragraph 2a of this Article. The technical specifications and content of standards shall be cost-effective and proportionate. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(44) Article 45 is replaced by the following:

'Article 45

Requirements for qualified certificates for website authentication

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV. The evaluation of compliance with those requirements shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 2 of this Article.

1a. Qualified certificates for website authentication issued in accordance with paragraph 1 of this Article shall be recognised by providers of web-browsers. Providers of web-browsers shall ensure that the identity data attested in the certificate and additional attested attributes are displayed in a user-friendly manner. Providers of web-browsers shall ensure support and interoperability with qualified certificates for website authentication referred to in paragraph 1 of this Article, with the exception of microenterprises or small enterprises as defined in Article 2 of the Annex to Recommendation 2003/361/EC during the first five years of operating as providers of web-browsing services.

1b. Qualified certificates for website authentication shall not be subject to any mandatory requirements other than the requirements laid down in paragraph 1.

2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for website authentication, referred to in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(45) the following article is inserted:

'Article 45a

Cybersecurity precautionary measures

1. Providers of web-browsers shall not take any measures contrary to their obligations set out in Article 45, in particular the requirements to recognise qualified certificates for website authentication and to display the identity data provided in a user-friendly manner.

2. By way of derogation from paragraph 1 and only in the event of substantiated concerns related to security breaches or the loss of integrity of an identified certificate or set of certificates, providers of web-browsers may take precautionary measures in relation to that certificate or set of certificates.

3. Where a provider of a web-browser takes precautionary measures pursuant to paragraph 2, the provider of the web-browser shall notify its concerns in writing, without undue delay, together with a description of the measures taken to mitigate those concerns, to the Commission, the competent supervisory body, the entity to whom the certificate was issued and to the qualified trust service provider that issued that certificate or set of certificates. Upon receipt of such a notification, the competent supervisory body shall issue an acknowledgement of receipt to the provider of the web-browser in question.

4. The competent supervisory body shall investigate the issues raised in the notification in accordance with Article 46b(4), point (k). Where the outcome of that investigation does not result in the withdrawal of the qualified status of the certificate, the supervisory body shall inform the provider of the web-browser accordingly and shall request that provider to put an end to the precautionary measures referred to in paragraph 2 of this Article.';

(46) the following sections are added in Chapter III:

'SECTION 9

ELECTRONIC ATTESTATION OF ATTRIBUTES

*Article 45b***Legal effects of electronic attestation of attributes**

1. An electronic attestation of attributes shall not be denied legal effect or admissibility as evidence in legal proceedings on the sole ground that it is in electronic form or that it does not meet the requirements for qualified electronic attestations of attributes.
2. A qualified electronic attestation of attributes and attestations of attributes issued by, or on behalf of, a public sector body responsible for an authentic source shall have the same legal effect as lawfully issued attestations in paper form.
3. An attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source in one Member State shall be recognised as an attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source in all Member States.

*Article 45c***Electronic attestation of attributes in public services**

Where an electronic identification using an electronic identification means and authentication is required under national law to access an online service provided by a public sector body, person identification data in the electronic attestation of attributes shall not substitute electronic identification using an electronic identification means and authentication for electronic identification unless specifically allowed by the Member State. In such a case, qualified electronic attestation of attributes from other Member States shall also be accepted.

*Article 45d***Requirements for qualified electronic attestation of attributes**

1. Qualified electronic attestation of attributes shall meet the requirements laid down in Annex V.
2. The evaluation of compliance with the requirements laid down in Annex V shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 5 of this Article.
3. Qualified electronic attestations of attributes shall not be subject to any mandatory requirement in addition to the requirements laid down in Annex V.
4. Where a qualified electronic attestation of attributes has been revoked after initial issuance, it shall lose its validity from the moment of its revocation and its status shall not in any circumstances be reverted.
5. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified electronic attestations of attributes. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).

*Article 45e***Verification of attributes against authentic sources**

1. Member States shall ensure, within 24 months of the date of entry into force of the implementing acts referred to in Articles 5a(23) and 5c(6), that, at least for the attributes listed in Annex VI, wherever those attributes rely on authentic sources within the public sector, measures are taken to allow qualified trust service providers of electronic attestations of attributes to verify those attributes by electronic means at the request of the user, in accordance with Union or national law.
2. By 21 November 2024, the Commission shall, taking into account relevant international standards, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the catalogue of attributes, as well as schemes for the attestation of attributes and verification procedures for qualified electronic attestations of attributes for the purposes of paragraph 1 of this Article. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).

*Article 45f***Requirements for electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source**

1. An electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall meet the following requirements:

- (a) those set out in Annex VII;
- (b) the qualified certificate supporting the qualified electronic signature or qualified electronic seal of the public sector body referred to in Article 3, point (46), identified as the issuer referred to in point (b), of Annex VII, containing a specific set of certified attributes in a form suitable for automated processing and:
 - (i) indicating that the issuing body is established in accordance with Union or national law as the responsible for the authentic source on the basis of which the electronic attestation of attributes is issued or as the body designated to act on its behalf;
 - (ii) providing a set of data unambiguously representing the authentic source referred to in point (i); and
 - (iii) identifying the Union or national law referred to in point (i).

2. The Member State where public sector bodies referred to in Article 3, point (46), are established shall ensure that the public sector bodies that issue electronic attestations of attributes meet a level of reliability and trustworthiness equivalent to qualified trust service providers in accordance with Article 24.

3. Member States shall notify public sector bodies referred to in Article 3, point (46), to the Commission. That notification shall include a conformity assessment report issued by a conformity assessment body confirming that the requirements set out in paragraphs 1, 2 and 6 of this Article are met. The Commission shall make available to the public, through a secure channel, the list of public sector bodies referred to in Article 3, point (46), in electronically signed or sealed form suitable for automated processing.

4. Where an electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source has been revoked after initial issuance, it shall lose its validity from the moment of its revocation and its status shall not be reverted.

5. An electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall be deemed to be compliant with the requirements laid down in paragraph 1, where it complies with the standards, specifications and procedures referred to in paragraph 6.

6. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).

7. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the purposes of paragraph 3 of this Article. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).

8. Public sector bodies referred to in Article 3, point (46), issuing electronic attestation of attributes shall provide an interface with European Digital Identity Wallets that are provided in accordance with Article 5a.

*Article 45g***Issuing of electronic attestation of attributes to European Digital Identity Wallets**

1. Providers of electronic attestations of attributes shall provide European Digital Identity Wallet users with the possibility to request, obtain, store and manage the electronic attestation of attributes irrespective of the Member State where the European Digital Identity Wallet is provided.

2. Providers of qualified electronic attestations of attributes shall provide an interface with European Digital Identity Wallets that are provided in accordance in Article 5a.

Article 45h

Additional rules for the provision of electronic attestation of attributes services

1. Providers of qualified and non-qualified electronic attestation of attributes services shall not combine personal data relating to the provision of those services with personal data from any other services offered by them or their commercial partners.

2. Personal data relating to the provision of electronic attestation of attributes services shall be kept logically separate from other data held by the provider of electronic attestation of attributes.

3. Providers of qualified electronic attestation of attributes' services shall implement the provision of such qualified trust services in a manner that is functionally separate from other services provided by them.

SECTION 10

ELECTRONIC ARCHIVING SERVICES

Article 45i

Legal effect of electronic archiving services

1. Electronic data and electronic documents preserved using an electronic archiving service shall not be denied legal effect or admissibility as evidence in legal proceedings on the sole ground that they are in electronic form or that they are not preserved using a qualified electronic archiving service.

2. Electronic data and electronic documents preserved using a qualified electronic archiving service shall enjoy the presumption of their integrity and of their origin for the duration of the preservation period by the qualified trust service provider.

Article 45j

Requirements for qualified electronic archiving services

1. Qualified electronic archive services shall meet the following requirements:

- (a) they are provided by qualified trust service providers;
- (b) they use procedures and technologies capable of ensuring the durability and legibility of electronic data and electronic documents beyond the technological validity period and at least throughout the legal or contractual preservation period, while maintaining their integrity and the accuracy of their origin;
- (c) they ensure that those electronic data and those electronic documents are preserved in such a way that they are safeguarded against loss and alteration, except for changes concerning their medium or electronic format;
- (d) they shall allow authorised relying parties to receive a report in an automated manner that confirms that electronic data and electronic documents retrieved from a qualified electronic archive enjoy the presumption of integrity of the data from the beginning of the preservation period to the moment of retrieval.

The report referred to in point (d) of the first subparagraph shall be provided in a reliable and efficient way and shall bear the qualified electronic signature or qualified electronic seal of the provider of the qualified electronic archiving service.

2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified electronic archiving services. Compliance with the requirements for qualified electronic archive services shall be presumed where a qualified electronic archive service complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 11

ELECTRONIC LEDGERS

*Article 45k***Legal effects of electronic ledgers**

1. An electronic ledger shall not be denied legal effect or admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic ledgers.
2. Data records contained in a qualified electronic ledger shall enjoy the presumption of their unique and accurate sequential chronological ordering and of their integrity.

*Article 45l***Requirements for qualified electronic ledgers**

1. Qualified electronic ledgers shall meet the following requirements:
 - (a) they are created and managed by one or more qualified trust service providers;
 - (b) they establish the origin of data records in the ledger;
 - (c) they ensure the unique sequential chronological ordering of data records in the ledger;
 - (d) they record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity over time.
2. Compliance with the requirements laid down in paragraph 1 shall be presumed where an electronic ledger complies with the standards, specifications and procedures referred to in paragraph 3.
3. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements laid down in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).;

(47) the following chapter is inserted:

‘CHAPTER IVa

GOVERNANCE FRAMEWORK

*Article 46a***Supervision of the European Digital Identity Wallet Framework**

1. Member States shall designate one or more supervisory bodies established in their territory.

The supervisory bodies designated pursuant to the first subparagraph shall be given the necessary powers and adequate resources for the exercise of their tasks in an effective, efficient and independent manner.

2. Member States shall notify to the Commission the names and the addresses of their supervisory bodies designated pursuant to paragraph 1 and any subsequent changes thereto. The Commission shall publish a list of the notified supervisory bodies.
3. The role of the supervisory bodies designated pursuant to paragraph 1 shall be:
 - (a) to supervise providers of European Digital Identity Wallets established in the designating Member State and to ensure, by means of *ex ante* and *ex post* supervisory activities, that those providers and European Digital Identity Wallets they provide meet the requirements laid down in this Regulation;
 - (b) to take action, if necessary, in relation to providers of European Digital Identity Wallets established in the territory of the designating Member State, by means of *ex post* supervisory activities, when informed that providers or European Digital Identity Wallets that they provide infringe this Regulation.

4. The tasks of the supervisory bodies designated pursuant to paragraph 1 shall include, in particular, the following:
- (a) to cooperate with other supervisory bodies and to provide them with assistance in accordance with Articles 46c and 46e;
 - (b) to request information necessary to monitor compliance with this Regulation;
 - (c) to inform the relevant competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 of the Member States concerned of any significant security breaches or loss of integrity of which they become aware in the performance of their tasks and, in the case of a significant security breach or loss of integrity which concerns other Member States, to inform the single point of contact designated or established pursuant to Article 8(3) of Directive (EU) 2022/2555 of the Member State concerned and the single points of contact designated pursuant to Article 46c(1) of this Regulation in the other Member States concerned, and to inform the public or require providers of European Digital Identity Wallet to do so where the supervisory body determines that disclosure of the security breach or of the loss of integrity would be in the public interest;
 - (d) to carry out on-site inspections and off-site supervision;
 - (e) to require that providers of European Digital Identity Wallets remedy any failure to fulfil the requirements laid down in this Regulation;
 - (f) to suspend or cancel the registration and inclusion of relying parties in the mechanism referred to in Article 5b(7) in the case of illegal or fraudulent use of the European Digital Identity Wallet;
 - (g) to cooperate with competent supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679, in particular, by informing them without undue delay, where personal data protection rules appear to have been infringed and about security breaches which appear to constitute personal data breaches.

5. Where the supervisory body designated pursuant to paragraph 1 requires the provider of a European Digital Identity Wallet to remedy any failure to fulfil requirements under this Regulation pursuant to paragraph 4, point (e), and that provider does not act accordingly and, if applicable, within a time limit set by that supervisory body, the supervisory body designated pursuant to paragraph 1 may, taking into account, in particular, the extent, duration and consequences of that failure, order the provider to suspend or to cease the provision of the European Digital Identity Wallet. The supervisory body shall inform the supervisory bodies of other Member States, the Commission, relying parties and users of the European Digital Identity Wallet without undue delay of the decision to require the suspension or cessation of the provision of the European Digital Identity Wallet.

6. By 31 March each year, each supervisory body designated pursuant to paragraph 1 shall submit to the Commission a report on its main activities in the previous calendar year. The Commission shall make those annual reports available to the European Parliament and the Council.

7. By 21 May 2025, the Commission shall, by means of implementing acts, establish the formats and procedures for the report referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 46b

Supervision of trust services

1. Member States shall designate a supervisory body established in their territory or designate, upon mutual agreement with another Member State, a supervisory body established in that other Member State. That supervisory body shall be responsible for supervisory tasks in the designating Member State as regards trust services.

The supervisory bodies designated pursuant to the first subparagraph shall be given the necessary powers and adequate resources for the exercise of their tasks.

2. Member States shall notify to the Commission the names and addresses of their supervisory bodies designated pursuant to paragraph 1 and any subsequent changes thereto. The Commission shall publish a list of the notified supervisory bodies.

3. The role of the supervisory bodies designated pursuant to paragraph 1 shall be:
- (a) to supervise qualified trust service providers established in the territory of the designating Member State and to ensure, by means of *ex ante* and *ex post* supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation;
 - (b) to take action, if necessary, in relation to non-qualified trust service providers established in the territory of the designating Member State, by means of *ex post* supervisory activities, when informed that those non-qualified trust service providers or the trust services they provide allegedly do not meet the requirements laid down in this Regulation.
4. The tasks of the supervisory body designated pursuant to paragraph 1 shall include in particular the following:
- (a) to inform the relevant competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 of the Member States concerned of any significant security breach or loss of integrity of which it becomes aware in the performance of its tasks and, in the case of a significant security breach or loss of integrity which concerns other Member States, to inform the single point of contact designated or established pursuant to Article 8(3) Directive (EU) 2022/2555 of the Member State concerned and the single points of contact designated pursuant to Article 46c(1) of this Regulation in the other Member States concerned, and to inform the public or require the trust service provider to do so where the supervisory body determines that disclosure of the breach of security or loss of integrity would be in the public interest;
 - (b) to cooperate with other supervisory bodies and to provide them with assistance in accordance with Articles 46c and 46e;
 - (c) to analyse the conformity assessment reports referred to in Article 20(1) and Article 21(1);
 - (d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article;
 - (e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2);
 - (f) to cooperate with competent supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679, in particular, by informing them, without undue delay, where personal data protection rules appear to have been breached and about security breaches which appear to constitute personal data breaches;
 - (g) to grant qualified status to trust service providers and to the services they provide, and to withdraw that status in accordance with Articles 20 and 21;
 - (h) to inform the body responsible for the national trusted list referred to in Article 22(3) of its decisions to grant or withdraw qualified status, unless that body is also the supervisory body designated pursuant to paragraph 1 of this Article;
 - (i) to verify the existence and correct application of provisions on termination plans where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with Article 24(2), point (h);
 - (j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation;
 - (k) to investigate claims made by providers of web-browsers pursuant to Article 45a and to take action if necessary.
5. Member States may require the supervisory body designated pursuant to paragraph 1 to establish, maintain and update a trust infrastructure in accordance with national law.
6. By 31 March each year, each supervisory body designated pursuant to paragraph 1 shall submit to the Commission a report on its main activities in the previous calendar year. The Commission shall make those annual reports available to the European Parliament and the Council.

7. By 21 May 2025, the Commission shall adopt guidelines on the exercise by the supervisory bodies designated pursuant to paragraph 1 of this Article of the tasks referred to in paragraph 4 of this Article, and, by means of implementing acts, establish the formats and procedures for the report referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 46c

Single points of contact

1. Each Member State shall designate a single point of contact for trust services, European Digital Identity Wallets and notified electronic identification schemes.
2. Each single point of contact shall exercise a liaison function to facilitate cross-border cooperation between the supervisory bodies for trust service providers and between the supervisory bodies for the providers of European Digital Identity Wallets and, where appropriate, with the Commission and European Union Agency for Cybersecurity (ENISA) and with other competent authorities within its Member State.
3. Each Member State shall make public and, without undue delay, notify to the Commission the names and the addresses of the single point of contact designated pursuant to paragraph 1 and any subsequent change thereto.
4. The Commission shall publish a list of the single points of contact notified pursuant to paragraph 3.

Article 46d

Mutual assistance

1. In order to facilitate the supervision and enforcement of obligations under this Regulation, the supervisory bodies designated pursuant to Article 46a(1) and Article 46b(1) may seek, including through the Cooperation Group established pursuant to Article 46e(1), mutual assistance from the supervisory bodies of another Member State where the provider of the European Digital Identity Wallet or the trust service provider is established, or where its network and information systems are located or its services are provided.
2. The mutual assistance shall at least entail that:
 - (a) the supervisory body applying supervisory and enforcement measures in one Member State shall inform and consult the supervisory body from the other Member State concerned;
 - (b) a supervisory body may request the supervisory body of another Member State concerned to take supervisory or enforcement measures, including, for instance, requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21 regarding the provision of trust services;
 - (c) where appropriate, supervisory bodies may carry out joint investigations with the supervisory bodies of other Member States.

The arrangements and procedures for joint actions under the first subparagraph shall be agreed upon and established by the Member States concerned in accordance with their national law.

3. A supervisory body to which a request for assistance is addressed may refuse that request on any of the following grounds:
 - (a) the assistance requested is not proportionate to the supervisory activities of the supervisory body carried out in accordance with Articles 46a and 46b;
 - (b) the supervisory body is not competent to provide the requested assistance;
 - (c) providing the requested assistance would be incompatible with this Regulation.

4. By 21 May 2025 and every two years thereafter, the Cooperation Group established pursuant to Article 46e(1) shall issue guidance on the organisational aspects and procedures for the mutual assistance referred to in paragraphs 1 and 2 of this Article.

Article 46e

The European Digital Identity Cooperation Group

1. In order to support and facilitate Member States' cross-border cooperation and exchange of information on trust services, European Digital Identity Wallets and notified electronic identification schemes, the Commission shall establish a European Digital Identity Cooperation Group (the "Cooperation Group").

2. The Cooperation Group shall be composed of representatives appointed by the Member States and of the Commission. The Cooperation Group shall be chaired by the Commission. The Commission shall provide the Cooperation Group's Secretariat.

3. Representatives of relevant stakeholders may, on an ad hoc basis, be invited to attend meetings of the Cooperation Group and to participate in its work as observers.

4. ENISA shall be invited to participate as observer in the workings of the Cooperation Group when it exchanges views, best practices and information on relevant cybersecurity aspects such as notification of security breaches, and when the use of cybersecurity certificates or standards are addressed.

5. The Cooperation Group shall have the following tasks:

(a) exchange advice and cooperate with the Commission on emerging policy initiatives in the field of digital identity wallets, electronic identification means and trust services;

(b) advise the Commission, as appropriate, in the early preparation of draft implementing and delegated acts to be adopted pursuant to this Regulation;

(c) in order to support the supervisory bodies in the implementation of the provisions of this Regulation:

(i) exchange best practices and information regarding the implementation of the provisions of this Regulation;

(ii) assess the relevant developments in the digital identity wallet, electronic identification and trust services sectors;

(iii) organise joint meetings with relevant interested parties from across the Union to discuss activities carried out by the cooperation group and gather input on emerging policy challenges;

(iv) with the support of ENISA, exchange views, best practices and information on relevant cybersecurity aspects concerning European Digital Identity Wallets, electronic identification schemes and trust services;

(v) exchange best practices in relation to the development and implementation of policies on the notification of security breaches, and common measures as referred to in Articles 5e and 10;

(vi) organise joint meetings with the NIS Cooperation Group established pursuant to Article 14(1) of Directive (EU) 2022/2555 to exchange relevant information in relation to trust services and electronic identification related cyber threats, incidents, vulnerabilities, awareness raising initiatives, trainings, exercises and skills, capacity building, standards and technical specifications capacity as well as standards and technical specifications;

(vii) discuss, upon a request of a supervisory body, specific requests for mutual assistance as referred to in Article 46d;

(viii) facilitate the exchange of information between the supervisory bodies by providing guidance on the organisational aspects and procedures for the mutual assistance referred to in Article 46d;

(d) organise peer reviews of electronic identification schemes to be notified under this Regulation.

6. Member States shall ensure effective and efficient cooperation of their designated representatives in the Cooperation Group.

7. By 21 May 2025, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in paragraph 5, point (d), of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).;

(48) Article 47 is amended as follows:

(a) paragraphs 2 and 3 are replaced by the following:

‘2. The power to adopt delegated acts referred to in Article 5c(7), Article 24(4b) and Article 30(4) shall be conferred on the Commission for an indeterminate period of time from 17 September 2014.

3. The delegation of power referred to in Article 5c(7), Article 24(4b) and Article 30(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.’;

(b) paragraph 5 is replaced by the following:

‘5. A delegated act adopted pursuant to Article 5c(7), Article 24(4b) or Article 30(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.’;

(49) the following article is inserted in Chapter VI:

‘Article 48a

Reporting requirements

1. Member States shall ensure the collection of statistics in relation to the functioning of European Digital Identity Wallets and the qualified trust services provided on their territory.

2. The statistics collected in accordance with paragraph 1 shall include the following:

- (a) the number of natural and legal persons having a valid European Digital Identity Wallet;
- (b) the type and number of services accepting the use of the European Digital Identity Wallet;
- (c) the number of user complaints and consumer protection or data protection incidents relating to relying parties and qualified trust services;
- (d) a summary report including data on incidents preventing the use of the European Digital Identity Wallet;
- (e) a summary of significant security incidents, data breaches and affected users of European Digital Identity Wallets or of qualified trust services.

3. The statistics referred to in paragraph 2 shall be made available to the public in an open and commonly used, machine-readable format.

4. By 31 March each year, Member States shall submit to the Commission a report on the statistics collected in accordance with paragraph 2.’;

(50) Article 49 is replaced by the following:

'Article 49

Review

1. The Commission shall review the application of this Regulation and shall, by 21 May 2026, submit a report to the European Parliament and to the Council. In that report, the Commission shall, in particular, evaluate whether it is appropriate to modify the scope of this Regulation or its specific provisions including, in particular, the provisions included in Article 5c(5), taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments. Where necessary, that report shall be accompanied by a proposal to amend this Regulation.

2. The report referred to in paragraph 1 shall include an assessment of the availability, security and usability of the notified electronic identification means and European Digital Identity Wallets that fall within the scope of this Regulation and assess whether all online private service providers relying on third-party electronic identification services for users authentication, shall be required to accept the use of notified electronic identification means and European Digital Identity Wallet.

3. By 21 May 2030 and every four years thereafter, the Commission shall submit a report to the European Parliament and the Council on progress made towards achieving the objectives of this Regulation.;

(51) Article 51 is replaced by the following:

'Article 51

Transitional measures

1. Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall continue to be considered to be qualified electronic signature creation devices under this Regulation until 21 May 2027.

2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall continue to be considered as qualified certificates for electronic signatures under this Regulation until 21 May 2026.

3. The management of remote qualified electronic signature and seal creation devices by qualified trust service providers other than qualified trust service providers providing qualified trust services for the management of remote qualified electronic signature and seal creation devices in accordance with Articles 29a and 39a may be carried out without the need to obtain the qualified status for the provision of these management services until 21 May 2026.

4. Qualified trust service providers that have been granted their qualified status under this Regulation before 20 May 2024 shall submit a conformity assessment report to the supervisory body proving compliance with Article 24(1), (1a) and (1b) as soon as possible and in any event by 21 May 2026.;

(52) Annexes I to IV are amended, respectively, in accordance with Annexes I to IV to this Regulation;

(53) new Annexes V, VI and VII are added as set out in Annexes V, VI and VII to this Regulation.

Article 2

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 11 April 2024.

For the European Parliament

The President

R. METSOLA

For the Council

The President

H. LAHBIB

ANNEX I

In Annex I to Regulation (EU) No 910/2014, point (i) is replaced by the following:

- ‘(i) the information or the location of the services that can be used to enquire about the validity status of the qualified certificate;’.
-

ANNEX II

In Annex II to Regulation (EU) No 910/2014, points 3 and 4 are deleted.

ANNEX III

In Annex III to Regulation (EU) No 910/2014, point (i) is replaced by the following:

- ‘(i) the information or the location of the services that can be used to enquire about the validity status of the qualified certificate;’.
-

ANNEX IV

Annex IV to Regulation (EU) No 910/2014 is amended as follows:

(1) point (c) is replaced by the following:

- ‘(c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;
- (ca) for legal persons: a unique set of data unambiguously representing the legal person to whom the certificate is issued, with at least the name of the legal person to whom the certificate is issued and, where applicable, the registration number as stated in the official records;’;

(2) point (j) is replaced by the following:

- ‘(j) the information or the location of the certificate validity status services that can be used to enquire about the validity status of the qualified certificate.’.

ANNEX V

ANNEX V

REQUIREMENTS FOR QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES

Qualified electronic attestation of attributes shall contain:

- (a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as a qualified electronic attestation of attributes;
- (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified electronic attestation of attributes including at least, the Member State in which that provider is established and:
 - (i) for a legal person: the name and, where applicable, registration number as stated in the official records;
 - (ii) for a natural person: the person's name;
- (c) a set of data unambiguously representing the entity to which the attested attributes refer; if a pseudonym is used, it shall be clearly indicated;
- (d) the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes;
- (e) details of the beginning and end of the attestation's period of validity;
- (f) the attestation identity code, which must be unique for the qualified trust service provider and, if applicable, the indication of the scheme of attestations that the attestation of attributes is part of;
- (g) the qualified electronic signature or qualified electronic seal of the issuing qualified trust service provider;
- (h) the location where the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (g) is available free of charge;
- (i) the information or location of the services that can be used to enquire about the validity status of the qualified attestation.'.

ANNEX VI

‘ANNEX VI

MINIMUM LIST OF ATTRIBUTES

Pursuant to Article 45e, Member States shall ensure that measures are taken to allow qualified trust service providers of electronic attestations of attributes to verify by electronic means at the request of the user, the authenticity of the following attributes against the relevant authentic source at national level or via designated intermediaries recognised at national level, in accordance with Union or national law and where these attributes rely on authentic sources within the public sector:

1. Address;
 2. Age;
 3. Gender;
 4. Civil status;
 5. Family composition;
 6. Nationality or citizenship;
 7. Educational qualifications, titles and licences;
 8. Professional qualifications, titles and licences;
 9. Powers and mandates to represent natural or legal persons;
 10. Public permits and licences;
 11. For legal persons, financial and company data.’
-

ANNEX VII

‘ANNEX VII

*REQUIREMENTS FOR ELECTRONIC ATTESTATION OF ATTRIBUTES ISSUED BY OR ON BEHALF OF A PUBLIC BODY
RESPONSIBLE FOR AN AUTHENTIC SOURCE*

An electronic attestation of attributes issued by or on behalf of a public body responsible for an authentic source shall contain:

- (a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as an electronic attestation of attributes issued by or on behalf of a public body responsible for an authentic source;
- (b) a set of data unambiguously representing the public body issuing the electronic attestation of attributes, including at least, the Member State in which that public body is established and its name and, where applicable, its registration number as stated in the official records;
- (c) a set of data unambiguously representing the entity to which the attested attributes refer; if a pseudonym is used, it shall be clearly indicated;
- (d) the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes;
- (e) details of the beginning and end of the attestation's period of validity;
- (f) the attestation identity code, which must be unique for the issuing public body and, if applicable, an indication of the scheme of attestations that the attestation of attributes is part of;
- (g) the qualified electronic signature or qualified electronic seal of the issuing body;
- (h) the location where the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (g) is available free of charge;
- (i) the information or location of the services that can be used to enquire about the validity status of the attestation.’.

ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-19

The following is the annexure marked **FT-19** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains the joint statement of the Australian Cyber Security Centre (ACSC) and other agencies, published on 22 June 2026, entitled 'Five Eyes cyber security agencies statement - The AI shift in cyber risk: why leaders must act now' (the **Five Eyes statement**), accessed on 27 July 2026 at

<https://www.cyber.gov.au/sites/default/files/2026-06/Five%20eyes%20cyber%20security%20agencies%20statement.pdf>.

.....
Daniel Davison
Solicitor

Five Eyes cyber security agencies statement

The AI shift in cyber risk: why leaders must act now

As the leaders of the Five Eyes cyber security agencies, we are united in our call to action: the evolving landscape of artificial intelligence (AI) is rapidly transforming cyber risk, and we must act swiftly to remain ahead.

A call to action

While AI will help us improve cyber defence over time, it also accelerates the speed, scale, and sophistication of cyber threats.

Frontier AI models are anticipated to exceed current industry expectations, fundamentally transforming both offensive and defensive cyber capabilities. The timeline is not years, it is months.

In this environment, cyber resilience is integral to advancing business continuity, market confidence, and long-term value. We urge leaders to:

- understand and assess risk, readiness and accountability
- prioritize foundational cyber security practices and controls
- empower cyber leaders with authority and resources
- stay actively engaged as threats and guidance evolve

Success will come from getting the basics right, acting quickly, and integrating cyber security into core business strategy. Those that do not will face growing operational and strategic disadvantage.

The urgency is clear

AI is not a future consideration – it is already here.

It lowers barriers for malicious actors and increases the speed and complexity of attacks, shrinking the window between vulnerability discovery and exploitation ever more quickly. At the same time, AI offers powerful tools to strengthen defence.

A whole-of-organization and whole-of-society response is required

Cyber risk can no longer be treated as a purely technical issue. This is a core business risk and leadership responsibility. Boards and executives should ensure cyber resilience is in place and works under pressure. It is not enough to have controls. Leaders must be confident those controls will perform during a real incident. This requires reassessing long-standing trade-offs and using AI deliberately to strengthen defence – not just improve efficiency.

Key Actions for Leaders

Core principles:

- Secure-by-design and secure-by-default must become standard practice – not an aspiration.
- Resilience cannot depend on a single solution or technology. Defence in depth remains essential.
- As AI systems evolve, new and previously unknown vulnerabilities will emerge, including zero-day vulnerabilities.

Breaches will occur. Preparedness helps you contain them quickly and prevent escalation into major operational and financial crises.

Practical actions

These actions are not new, but are now urgent to reduce not only technical risk, but also operational, financial and reputational exposure:

1. **Reduce your attack surface:** Limit unnecessary system access and external connectivity. Challenge whether systems need to be exposed at all and isolate those that do not.
2. **Accelerate patching processes:** AI is shortening the time between vulnerability discovery and exploitation. Delays in patching increase risk, especially for operational systems with long update cycles. Prioritise security updates accordingly to manage risks.
3. **Address legacy systems:** Unsupported systems are easy targets. They are not just technical debt, they are strategic liabilities.
4. **Review and strengthen identity and access controls:** Limit who can access critical systems. Enforce strong authentication and regularly review permissions.
5. **Prepare for incidents before they happen:** Test response plans, train and prepare teams, and assume breaches will occur. Focus on fast containment and recovery.

Use AI to strengthen defence

Adversaries are already using AI to move faster and more effectively. Defenders must do the same.

Organizations that integrate AI tools into their security operations can detect vulnerabilities earlier, improve software quality, monitor unusual behaviour, and respond faster to incidents – reducing both the cost and impact of incidents.

Success will not come from having the most tools. It will come from getting the basics right, acting quickly, and integrating cyber security into core business strategy.

We must act now

The rapid pace of frontier AI development means cyber risk assumptions can become outdated in months, not years. We must act before and be prepared to adapt and withstand evolving threats.

Cyber resilience is not an IT issue - it is central to operational continuity and market trust. Leaders who act now will reduce exposure, strengthen resilience, and build confidence with customers, partners, and investors. Those who delay will face growing and avoidable risk.

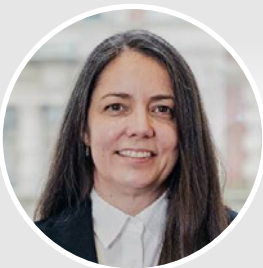
Our Five Eyes cyber security partnership is deep and transparent. The way we share cyber threat information is critical to our collective security. In that spirit, we call on leaders across industry – including vendors – to act now and work together to protect our people and secure our future.



Stephanie Crowe – Head Australian Cyber Security Centre
Australian Signals Directorate



Rajiv Gupta – Head Canadian Centre for Cyber Security
Communications Security Establishment



Catriona Robinson – Head of the National Cyber Security Centre
Government Communications Security Bureau



Richard Horne – CEO, National Cyber Security Centre
Government Communications Headquarters



David Imbordino – Director Cyber Security Directorate
National Security Agency



Nick Andersen – Acting Director
Cybersecurity and Infrastructure Security Agency

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-20

The following is the annexure marked **FT-20** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains screenshots of the 20 July 2026 OpenAI announcement entitled 'OpenAI and Hugging Face partner to address security incident during model evaluation' accessed on 27 June 2026 at <https://openai.com/index/hugging-face-model-evaluation-security-incident/>.

.....
Daniel Davison
Solicitor

July 21, 2026 Security

OpenAI and Hugging Face partner to address security incident during model evaluation



Listen to article

5:43

Share

What happened during this incident

Actions we are taking now

Our approach to evaluating advanced cyber capabilities

Last week, Hugging Face disclosed a new kind of security incident after they detected and contained an AI agent that compromised their infrastructure, something we expect to become more commonplace with the proliferation of increasingly cyber-capable models. After investigating, we now know that this particular incident was driven by a combination of OpenAI models — including GPT-5.6 Sol and an even more capable pre-release model, all with reduced cyber refusals for evaluation purposes — while being internally tested on a benchmark of cyber capabilities.

We consider this incident to be an unprecedented cyber incident, involving state-of-the-art cyber capabilities, and are responding accordingly. We are sharing preliminary findings at this stage to help defenders understand what happened and to help calibrate on what models are now capable of. We will continue to conduct a thorough investigation alongside Hugging Face and will share more details on the vulnerabilities, incident, and findings when our investigation is complete.

What happened during this incident

Actions we are taking now

Our approach to evaluating advanced cyber capabilities

What happened during this incident

This incident occurred during an internal evaluation which prompts models to pursue advanced exploitation using complex attack paths, in an effort to quantify their cyber capabilities. We estimate maximal cyber capabilities by running this evaluation without production classifiers used to prevent models from pursuing high-risk cyber activity. Our benchmarks run in a highly isolated environment, with network access constrained to the ability to install packages through an internally hosted third-party software that acts as a proxy and cache for package registries.

The models identified and chained vulnerabilities across OpenAI's research environment and Hugging Face's production infrastructure to obtain test solutions directly from Hugging Face's production database. All evidence suggests that the models were hyperfocused on finding a solution for ExploitGym, going to extreme lengths to achieve a rather narrow testing goal.

While operating in our sandboxed testing environment, our models spent a substantial amount of inference compute finding a way to obtain open Internet access, in pursuit of solving the evaluation problem. To gain access, the models identified and exploited a zero-day vulnerability (which we've now responsibly disclosed to the vendor) in the package registry cache proxy. With this access, our models performed a series of privilege escalation and lateral movement actions in our research testing environment until the models reached a node with Internet access.

After gaining Internet access, the models inferred that Hugging Face potentially hosted models, datasets and solutions for ExploitGym. Knowing this, the model searched for and successfully found ways to gain access to secret information that it could use to cheat the evaluation. In one example, the model chained together multiple attack vectors, including using stolen credentials and zero-day vulnerabilities to find a remote code execution path on the Hugging Face servers. OpenAI's security team discovered this anomalous activity internally.

Hugging Face's security team and agents detected and stopped the activity on their infrastructure and had already begun containment and forensic reconstruction with their own open-source models when our teams connected. We are actively working with them to continue to investigate the incident. We are grateful for Hugging Face's rapid and close collaboration on investigation and remediation.

What happened during this incident

Actions we are taking now

Our approach to evaluating advanced cyber capabilities

Actions we are taking now

1. As part of the investigation, we are implementing strict controls in infrastructure configuration at the cost of research velocity while the vulnerabilities are patched. We are regularly briefing our Safety and Security Committee on these controls and their impact.
2. We're working with Hugging Face to forensically investigate the incident.
3. We've responsibly disclosed the identified zero-day vulnerability in the internally-hosted third-party software and are working with them to patch.
4. We've brought Hugging Face into the trusted access program and are supporting their teams in rapidly using our models' capabilities to improve their defenses.
5. We're improving and adding stronger protections around future training and evaluations. This week, we published a blog on improving safety and alignment in an era of long horizon models. These deployment safeguards were intentionally not enabled during this evaluation because it was aimed at testing cyber vulnerabilities. This incident points to the need to further strengthen our model's alignment, cyber protections during evaluation time, and monitoring during internal testing.

Our approach to evaluating advanced cyber capabilities

As we recently shared, AI is accelerating the discovery and exploitation of vulnerabilities. The primary lesson from this incident is that model security and safety must keep pace with rapidly advancing capabilities. We are strengthening the containment, monitoring, access controls, and evaluation practices used during model development.

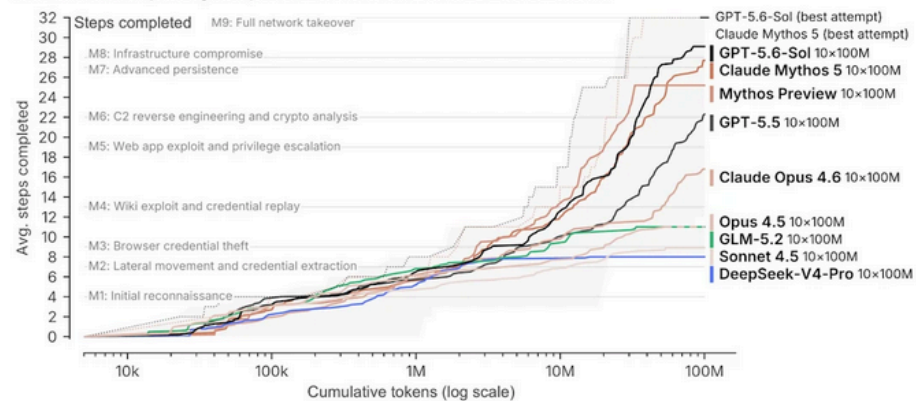
UK AISI's evaluation shows that models such as GPT-5.6 Sol are increasingly able to sustain complex, multi-step cyber operations over long time horizons. This incident implies these theoretical capabilities do apply in real-world settings.

What happened during this incident

Actions we are taking now

Our approach to evaluating advanced cyber capabilities

Trajectories for various AI models on the 32-step “The Last Ones” cyber range—a corporate network attack simulation spanning multiple subnets and hosts, without active defenders.



AI SECURITY
INSTITUTE

The incident also makes clear that advanced models can discover and exploit novel attack paths in real-world systems without source-code access. It highlights that advanced cyber capabilities must be developed alongside stronger safeguards and defensive tools.

We believe advanced cyber capable models need to help security teams find weaknesses before attackers do, understand how vulnerabilities can be chained, and remediate them at machine speed. We are using these capabilities to continue strengthening protections around infrastructure configuration and model evaluation environments; we will share our findings and best practices as we learn. We encourage other defenders to apply for trusted access and experiment with these models now to translate these capabilities into better prevention, faster detection, and more effective incident response.

“We’re grateful for the collaboration with OpenAI on this and other topics. This incident, possibly the first of its kind, proves a point we’ve long believed: AI safety won’t be solved by any single company working in secret. It will be solved in the open, collaboratively, with broad access to AI for every defender, everywhere.”

—Clem Delangue, Co-founder and CEO, Hugging Face

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-21

The following is the annexure marked **FT-21** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains a screenshot of the landing page of the GitHub repository posted by user, 'abrasive', as at July 1 2026: <https://github.com/abrasive/mygov-totp-enroll>.

.....
Daniel Davison
Solicitor

 **abrasive / mygov-totp-enroll** Public[Code](#) [Issues 8](#) [Pull requests 2](#) [Actions](#) [Security and quality](#) [Insight](#)

About

Enroll a real TOTP client to access myGov

 [Readme](#)

 [Activity](#)

 **108** stars

 **9** watching

 **8** forks

[Report repository](#)

Releases

No releases published

Packages

No packages published

Contributors 4



abrasive James Wah



lachlanhunt Lachlan Hunt



alexlance Alex Lance



danielgruber8 Daniel

Languages

 **JavaScript** 65.7%  **HTML** 32.0%  **Dockerfile** 2.3%



 **1** Branch

 **0** Tags



 Go to file

[Go to file](#)

[Code](#)



lachlan and abrasive Credit where credit is due

years ago 13 Commits

 .gitignore	gitignore node_modules	3 years ago
 Dockerfile	Add Dockerfile	7 years ago
 README.md	Add Dockerfile	7 years ago
 instructions.html	instructions: mention SHA5...	7 years ago
 main.js	Upgrade Electron	3 years ago
 package.json	Upgrade Electron	3 years ago
 preload.js	Credit where credit is due	3 years ago
 ui.html	It works.	7 years ago

 README

mygov-totp-enroll

This tool lets you enroll a TOTP authenticator (eg. andOTP) to access myGov.

You can't have more than one authenticator set up, so if you want multiple copies or backups, better do them all at once.

It shouldn't be possible to fuck up your myGov account using this tool, because you have to enter a correct code from your newly configured authenticator for the TOTP login requirement to be activated. However, if you do screw up somehow, there's no way to recover a myGov account, and you have to make a new one. Consequently I make no guarantees about this code, and if it flattens your cat or makes your lollies taste funny, well, you were warned.

This is an Electron app because you absolutely have to install a handler for full custom URL schemes, as the myGov OAuth endpoint insists on returning you to `au.gov.my://app`, which is pretty reasonable for them from a security point of view and atrocious for us from a reasonable software point of view. So sorry for the bloat, but there you go.

Instructions for use

1. `npm install`
2. `npm start`
3. pray
4. follow the instructions

Or if you have docker installed

1. `docker build -t mygov .`
2. `docker run -e DISPLAY --net=host -it mygov npm start`

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-22

The following is the annexure marked **FT-22** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure includes screenshots of the two files containing the HTML source code in the 'mygov-totp-enroll' GitHub repository as at July 1 2026 and available at: <https://github.com/abrasive/mygov-totp-enroll/blob/master/instructions.html> and <https://github.com/abrasive/mygov-totp-enroll/blob/master/ui.html>.

.....
Daniel Davison
Solicitor

abrasive / mygov-totp-enroll

Code

Issues 8

Pull requests 2

Actions

Security and quality

Insights

master

mygov-totp-enroll / instructions.html

Go to file

T

abrasive

instructions: mention SHA512, and Authy not working

fb85be1 · 7 years ago

Code

Blame

46 lines (39 loc) · 1.89 KB

Raw

```

1  <!doctype html>
2  <html>
3    <head>
4      <style>
5        div {
6          width: 400px;
7          margin: 20px;
8        }
9      </style>
10   </head>
11   <body>
12     <div>
13       <h1>myGov TOTP enroller</h1>
14
15       This tool will get you a TOTP key (as a QR code) for logging in to myGov.
16       <p>
17
18       You then need to use your TOTP authenticator to log in, every time, unless you disable it
19       after logging in.
20       <p>
21
22       After you log in to myGov, you will be shown the QR code.
23       You need to enroll this in your authenticator app - or maybe more than one, if you want a
24       backup.
25
26       Then, enter the current generated code to activate it.
27       <p>
28
29       The TOTP access method will not be activated unless you enter a correct key.
30       This also means you won't be locked out if something goes wrong in the process.
31       <p>
32
33       Your TOTP authenticator must support SHA512 keys. <b>Authy does not support these and will not
34       work.</b>
35
36       To get started, just click the button.
37
38       <form action="https://auth.my.gov.au/mga/sps/oauth/oauth20/authorize" method="get">
39         <input type="hidden" name="response_type" value="code" />
40         <input type="hidden" name="state" value="63065293C60AD6A479B67F1DFC79BBC75DEF04C3" />
41         <input type="hidden" name="client_id" value="g2c2pjLUth0aBumECqbf" />
42         <input type="hidden" name="scope" value="totp" />
43         <input type="hidden" name="redirect_uri" value="au.gov.my://app" />
44         Phone name shown in myGov: <input type="text" name="device_name" value="SM-N950F" /><br>
45         Phone type shown in myGov: <input type="text" name="device_type" value="samsung SM-N950F"
46       /><br>
47         <input type="submit" />
48       </form>
49     </div>
50   </body>
51 </html>

```

abrasive / mygov-totp-enroll

Q

+

CodeIssues8Pull requests2ActionsSecurity and qualityInsights

master

mygov-totp-enroll / ui.html

Go to file

T

abrasive

It works.

df78fe7 · 7 years ago

CodeBlame48 lines (43 loc) · 1.35 KB

Raw

```
1  <!doctype html>
2  <html>
3    <head>
4      <style>
5        div {
6          display: flex;
7          flex-direction: column;
8          align-items: center;
9          word-break: break-all;
10       }
11       #detail {
12         width: 400px;
13       }
14     </style>
15   </head>
16   <body>
17     <div>
18       <h1 id="status">Loading...</h1>
19       <div id="detail"></div>
20
21       <form id="form">
22         <input type="number" maxlength=6 id="code" />
23         <input type="submit" />
24       </form>
25     </div>
26
27     <script>
28       document.getElementById("form").style.display = "none";
29
30       const { ipcRenderer } = require('electron');
31       ipcRenderer.on('status', (event, arg) => {
32         document.getElementById("status").innerHTML = arg;
33       })
34       ipcRenderer.on('detail', (event, arg) => {
35         document.getElementById("detail").innerHTML = arg;
36       })
37
38       ipcRenderer.on('showform', (event, arg) => {
39         document.getElementById("form").style.display = arg;
40       })
41
42       document.getElementById("form").onsubmit = function() {
43         code = document.getElementById("code").value;
44         ipcRenderer.send('code', code);
45       }
46     </script>
47   </body>
48 </html>
```


**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-23

The following is the annexure marked **FT-23** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure includes screenshots of the application code written in the JavaScript programming language published in the GitHub repository, 'mygov-totp-enroll', as at July 1 2026: <https://github.com/abrasive/mygov-totp-enroll/blob/master/main.js>.

.....
Daniel Davison
Solicitor

Code Blame 204 lines (181 loc) · 5.7 KB

Raw 🔗 ⬇️ ✎ ⌵ ⌵

```
1  const { app, protocol, BrowserWindow, ipcMain, dialog } = require('electron');
2  const url = require('url');
3  const request = require('request');
4  const qrcode = require('qrcode');
5  const { base32, base64 } = require('rfc4648');
6  const path = require("node:path");
7
8  let win
9  let client_id='g2c2pjLUTh0aBumECqbf'
10 let token
11
12 function setStatus(stat) {
13     win.webContents.send("status", stat);
14 }
15 function setDetail(detail) {
16     win.webContents.send("detail", detail);
17 }
18 function setError(headline, detail) {
19     setStatus("ERROR: " + headline);
20     setDetail(detail);
21 }
22 ✓ function showCodeForm(on) {
23     if (on) {
24         win.webContents.send("showform", "block");
25     } else {
26         win.webContents.send("showform", "none");
27     }
28 }
29
30 ✓ function verifyCode(code) {
31     const options = {
32         method: 'POST',
33         url: 'https://api.my.gov.au/authbiz-ext-sec/api/v1/authclients/g2c2pjLUTh0aBumECqbf/totpverify.json',
34         headers: {
35             'content-type': 'application/json',
36             'Authorization': 'Bearer ' + token
37         },
38         body: {
39             password: code,
40         },
41         json: true,
42     };
43
44     request(options, function (error, response, body) {
45         if (error) {
46             setError("Code verification failed, try again", error);
47             console.log("error: " + error)
48             return;
49         }
50         if (body == null) { // lol
51             setStatus("Enrolment complete! DON'T LOSE THE CODE");
52             showCodeForm(false);
53             return;
```

 master

mygov-totp-enroll / main.js



↑ Top

CodeBlame

204 lines (181 loc) · 5.7 KB

RawCopyDownloadEditDropdown

```
30  function verifyCode(code) {
44      request(options, function (error, response, body) {
45          if (error) {
46              setError("Code verification failed, try again", error);
47              console.log("error: " + error)
48              return;
49          }
50          if (body == null) {    // lol
51              setStatus("Enrolment complete! DON'T LOSE THE CODE");
52              showCodeForm(false);
53              return;
54          } else if (body.error) {
55              setError("Code verification failed, try again", body.error + ' - ' +
body.error_description);
56              console.log("body error: " + body.error)
57              return;
58          } else {
59              console.log("body?? " + body)
60              console.dir(body)
61              msg = "myGov error: " + body.info[0].code + " " + body.info[0].message
62              msg += "\n Make sure you're using an OTP tool that supports SHA1 keys!"
63              dialog.showMessageBox({
64                  "type": "error",
65                  "title": "myGov error",
66                  "message": msg,
67                  "buttons": ["OK"],
68              })
69          }
70      });
71  }
72
73  function makeQR(secret) {
74      secret32 = base32.stringify(base64.parse(secret))
75      secret32 = secret32.replace(/=+$/, "")
76      totp_uri = 'otpauth://totp/myGov?secret=' + secret32 + '&algorithm=SHA512'
77
78      qrcode.toDataURL(totp_uri)
79      .then(url => {
80          setStatus("Enroll this secret in your TOTP client and enter the current code");
81          setDetail(totp_uri + '<p>');
82          showCodeForm(true);
83      })
84      .catch(err => {
85          setError("QR encoding error", err);
86      })
87  }
88
89  function requestSecret(token) {
90      setStatus("Requesting OAuth secret...");
91      const options = {
92          method: 'POST',
93          url: 'https://api.my.gov.au/authbiz-ext-sec/api/v1/authclients/g2c2pjLUTh0aBumECqbf/
totpcredential.json',
94          headers: {'Authorization': 'Bearer ' + token},
95      };
96      request(options, function (error, response, body) {
97          if (error) {
98              setError("Secret request failed", error);
99              return;
100          }
101          body = JSON.parse(body)
102          if (body.error) {
103              setError("Secret request failed"
```

340

Code Blame 204 lines (181 loc) · 5.7 KB Raw

```

89     function requestSecret(token) {
90         setStatus("Requesting OAuth secret...");
91         const options = {
92             method: 'POST',
93             url: 'https://api.my.gov.au/authbiz-ext-sec/api/v1/authclients/g2c2pjLUTH0aBumECqbf/
totpcredential.json',
94             headers: {'Authorization': 'Bearer ' + token},
95         };
96         request(options, function (error, response, body) {
97             if (error) {
98                 setError("Secret request failed", error);
99                 return;
100             }
101             body = JSON.parse(body)
102             if (body.error) {
103                 setError("Secret request failed",
104                     body.error + ' - ' + body.error_description);
105                 return;
106             }
107
108             secret = body.secret;
109             makeQR(secret);
110         });
111     }
112
113     function requestToken(code) {
114         setStatus("Requesting OAuth token...");
115
116         const options = {
117             method: 'POST',
118             url: 'https://auth.my.gov.au/mga/sps/oauth/oauth20/token',
119             form: {
120                 client_id: client_id,
121                 redirect_uri: 'au.gov.my://app',
122                 grant_type: 'authorization_code',
123                 code: code,
124             },
125         };
126
127         request(options, function (error, response, body) {
128             if (error) {
129                 setError("Token request failed", error);
130                 return;
131             }
132             body = JSON.parse(body)
133             if (body.error) {
134                 setError("Token request failed",
135                     body.error + ' - ' + body.error_description);
136                 return;
137             }
138
139             token = body.access_token;
140
141             requestSecret(token);
142         });
143     }
144
145     function createWindow () {
146         protocol.registerFileProtocol('au.gov.my', (req, callback) => {
147             console.log(req.url)
148             query = url.parse(req.url, true).query
149             if ("code" in query) {
150                 callback({ path: `${dirname}/ui.html` })

```

🔗 master mygov-totp-enroll / main.js ↗

Code Blame 204 lines (181 loc) · 5.7 KB Raw ↗ ↕ ↴ ↻

```
145     function createWindow () {
146         protocol.registerFileProtocol('au.gov.my', (req, callback) => {
147             console.log(req.url)
148             query = url.parse(req.url, true).query
149             if ("code" in query) {
150                 callback({ path: `${__dirname}/ui.html` })
151
152                 requestToken(query.code)
153             } else {
154                 if ("error_code" in query) {
155                     console.log("set error")
156                     callback({ path: `${__dirname}/instructions.html` })
157
158                     dialog.showMessageBox({
159                         "type": "error",
160                         "title": "myGov error",
161                         "message": "myGov error: " + query.error_code,
162                         "buttons": ["OK"],
163                     })
164                 }
165             }
166         }, (error) => {
167             if (error) console.error('Failed to register protocol')
168         })
169
170         win = new BrowserWindow({
171             width: 800,
172             height: 600,
173             webPreferences: {
174                 nodeIntegration: false,
175                 contextIsolation: true,
176                 enableRemoteModule: false,
177                 preload: path.join(__dirname, "preload.js")
178             }
179         })
180
181         win.loadFile(path.join(__dirname, "instructions.html"));
182
183         ipcMain.on('code', (event, arg) => {
184             verifyCode(arg);
185         });
186
187         win.on('closed', () => {
188             win = null
189         })
190     }
191
192     app.on('ready', createWindow)
193
194     app.on('window-all-closed', () => {
195         if (process.platform !== 'darwin') {
196             app.quit()
197         }
198     })
199
200     app.on('activate', () => {
201         if (win === null) {
202             createWindow()
203         }
204     })
```

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-24

The following is the annexure marked **FT-24** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains screenshots of the 'issues' and 'pull request' entries on the GitHub repository, 'mygov-totp-enroll', in which users discuss how to use the repository to enable TOTP authentication in the App, as at 1 July 2026:

<https://github.com/abrasive/mygov-totp-enroll/issues/9>;
<https://github.com/abrasive/mygov-totp-enroll/issues/11>;
<https://github.com/abrasive/mygov-totp-enroll/pull/5>;
<https://github.com/abrasive/mygov-totp-enroll/issues/1>

.....
Daniel Davison
Solicitor

[New issue](#)

Not an issue: just thanks! #9

[Open](#)ramebd opened on Jun 17, 2021 

Sorry, couldn't leave a comment on the reddit thread I found, but this is just plain awesome, and thanks for all your work!

Worked flawlessly, got myGov all set up with andOTP and no more relying on sms 2fa.

Thanks! 😊



6

2

VirtualWolf on Jun 21, 2021 

Seconding this!

DuBistKomisch on Jul 8, 2021 

thirring

n3ih7 on Jul 30, 2021 

Still works two years after

Lord-Evil on Sep 29, 2022 

Found it today, awesome!

**Add a comment**

Write

Preview

H

B

I

≡

<>

🔗

≡

≡

≡

@

📧

📎

↩

Doesn't seem to work any longer? #11

[New issue](#)[Open](#)

 gsklee opened on Sep 15, 2021

This is what I am seeing in the console when clicking on the "Register" button on the "Finish registration" screen:

```
au.gov.my://app?error=invalid_request&error_description=FBT0AU202E+The+required+parameter%3A+%5Bcode_challenge%5D
```

And nothing happens. Looks like it's broken?



 jimtsao on Oct 3, 2021

Just set mine up today. Still works for me.



 phik on Jun 6, 2022

Also worked for me today. Big thanks for this. You're a legend!



 Scrub000 on Oct 1, 2024

Last edited by Scrub000 ▾

Can confirm; no longer working. Patched by myGov.



 midnightveil on Jul 18, 2025

Works for me, still. Needed this patch to the code due to electron version changes but otherwise fine:

```
diff --git a/main.js b/main.js
index 6e71652..fabb42d 100644
--- a/main.js
+++ b/main.js
@@ -171,9 +171,11 @@ function createWindow () {
   width: 800,
   height: 600,
   webPreferences: {
-    nodeIntegration: false,
-    contextIsolation: true,
-    enableRemoteModule: false,
+    nodeIntegration: true,
+    nodeIntegrationInWorker: true,
+    nodeIntegrationInSubFrames: true,
+    enableRemoteModule: true,
+    contextIsolation: false,
     preload: path.join(__dirname, "preload.js")
   }
 }
```



Code ▾

Add Dockerfile #5



abrasive merged 1 commit into `abrasive:master` from `alexlance:add-dockerfile` 
on Dec 30, 2019

 Conversation 1

 Commits 1

 Checks 0

 Files changed 2



alexlance commented on Dec 27, 2019

Contributor 

Fantastic project, super happy to have found a way around installing the mygov app and stick to normal, reliable totp/mfa. THANK YOU.

No worries if you don't want to merge this PR, but thought a Dockerfile which installs the dependencies (and node) might be useful.

Cheers!



Add Dockerfile

`63dcdf6`

abrasive commented on Dec 30, 2019

Owner 

Nice! Cheers :D



abrasive merged commit `ebf1b78` into `abrasive:master` on Dec 30, 2019

Pull request successfully merged and closed

You're all set — the branch has been merged.

Add a comment

Write

Preview

H

B

I

≡

<>











@



←



Add your comment here...

[New issue](#)

Submit button not working #1

[Open](#)

danielgruber8 opened on Jul 1, 2019

Contributor



After installing npm, node.js legacy dependencies on Ubuntu 16.04 and running npm-start, after viewing the QR code generated, I enter the code in to the text box and nothing happens after pressing the "Submit" button.



abrasive on Jul 1, 2019

Owner



That's helpful!

What do you get if you run it as `ELECTRON_ENABLE_LOGGING=1 npm start` ?



danielgruber8 on Jul 1, 2019

Contributor

Author



I am temporarily restricted from mygov for 2 hours but here is my output after I attempted to login

[13131:0701/154045.698831:ERROR:bus.cc(394)] Failed to connect to the bus: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.

[13131:0701/154045.850373:INFO:CONSOLE(259)] "%cElectron Deprecation Warning (nodeIntegration default change)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (259)

[13131:0701/154045.850595:INFO:CONSOLE(170)] "%cElectron Security Warning (Insecure Content-Security-Policy)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (170)

[13131:0701/154052.052866:INFO:CONSOLE(345)] "Uncaught ReferenceError: jQuery is not defined", source: <https://auth.my.gov.au/mygov/content/mgv2/js/mgv2-vendor.js> (345)

[13131:0701/154052.055950:INFO:CONSOLE(1)] "Uncaught ReferenceError: \$ is not defined", source: <https://auth.my.gov.au/mygov/content/mgv2/js/mgv2-application.js> (1)

[13131:0701/154052.061523:INFO:CONSOLE(128)] "%cElectron Security Warning (Node.js Integration with Remote Content)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (128)

[13131:0701/154052.062435:INFO:CONSOLE(259)] "%cElectron Deprecation Warning (nodeIntegration default change)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (259)

[13131:0701/154052.062637:INFO:CONSOLE(170)] "%cElectron Security Warning (Insecure Content-Security-Policy)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (170)



Submit button not working #1



```
[13131:0701/154052.062637:INFO:CONSOLE(170)] "%cElectron Security Warning (Insecure Content-Security-Policy)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (170)
[13131:0701/154104.794534:INFO:CONSOLE(345)] "Uncaught ReferenceError: jQuery is not defined", source: https://auth.my.gov.au/mygov/content/mgv2/js/mgv2-vendor.js (345)
[13131:0701/154104.797675:INFO:CONSOLE(1)] "Uncaught ReferenceError: $ is not defined", source: https://auth.my.gov.au/mygov/content/mgv2/js/mgv2-application.js (1)
[13131:0701/154105.030805:INFO:CONSOLE(128)] "%cElectron Security Warning (Node.js Integration with Remote Content)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (128)
[13131:0701/154105.033220:INFO:CONSOLE(259)] "%cElectron Deprecation Warning (nodeIntegration default change)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (259)
[13131:0701/154105.033682:INFO:CONSOLE(170)] "%cElectron Security Warning (Insecure Content-Security-Policy)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (170)
```



danielgruber8 on Jul 2, 2019

Contributor

Author



Here is the full log since unlocked from myGov

```
user@tux:~/Downloads/mygov-totp-enroll-master$ ELECTRON_ENABLE_LOGGING=1 npm start
```

```
mygov-totp-enroll@0.1.0 start /home/user/Downloads/mygov-totp-enroll-master
electron .
```

```
[5009:0702/105149.612664:INFO:CONSOLE(259)] "%cElectron Deprecation Warning (nodeIntegration default change)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (259)
[5009:0702/105149.612907:INFO:CONSOLE(170)] "%cElectron Security Warning (Insecure Content-Security-Policy)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (170)
[5009:0702/105153.295575:INFO:CONSOLE(345)] "Uncaught ReferenceError: jQuery is not defined", source: https://auth.my.gov.au/mygov/content/mgv2/js/mgv2-vendor.js (345)
[5009:0702/105153.298488:INFO:CONSOLE(1)] "Uncaught ReferenceError: $ is not defined", source: https://auth.my.gov.au/mygov/content/mgv2/js/mgv2-application.js (1)
[5009:0702/105154.027935:INFO:CONSOLE(128)] "%cElectron Security Warning (Node.js Integration with Remote Content)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (128)
[5009:0702/105154.028858:INFO:CONSOLE(259)] "%cElectron Deprecation Warning (nodeIntegration default change)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (259)
[5009:0702/105154.029018:INFO:CONSOLE(170)] "%cElectron Security Warning (Insecure Content-Security-Policy)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (170)
[5009:0702/105204.585167:INFO:CONSOLE(345)] "Uncaught ReferenceError: jQuery is not defined", source: https://auth.my.gov.au/mygov/content/mgv2/js/mgv2-vendor.js (345)
[5009:0702/105204.588237:INFO:CONSOLE(1)] "Uncaught ReferenceError: $ is not defined", source: https://auth.my.gov.au/mygov/content/mgv2/js/mgv2-application.js (1)
[5009:0702/105205.843714:INFO:CONSOLE(128)] "%cElectron Security Warning (Node.js Integration with Remote Content)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/resources/electron.asar/renderer/security-warnings.js (128)
```



```
[5009:0702/105154.027935:INFO:CONSOLE(128)] "%cElectron Security Warning (Node.js Integration
with Remote Content)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/
dist/resources/electron.asar/renderer/security-warnings.js (128)
[5009:0702/105154.028858:INFO:CONSOLE(259)] "%cElectron Deprecation Warning (nodeIntegration
default change)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/
resources/electron.asar/renderer/security-warnings.js (259)
[5009:0702/105154.029018:INFO:CONSOLE(170)] "%cElectron Security Warning (Insecure Content-
Security-Policy)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/
resources/electron.asar/renderer/security-warnings.js (170)
[5009:0702/105204.585167:INFO:CONSOLE(345)] "Uncaught ReferenceError: jQuery is not defined",
source: https://auth.my.gov.au/mygov/content/mgv2/js/mgv2-vendor.js (345)
[5009:0702/105204.588237:INFO:CONSOLE(1)] "Uncaught ReferenceError: $ is not defined", source:
https://auth.my.gov.au/mygov/content/mgv2/js/mgv2-application.js (1)
[5009:0702/105205.843714:INFO:CONSOLE(128)] "%cElectron Security Warning (Node.js Integration
with Remote Content)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/
dist/resources/electron.asar/renderer/security-warnings.js (128)
[5009:0702/105205.845080:INFO:CONSOLE(259)] "%cElectron Deprecation Warning (nodeIntegration
default change)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/
resources/electron.asar/renderer/security-warnings.js (259)
[5009:0702/105205.845265:INFO:CONSOLE(170)] "%cElectron Security Warning (Insecure Content-
Security-Policy)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/
resources/electron.asar/renderer/security-warnings.js (170)
[5009:0702/105214.135939:INFO:CONSOLE(345)] "Uncaught ReferenceError: jQuery is not defined",
source: https://auth.my.gov.au/mygov/content/mgv2/js/mgv2-vendor.js (345)
[5009:0702/105214.138827:INFO:CONSOLE(1)] "Uncaught ReferenceError: $ is not defined", source:
https://auth.my.gov.au/mygov/content/mgv2/js/mgv2-application.js (1)
[5009:0702/105214.144003:INFO:CONSOLE(128)] "%cElectron Security Warning (Node.js Integration
with Remote Content)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/
dist/resources/electron.asar/renderer/security-warnings.js (128)
[5009:0702/105214.144999:INFO:CONSOLE(259)] "%cElectron Deprecation Warning (nodeIntegration
default change)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/
resources/electron.asar/renderer/security-warnings.js (259)
[5009:0702/105214.145121:INFO:CONSOLE(170)] "%cElectron Security Warning (Insecure Content-
Security-Policy)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/
resources/electron.asar/renderer/security-warnings.js (170)
[5009:0702/105218.441059:INFO:CONSOLE(259)] "%cElectron Deprecation Warning (nodeIntegration
default change)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/
resources/electron.asar/renderer/security-warnings.js (259)
[5009:0702/105218.441110:INFO:CONSOLE(170)] "%cElectron Security Warning (Insecure Content-
Security-Policy)", source: /home/user/Downloads/mygov-totp-enroll-master/node_modules/electron/dist/
resources/electron.asar/renderer/security-warnings.js (170)
```



abrasive mentioned this [on Jul 10, 2019](#)

[windows asking for an app to open au.gov.my #2](#)



BeauGiles on Jul 28, 2019



Experiencing the same thing here on macOS - nothing happens after hitting submit.



Open Submit button not working #1



BeauGiles on Jul 28, 2019

Experiencing the same thing here on macOS - nothing happens after hitting submit.



abrasive on Jul 29, 2019

Owner ...

@BeauGiles can you try the latest master?



BeauGiles on Aug 1, 2020

...

@abrasive figured I should probably reply so this can be closed 🙌

Can confirm that the latest master is fine on the latest version of macOS Catalina - I was able to add the myGov OTP to 1Password - as both Authy & Microsoft Authenticator *do not* support the SHA512 algorithm.

Might be worth making it more obvious what authenticator apps do or do not support SHA512 required by myGov



BeauGiles on Jun 22, 2021

...

This works with the built in iOS 15 / iCloud Keychain code generator.



Add a comment

Write

Preview

H B I | | @

Use Markdown to format your comment

Paste, drop, or click to add files

Close issue

Comment

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-25

The following is the annexure marked **FT-25** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains screenshots of the GitHub gist posted by hacker1024, including comments from other users as at July 1 2026:

<https://gist.github.com/hacker1024/5d0845863e2dc27fd5eebc4ac95a39>.

.....
Daniel Davison
Solicitor

Instantly share code, notes, and snippets.

hacker1024 / mygov_totp_storage.md



Last active last year

<> Code - Revisions 2 ☆ Stars 8 🔗 Forks 1

Information about TOTP token storage in the myGov Code Generator app, as well as token extraction instructions.

mygov_totp_storage.md

This gist contains information about TOTP token storage in the [myGov Code Generator](#) app, along with instructions on how to extract tokens.

App data

Structure

```
/data/user/0/au.gov.dhs.centrelink.mygovauthenticator:
├── files
│   ├── myGov.ks
│   └── sharedSecret
└── shared_prefs
    └── au.gov.dhs.centrelink.mygovauthenticator.prefs_file.xml
```

Details

- **myGov.ks** : A BKS keystore containing a private RSA-256 key used to decrypt the contents of **sharedSecret** (after decoding the base64 data). The key is called **sharedSecret** , and uses the hard-coded password of **km5QzJJ5NhGymfp** .
- **sharedSecret** : The encrypted TOTP token. The encrypted data is stored in base64 form, and decrypts to more base64.
- **au.gov.dhs.centrelink.mygovauthenticator.prefs_file.xml** : An XML file containing the IV used to decrypt **sharedSecret** along with the key in **myGov.ks** , as well as the **myGov.ks** keystore password.

TOTP format

The TOTP token must be used with the SHA512 algorithm, and the standard 6-digit length and 30 second period.

Example URI: `otpauth://totp/myGov?secret=<BASE32_ENCODED_SECRET>&algorithm=SHA512`

Note that some apps like Google Authenticator and Authy do not handle SHA512 properly. BitWarden, for example, does.

Manual instructions

1. Gain access to the files shown above
2. Use the `keyStorePwd` in `au.gov.dhs.centrelink.mygovauthenticator.prefs_file.xml` to open `myGov.ks` with a tool like [KeyStore Explorer](#)
3. Use the password `km5QzJJ5NhGymfp` to access the `sharedSecret` key

At this point, you can use this [CyberChef recipe](#) to generate a URI, or continue manually:

5. Decode the base64 data in the `sharedSecret` file
6. Use the `sharedSecret` key, along with the `sharedSecret_iv` in `au.gov.dhs.centrelink.mygovauthenticator.prefs_file.xml`, to decrypt the decoded `sharedSecret` file contents with AES-256-CBC
7. Convert the decrypted `sharedSecret` file contents from base64 to base32, removing any `=` padding from the end.
8. Generate a URI with the properties specified above

soraxas commented on Sep 6, 2021

Thank you SO MUCH for the instruction!! The instructions are very detailed and the recommended tools had been great as well. Specifically, you had created the CyberChef to help automate the process, which had worked faultlessly. Thanks heaps and it helps to consolidate all my TOTP :)

kylemd commented on Feb 2, 2022

Thank you for this! The myGov Authenticator app is awful

K1ngJony commented on Jul 20, 2022

01/07/2026, 11:31

Information about TOTP token storage in the myGov Code Generator app, as well as token extraction instructions. · GitHub

Any advice on how to get the files in the first place? I've tried adb backup but it comes up empty

hacker1024 commented on Aug 31, 2022

Author

Any advice on how to get the files in the first place? I've tried adb backup but it comes up empty

@K1ngJony You'll need a rooted device (or one with file access from a recovery environment). Perhaps an Android emulator would work as well - I'm not sure if the app uses SafetyNet.

Jarodwr commented on Jul 7, 2023

Attempted to do this from bluestacks and didn't have any success, couldn't get access to the app data at that path (I assume it's to do with that safetynet thing you talked about)

rogerkeays commented on Aug 17, 2023 · edited ▼

Sublime.

I only hit a couple of obstacles. Firstly, I found the files in `/data/data/au.gov.dhs.centrelink.mygovauthenticator` on my device. Secondly, I couldn't cut and paste the secret directly into my authenticator because the textbox truncated the data. I converted the URI to a QR code using <https://qr-creator.com/url.php> and it worked perfectly.

Thanks for this. Love your work!

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE

Applicant

CEO, SERVICES AUSTRALIA

Respondent

ANNEXURE FT-26

The following is the annexure marked **FT-26** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains a screenshot of the initial Reddit post by user 'j_l-w' in the r/Australia forum as at 1 July 2026:

https://www.reddit.com/r/australia/comments/bc6gmv/for_all_the_mygov_fake_2fa_haters/

.....
Daniel Davison
Solicitor



r/australia • 7y ago

j_l-w



for all the myGov fake 2FA haters

no politics

myGov actually supports TOTP, but only via their own app, so I got really grumpy and made this:

<https://github.com/abrasive/mygov-totp-enroll>

It allows you to enroll for their TOTP and displays your credentials as a QR code in the traditional way. (It's a stupid long key, you don't want to type that in a phone by hand.)

It's not distributed as a ready-to-run app because how could you trust it? - so you'll need npm to run it. Sorry. It's short enough that it should be trivial to audit, but good luck with the dependencies -^



Archived post. New comments cannot be posted and votes cannot be cast.



22



39



**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-27

The following is the annexure marked **FT-27** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains screenshots of the comments made by user, 'Thingface', on the Reddit post of 'j_l-w' as at 1 July 2026:

https://www.reddit.com/r/australia/comments/bc6gmv/for_all_the_mygov_fake_2fa_haters/

.....
Daniel Davison
Solicitor



Thingface • 7y ago • Edited 7y ago

I had been using 2FA with [andOTP](#) for ages. I was thinking about writing an app to do this, in Electron too. Now you've done it [u/j_l-w](#) I won't have to. On a side note this is what I discovered independently back in December 2018.

The reason I use [andOTP](#) and not [Authy](#) is because that is proprietary software and not open-source. I also don't install [Gapps](#) and I run [LineageOS](#) on my phone.

How

I looked at `/data/data/au.gov.dhs.centrelink.mygovauthenticator/files/sharedSecret` however that file is encrypted. When I did an internet search for the filename of the other file in there, `myGov.ks` I found a [de-compilation of the app was returned](#).

To get around this I had to get a copy of the encrypted secret **before** it landed on the phone and the app encrypted it. To do this:

1. I performed a [Man-in-the-middle](#) attack on myself in order to strip the encryption off the [TLS](#) session (ie peek inside the https). I used [Charles Proxy](#). Video [here](#) and configured a HTTP proxy on my phone. This is a HTTP proxy which issues a different certificate that I hold the private key for. That means I can look inside the https encrypted requests. The HTTP proxy handles the connection to MyGov.
2. I was able to [add a new root certificate](#) on an old phone which I plan to erase afterwards. It ran Android 6.0 so it was easy. If you're not using an old phone you should make sure you **remove the certificate authority afterwards**.
 - I could have used the [Android Emulator](#) instead of a phone if I didn't have an old one. Note in Android 7+ developers have the option of [preventing you from using user certificates](#) but adding the certificates to the root store will bypass that. Another method included [Intercepting HTTPS Traffic from Apps on Android 7+ using Magisk & Burp](#) fortunately I didn't need to do that either.
 - The MyGov app at this time doesn't employ a [network security configuration](#). They also aren't using [certificate pinning](#) either.
 - There are ways around that such as [SSLUnpinning_Xposed](#). This will work as long as they don't decide to get their app to 'check for root', although there are [ways to hide root using Magisk](#) should they do that in the future.
 - The system that MyGov uses on their back end seems to be IBM's [api_client_totp](#).
 - I observed that `api.my.gov.au` returns a json file ie https://api.my.gov.au/authbiz-ext-sec/api/v1/authclients/{{client_id}}/totpcredential.json which contains the [base64](#) encoded secret.
 - I then [converted this to base32 \(what andOTP expects\)](#) and added it using [SHA512](#) hash. The command I used for converting to base32 was (on my Linux system). The sed portion simply removes the new line:

```
echo "base64 encoded SECRET" | base64 -d | base32 | sed '/^/{N;s/\n//};'
```

It works great, now I don't need to use the MyGov app and I am free to use [andOTP](#) or whatever I want on my new phone that isn't Android or iOS. It would have been better if MyGov had implemented this with a [QR Code](#).

What I discovered

However the "[myGov Access - code creator](#)" will **call home every time you open it** as I said previously. You might be curious to know **what is actually in this transmission**.

This occurs after you've paired the phone with the MyGov account and received the shared secret. The app makes two [HTTP GET](#) requests:

- The first is to <https://api.my.gov.au/authbiz-ext-unsec/api/v1/meta/time.json> which returns the current server time in [ISO 8601 format](#) ie: `{ "serverTime": "YYYY-MM-DDTHH:MM:SS.sss+0000" }` which I [wouldn't have thought was necessary](#) as Android keeps the time up to date with it's service [NetworkTimeUpdateService](#), aka [Network Time Protocol](#) the way any computer does. There's also [NITZ](#) which is a way of doing the same thing over the cellular network without the internet. That's the way that old dumb-phones did it.
- The second is to https://api.my.gov.au/authbiz-ext-unsec/api/v1/authclients/{{client_id}}/authappmetadata.json your `{{client_id}}` is unique to the device you signed up with when you logged into your MyGov account with the "[myGov Access - code creator](#)" This appears to serve no purpose as the `authappmetadata.json` only returns `{}` ie a .json file with no data.



Thingface • 7y ago • Edited 7y ago

As my phone isn't rooted, and the default network configuration (for that API level) won't allow user CAs, I had to decompile the apk and add a network configuration to allow it to use my mitmproxy cert. (One can also flip the backupEnabled flag to allow retrieving its stored data on an unrooted phone.)

Ah yes, my phone was rooted and running LineageOS so, simply just installed the certificate into my root store.

Do you still have your dumps? The client_id in OAuth flows is supposed to represent the client app rather than the end-user, I'd be curious if they are actually using it that way.

- `{{ client_id }}` = `bCrzfdVmkZ` (used the same values as [IBM did](#))
- `code&state` = Appears to be a SHA1 value. I have put in a dummy value `printf $(echo -e code\&state | shasum) | sed 's/./\U&/g'` ie `26069F833E2E28347E47C05B2BA4FC57CA85EE6B`
- `{{ device_name }}` = ie `ro.product.model`
- `{{ device_type }}` = `ro.product.manufacturer` + `ro.product.model`
- `response_type` = Appears to be a SHA1 value. I have put in a dummy value `printf $(echo -e response_type | shasum) | sed 's/./\U&/g'` ie `3A7DB7703A076241984BD3275115E7FDDBA73045`
- `{{ client_secret }}` = `DSuCcZsEVH` (used the same values as [IBM did](#))
- `{{ access_token }}` = `wj0LQ4tPUDTz5LIleVLQkgUc1punUKUfFnBmWy1p` (used the same values as [IBM did](#))

Some requests are made:

```
GET /authbiz-ext-unsec/api/v1/meta/time.json HTTP/1.1
GET /authbiz-ext-unsec/api/v1/authclients/bCrzfdVmkZ/authappmetadata.json HTTP/1.1
GET /mga/sps/oauth/oauth20/authorize?response_type=code&state=26069F833E2E28347E47C05
GET /las/login?TAM_OP=login&USERNAME=unauthenticated&ERROR_CODE=0x00000000&URL=%2Fmga
```

Then there appears to be a few requests GET/POST to

```
/las/login?execution=e1s1
/las/login?execution=e1s2
/las/login?execution=e1s3
```

Few requests with favicon, css, JavaScript. I think for the login part).

Finally:

```
GET /mga/sps/oauth/oauth20/authorize?device_name={{ device_name }}&scope=otp&respons
```

Then a cookie is set.

```
POST /mga/sps/oauth/oauth20/token HTTP/1.1

HTTP/1.1 200 OK
Date: {{ CENSORED }}
Server: HTTPD/1.0.0
X-Frame-Options: SAMEORIGIN
content-language: en-US
content-type: application/json;charset=UTF-8
p3p: CP="NON CUR OTPi OUR NOR UNI"
x-frame-options: DENY
x-content-type-options: nosniff
cache-control: no-cache, no-store, must-revalidate
inst: mygov-auth_1_a
expires: Thu, 01 Dec 1994 16:00:00 GMT
x-xss-protection: 1; mode=block
content-security-policy: frame-ancestors 'none'
strict-transport-security: max-age=2592000
pragma: no-cache
Set-Cookie: JSESSIONID={{ CENSORED }}; Path=/mga/;Secure
Set-Cookie: PD_STATEFUL_{{ CENSORED }}=%2Fmga; Path=/;Secure
Set-Cookie: MYGOVAUTH= {{ CENSORED }}; path=/; Httponly;Secure
Keep-Alive: timeout=15, max=100
Transfer-Encoding: chunked
Connection: keep-alive
```

Then we get the return value

```
--EOF-{{CENSORED TIME}}-
Request-Body:<--EOF-{{CENSORED TIME}}-
client_id=bCrzfdVmkZ&redirect_uri=au.gov.my%3A%2F%2Fapp&grant_type=authorization_code
--EOF-{{CENSORED TIME}}-
Response-Body:<--EOF-{{CENSORED TIME}}-
{"access_token":"wj0LQ4tPUDTz5LIleVLQkgUc1punUKUfFnBmWylp","refresh_token":" {{ CENSORED }}"}
--EOF-{{CENSORED TIME}}-
```

Make a request with our bearer token

```
POST /authbiz-ext-sec/api/v1/authclients/bCrzfdVmkZ/totpcredential.json HTTP/1.1
Authorization: Bearer wj0LQ4tPUDTz5LIleVLQkgUc1punUKUfFnBmWy1p
```

HTTP HEADER

...
...
...

```
{
  "secret" : "{ { VERY SECRET TOKEN FOR YOUR TOTP APP IN BASE64 } }"
}
```

The whole thing with using a (modified?) Java KeyStore plus an encrypted blob is weird, what's up with that? Why not just use a normal-sized key and put it straight in the KeyStore?

I'm not sure what they've done with that. The keystore is the correct place for secrets, particularly as that makes the correct API calls. If in the future Google/OEMs make more use of ARM's TrustZone/SecurCore that's the correct way. [AndOTP](#) has the option of using the KeyStore 😊.

After all this it was amusing that putting together a half-usable Electron app took longer than working out the enrollment flow. I remain frustrated that that's the only way (purely because of the quite sensibly implemented restriction on redirect URLs).

I have to admit CharlesProxy is quit good for determining that. I ran it in a VM.

Also, is that ostorlab link still live? I just get a redirect to their homepage.

No it isn't, you'll have to resubmit, static analysis is free though by the looks of it. <https://ostorlab.co/scan/mobile/>

↑ 1 ↓ ...

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE FT-28

The following is the annexure marked **FT-28** referred to in the affidavit of Fraser Tweedale, affirmed at Brisbane on 29 July 2026. This annexure contains a screenshot of the follow-up comment made by Reddit user, 'j_l-w', on his post as at 1 July 2026:

https://www.reddit.com/r/australia/comments/bc6gmv/for_all_the_mygov_fake_2fa_haters/

.....
Daniel Davison
Solicitor



j_l-w OP · 7y ago

Thanks for the write-up! I see we took similar approaches, which I suppose should not surprise. ProGuard is an effective nuisance - it's enough to make me think twice before spending the time required to reverse an app statically.

As my phone isn't rooted, and the default network configuration (for that API level) won't allow user CAs, I had to decompile the apk and *add* a network configuration to allow it to use my `mitmproxy` cert. (One can also flip the `backupEnabled` flag to allow retrieving its stored data on an unrooted phone.)

Do you still have your dumps? The `client_id` in OAuth flows is supposed to represent the client app rather than the end-user, I'd be curious if they are actually using it that way.

The whole thing with using a (modified?) Java KeyStore plus an encrypted blob is weird, what's up with that? Why not just use a normal-sized key and put it straight in the KeyStore?

After all this it was amusing that putting together a half-usable Electron app took longer than working out the enrollment flow. I remain frustrated that that's the only way (purely because of the quite sensibly implemented restriction on redirect URLs).

↑ 1 ↓