EXPLANATORY STATEMENT

Issued by authority of the Digital ID Data Standards Chair

Digital ID Act 2024

Digital ID (Accreditation) Rules 2024

Digital ID (Accreditation) Data Standards 2024

Subsection 99(1) of the *Digital ID Act 2024* (the Digital ID Act) provides that the Digital ID Data Standards Chair (the Data Standards Chair) may, in writing, make one or more standards about the matters prescribed in that provision. Relevantly, data standards may be made about:

- technical integration requirements for entities to participate in the Australian Government Digital ID System (AGDIS);
- technical or design features that entities must have to participate in the AGDIS;
- technical, data or design standards if required to do so by the *Digital ID (Accreditation) Rules 2024* (Accreditation Rules) or the *Digital ID Rules 2024* (the Digital ID Rules); and
- other matters prescribed by the Digital ID Rules.

For the purposes of paragraph 99(1)(c) of the Digital ID Act, rule 7.7 of the Accreditation Rules sets out the standards that must be made by the Data Standards Chair, on the matters specified in subrule 7.7(2).

For the purposes of paragraphs 99(1)(c) and (d), the Digital ID Rules do not prescribe any of the matters in these *Digital ID (Accreditation) Data Standards 2024* (the Accreditation Data Standards).

The purpose of the Accreditation Data Standards is to support the operation of the accreditation scheme established by the Digital ID Act and the Accreditation Rules which aims to provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity for use in online transactions with government and businesses. In particular, the Accreditation Data Standards facilitate and promote trust in the digital ID services accredited under the accreditation scheme by providing:

- testing requirements to promote the accuracy of biometric technologies; and
- technical configuration requirements for authentication technologies and protocols to help prevent the compromise and misuse of digital IDs and related personal information.

1.1 An exposure draft of the Accreditation Data Standards and the accompanying consultation materials were released for public consultation from 28 May 2024 to 25 June 2024.

The Department undertook over 30 public consultation sessions in the form of webinars and face-to-face roundtables and bilateral meetings with over 250 parties over the 4-week consultation period. The Department received 42 long form submissions and 27 web-form comments from a range of parties including digital ID service providers, industry associations, consumer groups, privacy and inclusion advocates, government agencies and individuals. These built on previous consultations on the draft Digital ID legislation in late 2023, where 30 long form submissions specifically on the Accreditation Rules, which at the time contained the requirements of these Accreditation Data Standards, were received.

2.1 Stakeholder feedback was considered in formulating the policy reflected in the Accreditation Data Standards.

Details of the Accreditation Data Standards are set out in **Attachment A.**

Subsection 99(4) of the Digital ID Act provides that a standard made by the Data Standards Chair is a legislative instrument, but that section 42 (disallowance) of the *Legislation Act 2003* (Legislation Act) does not apply them. Paragraph 44(2)(a) of the Legislation Act provides that section 42 does not apply in relation to a legislative instrument if an Act declares, or has the effect, that section 42 does not apply in relation to the instrument or provision.

The Accreditation Data Standards are therefore a legislative instrument for the purposes of the Legislation Act but is not subject to disallowance.

The Accreditation Data Standards rely on section 4 of the *Acts Interpretation Act 1901*, as they are made in contemplation of commencement of subsection 99(1) of the Digital ID Act. The Accreditation Data Standards commence at the same time the Digital ID Act commences.

The Office of Impact Analysis (OIA) has been consulted in relation to the Accreditation Data Standards and an Impact Analysis **is not required** as these Accreditation Data Standards do not create any additional impact other than what has already been assessed in the Impact Analysis for the Digital ID Act. OIA reference number: OBPR23-04323.

As the instrument is not a disallowable instrument, a statement of compatibility is not required to be prepared under subsection 9(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011* or section 15J of the Legislation Act. However, a statement of compatibility has been prepared as a matter of best practice.

A Statement of Compatibility with Human Rights is at **Attachment B**.

The Accreditation Data Standards are compatible with human rights, and to the extent that they may limit human rights, those limitations are reasonable, necessary and proportionate.

ATTACHMENT A

Details of the *Digital ID (Accreditation) Data Standards 2024*

Chapter 1—Preliminary

Section 1.1 Name

1.1 This section provides that the name of this instrument is the *Digital ID (Accreditation) Data Standards 2024*.

Section 1.2 Commencement

1.2 This Accreditation Data Standards commences at the time as the Digital ID Act commences.

Section 1.3 Authority

1.3 The Accreditation Data Standards are made under section 99 of the Digital ID Act.

Section 1.4 Definitions

1.4 This section sets out the definition of expressions in the Accreditation Data Standards.

1.5 Notes 1 and 2 under this section relevantly provide that a number of expressions used in this instrument are defined in the Digital ID Act or the Accreditation Rules, respectively.

Section 1.5 Incorporated instruments

1.6 The Accreditation Data Standards incorporate by reference various documents as in force at the commencement of the Accreditation Data Standards.

1.7 Incorporating documents as in force from time to time is not appropriate because the Accreditation Data Standards are a non-disallowable legislative instrument. This means that any changes to these documents after the commencement of the Accreditation Data Standards will not automatically be incorporated into the Accreditation Data Standards.

1.8 The definition of approved cryptography is contained in the Accreditation Rules and therefore, the incorporated instrument that is within its definition is in force or existing from time to time as per Rule 1.5(1).

Table 1: Incorporated documents

Section(s)	Instrument title	Published by	Availability	Where to obtain
1.5 2.5 2.6	Guidelines for Cryptography	Australian Cyber Security Centre	Free, online	https://www.cyber.gov.au/resources-business-and-government/essential-cyber-

Section(s)	Instrument title	Published by	Availability	Where to obtain
2.9 2.10				security/ism/cyber-security-guidelines/guidelines-cryptography
2.1 2.7	*FIDO document authenticity verification requirements*	FIDO (Fast Identity Online) Alliance	Free, online	https://fidoalliance.org/specs/idv/docauth/document-authenticity-verification-requirements-v1.0-fd-20220815.html
1.5 2.2	*ISO/IEC 17025:2017*	International Organization for Standardization	Online purchase	https://www.iso.org/standard/66912.html
1.5 2.2 2.5	*ISO/IEC 19795-2:2007*	International Organization for Standardization	Online purchase	https://www.iso.org/standard/41448.html
1.5 2.5	*ISO/IEC TS 19795-9:2019*	International Organization for Standardization	Online purchase	https://www.iso.org/standard/78101.html
1.5	*ISO/IEC 2382-37:2022*	International Organization for Standardization	Free, online	https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip
1.5 3.13	*ISO/IEC 30107-1:2023*	International Organization for Standardization	Online purchase	https://www.iso.org/standard/83828.html
1.5 2.2 2.3	*ISO/IEC 30107-3:2023*	International Organization for Standardization	Online purchase	https://www.iso.org/standard/79520.html

1.9 The International Organization for Standardization (ISO) standards referenced are available for purchase through the websites linked in the table above. The ISO standards are not free to access online as they are copyrighted. The Department of Finance can facilitate access to view a hard copy of an ISO standard at an office in Australia by appointment, subject to licensing conditions. If access to the ISO standards is required, please email digitalid@finance.gov.au.

1.10 Use of the ISO standards referenced in these Accreditation Data Standards give confidence to the Digital ID Regulator and the community that the controls and information contained within are suitable and fit for purpose as a minimum baseline for all accredited entities.

1.11 Some free standards contain equivalent controls, however, those standards may not be updated regularly and robustly as the ISO standards. For instance, biometric technology is a rapidly changing and advancing field. As such, the ISO standards for biometric technology have been updated on a regular 5-year cycle by a panel of independent experts in the fields of biometrics. These standards are also consulted on before being published.

1.12 This provides confidence that relevant experts in the field of biometrics have developed and consulted on the ISO standards that are referenced in these Accreditation Data Standards. Engaging in a process to develop like-standards would not have been time or cost-effective, and it would create the risk of the Accreditation Data Standards not being of the same quality as the ISO standards.

Section 1.6 Application—Transitioned Accredited Entities

1.13 This section sets out the application of certain provisions for ***transitioned accredited entities***, as defined in rule 1.4 of the Accreditation Rules.

1.14 The term 'transitioned accredited entity' is intended to capture an entity who had previously been subject to the Trusted Digital Identity Framework (TDIF) pilot accreditation program which preceded the Digital ID Act. This program ran for over 5 years, with accredited entities being subject to the requirements of the TDIF. The Accreditation Rules and the Accreditation Data Standards are based on the requirements in the TDIF. While many requirements are similar, there are several new or changed requirements, which differ from the TDIF.

1.15 The effect of subsection 1.6(1) is that the requirement in paragraph (b) in column 2 of item 3 of the table in section 3.13 apply to a transitioned entity starting on the day that is 12 months after the day of commencement of the Accreditation Data Standards. This is because this is a new requirement that was not part of the TDIF, and as such, it is appropriate that transitioned accredited entities have 12 months to implement technical changes to their IT systems if they are subject to this requirement.

1.16 Subsection 1.6(2) confirms that a transitioned accredited entity is still subject to all other sections not specified in subsection 1.6(1).

Chapter 2—Data standards for accredited identity service providers

2.1 This Chapter applies only to certain kinds of Identity Service Providers (ISPs):

- For Part 1—Biometric Testing, this is because an ISP is the only kind of accredited service that is required to carry out biometric binding as part of the identity proofing requirements if the ISP is accredited to provide identity proofing levels IP2 plus, IP3 and IP4 in the Accreditation Rules.
- For Part 2—Authenticating to a digital ID, this is because an ISP that provides a reusable digital ID service is required to implement authentication and bind authenticators to that digital ID as per Division 3 of Part 5.1 of the Accreditation Rules.

Part 1—Biometric Testing

2.2 This Part of the Accreditation Data Standards sets out the testing requirements for biometric technology used to conduct biometric binding or authentication using biometric information. The testing standards that apply depend on which kind of biometric binding solution, biometric matching process, or authentication method using biometric information capability is implemented by the accredited entity. The table provided below is to assist entities in understanding which testing requirements set out in this Part will apply to them. Each column in the table below relates to a different type of biometric technology, including biometric matching solutions for identity proofing, covered by the Accreditation Rules and the Accreditation Data Standards, and each row corresponds to different sets of tests set out by the Accreditation Data Standards.

Table 2: Testing requirements for biometric technology

	Technical Biometric Matching (Rule 5.19)	**Source Biometric Matching**	**eIDVT (Rule 5.20)**	**Custom biometric capability (section 3.13, item 4)**
Section 2.3 Testing of presentation attack detection technology	Yes, if using online biometric binding (rule 5.17)	Yes, if using online biometric binding (rule 5.17)	Yes, if using online biometric binding (rule 5.17)	Yes
Section 2.5 Testing of the biometric matching algorithm	Yes	-	Yes	Yes

	Technical Biometric Matching (Rule 5.19)	Source Biometric Matching	eIDVT (Rule 5.20)	Custom biometric capability (section 3.13, item 4)
Section 2.6 Testing of source biometric matching	-	Yes	-	-
Section 2.7 Testing of eIDVT	-	-	Yes	-

Section 2.1 Definitions

2.3 This provision sets out the definitions which apply in this Part.

2.4 Specific definitions are required because biometrics, and particularly biometric testing, requires specific terminology with technical meaning. The definitions in this section are terms that have specific meaning for testing electronic identity verification technology (eIDVT), which assess images (or videos) of an identity document (such as a drivers licence) for authenticity. These terms help define key aspects of testing designed to determine if these eIDVT systems perform according to expectations, whether the systems meet the minimum standards set out in these requirements, and whether eIDVT testing is repeatable and has a pass/fail criteria.

2.5 Terms used throughout the Accreditation Data Standards relating to general requirements are defined in section 1.4 of the Accreditation Data Standards.

Section 2.2 Biometric testing entity

2.6 This section defines a ***biometric testing entity***, which is a person who meets the biometric testing criteria set out in this section. The term "person" is defined by the *Acts Interpretation Act 1901*. The kinds of testing that require a biometric testing entity are:

- Section 2.3 Testing of presentation attack detection technology
- Section 2.5 Testing of biometric matching algorithm, and
- Section 2.7 Testing of eIDVT.

2.7 Subsection 2.2(1) sets out a range of characteristics for a biometric testing entity, that, when considered together, establish the capability for one (or more) types of the biometric testing required by the Accreditation Data Standards. The overall value of testing that is carried out is influenced by whether the testing entity's laboratory (and its personnel) are appropriately qualified to perform the role.

2.8 Paragraph 2.2(1)(b) requires that a biometric testing entity can demonstrate that the laboratory used for testing biometric technology is appropriately qualified and certified to do that testing. This includes that the laboratory is accredited against ISO/IEC 17025:2017, which sets out the standards and requirements for a lab to demonstrate that it operates competently and can generate valid results for the types of testing it conducts.

2.9 In the case of biometric testing entities, the scope of ISO/IEC 17025:2017 accreditation requires that the lab be certified for the assessment of biometric technology testing standards. This ensures that a laboratory that is accredited against ISO/IEC 17025:2017 for one or more purposes other than biometric technology testing—for example, soil testing—cannot meet this requirement and be considered a biometric testing entity. Paragraph 2.2(1)(d) complements paragraph 2.2(1)(b) by ensuring that the biometric testing entity has established specific test methods for those standards if it conducts biometric testing for presentation attack detection or biometric matching algorithms.

2.10 Paragraph 2.2(1)(c) requires that the biometric testing entity has a policy for working with human test subjects that has been approved by a relevant national body. The relevant national body can be the national body within that biometric testing entity's operational jurisdiction. An example of a relevant national body in Australia is the National Health and Medical Research Council.

2.11 The biometric testing entity requirement is designed in such a way that a National Voluntary Laboratory Accreditation Program (NVLAP) accredited testing entity (as defined by the United States Department of Commerce's National Institute for Standards and Technology (NIST)) would automatically meet most components of this standard. NVLAP is a voluntary accreditation program managed by NIST, and provides accreditation for laboratories that perform conformance testing, interoperability testing, technology testing, scenario testing, and operational and usability testing for biometrics products (systems and subsystems). NVLAP is considered to be of a high standard and has global recognition within the biometrics industry. As such, achieving NVLAP accreditation is considered an equivalent way to meet these requirements and assists with avoiding duplication of effort for such entities.

2.12 Alternatively, non-NVLAP entities may meet these requirements individually, by asserting compliance with each element. These requirements have been determined by selecting the most relevant international standards that apply to testing biometric systems, and all of these requirements must be met if such an entity wanted to achieve NVLAP accreditation to become a biometric testing entity.

Section 2.3 Testing of presentation attack detection technology

2.13 This section prescribes requirements that the biometric testing entity must follow when performing presentation attack detection (PAD) testing.

Background to PAD testing

2.14 An ISP that conducts online biometric binding must engage an eligible biometric testing entity to test their PAD technology's ability to detect presentation attacks. These testing requirements are intended to mandate a minimum level of assurance to ensure an entity's PAD technology is fit for purpose. Generally, PAD testing involves personnel from the biometric testing entity identifying and executing ways to fool the PAD subsystem into accepting a fraudulent biometric presentation (e.g., using a mask, make-up, deepfake videos, etc.).

Strength of PAD testing

2.15 Defined in subsection 2.3(1) are the types of attack vectors, which are ***level A presentation attack instrument species*** and ***level B presentation attack instruments species*** for PAD testing. These are used by a testing entity as the primary way the strength of the testing is determined.

2.16 The strength of a particular attack type is classified based on how much time, effort, and knowledge an attacker would need to execute it. For example, printing a 2D image of an individual's face is much easier than creating a silicon-based mask of an individual's face. The testing required here involves the use of low-to-medium (i.e. level A and level B) sophistication attacks. High sophistication attacks are considered beyond the scope of this testing - but may be considered for inclusion in future if they become practical for testing labs to implement withing reasonable costs or such attacks become more commonly attempted by potential threat actors.

Requirements for testing procedures

2.17 Subsections 2.3(2) and (3) require the use of ISO/IEC 30107-3 compliant testing and reporting to ensure the test planning, execution, and associated reporting is delivered according to international standards and best practice for this kind of testing. Additionally, this testing is intended to mimic 'real life' scenarios, as far as it is feasible to do so, by requiring the ISP to provide the PAD subsystem to the testing entity exactly as intended to run in its deployed state. The standards for the PAD technology to meet are high, as specified in item 3(a) of the table under subsection 2.3(3). However, should the testing of the PAD technology fail to meet items (3)(a), the items in (3)(b)(i) and (ii) allow the entity to reconfigure its PAD technology, if necessary, and then retest the technology to demonstrate that it can meet the requirements in item 3(c) and item (4).

Section 2.4 ISP's response to testing report

2.18 This section sets out requirements for the ISP's response to the PAD testing report. This response is intended to provide ISPs with the ability to respond and implement enhancements to PAD technology to address issues identified by the testing and demonstrate that those issues have been satisfactorily resolved or will be resolved or mitigated at a later date.

2.19 Generally, PAD systems are probabilistic in nature, and chance scenarios can sometimes result in unexpected or unrepeatable outcomes. This may result in an attack presentation classification error rate (APCER) of 0% (i.e., the metric at item (3)(a) of the table under subsection 2.3) not being achieved by the system under test. An APCER of 0% effectively means a PAD system must make no errors during the testing process. While this is generally considered achievable for good PAD systems operating on level A and B artefacts, this risk-based response is designed to allow for the non-deterministic nature of PAD technologies.

2.20 An ISP's response to a testing report provides the ISP with an opportunity to provide a risk-based response with contextual information on how an issue identified during the PAD testing process has been resolved. Amongst other information, the ISP could provide information about the following factors specific to PAD testing:

- Repeatability: whether the PAD system be consistently fooled by the artefact that produced the reported error.
- Likelihood: whether the presentation attack type likely to be used against the system when it is operational.
- Action taken: whether the configuration of the PAD system been updated as a result of the results of the testing.

Section 2.5 Testing of the biometric matching algorithm

2.21 This section prescribes requirements the biometric testing entity must follow when performing testing of the biometric matching algorithm. The purpose of this section is to ensure that biometric matching algorithms used for face biometric matching undergo benchmark performance testing by a biometric testing entity.

Why is algorithm testing necessary?

2.22 Face matching algorithms are designed to compare 2 facial images and determine if they are of the same person or not. Within the context of identity proofing by an ISP, this involves determining if an individual's "selfie" image (acquired image) and the trusted reference image corresponding to the photo ID (for technical biometric matching, extracted from an ePassport) is of the same person. Biometric matching algorithms can be more reliable than a human operator manually comparing an individual's face to an image, however they are not 100% accurate.

2.23 Biometric matching errors are classified as a false match (incorrectly classifying 2 images as being of the same person) or a false reject (incorrectly classifying 2 images of the same person as being different people). Some algorithms perform better than others and so the algorithm testing required by this section ensures that all algorithms used by accredited entities meet minimum accuracy standards.

2.24 Testing the biometric matching algorithm in accordance with ISO/IEC 19795-2 is considered the industry standard. By requiring the use of a biometric testing entity, it ensures that the test planning, execution, and associated reporting of test results is robust and delivered according to best practice.

Section 2.6 Testing of source biometric matching

2.25 This section prescribes requirements for an ISP to test the image quality profile used before an image is submitted to a photo ID authoritative source, the overall reliability of the connection to the authoritative source and the end-to-end repeatable process for an entity's use of source biometric matching.

2.26 Source biometric matching refers to the process of using an authoritative source to verify that an individual's acquired image (after it has passed presentation attack detection) biometrically matches the corresponding image for the photo ID which is stored in the authoritative source. This is done by completing a one-to-one biometric match, meaning that the individual's acquired image is only ever attempted to match against the image that corresponds to their photo ID (for example, the image stored by the authoritative source of the individual's passport photo).

2.27 The testing defined here ensures the ISP has correctly connected and configured its communications with that authoritative source and has confirmed that source biometric matching works as a repeatable process.

2.28 **Example scenario:** An ISP could conduct source biometric matching through the Face Verification Service, one of the identity verification services established by the Identity Verification Services Act 2003. In this scenario, the ISP does not perform any biometric matching - it simply captures the individual's selfie (the acquired image), checks it is of high enough quality by establishing that the image meets the image quality profile, ensures that it passes PAD testing, and provides this image and the reference number for the photo ID to the Face Verification Service. The Face Verification Service will usually provide a binary yes/no response for match/no match. (If an ISP has a direct connection with an alternative authoritative source to the Face Verification Service, the ISP could seek to use that authoritative source to conduct source biometric matching).

Section 2.7 Testing of eIDVT

2.29 This section prescribes requirements the biometric testing entity must follow when performing testing of an eIDVT algorithm. The testing requirements in this section require testing in accordance with the FIDO document authenticity verification requirements and the additional requirements set out in the tables in this section.

2.30 Testing an eIDVT algorithm evaluates its ability to distinguish between genuine photo IDs (i.e., photo IDs that were issued by an authoritative source and have not been tampered with) and fraudulent photo IDs (i.e., photo IDs that are either counterfeits or forgeries, either physical or digital).

2.31 Testing an eIDVT requires the biometric testing entity to meet the additional requirements set out in subsection 2.7(2). These include requirements that the biometric testing entity is a FIDO Accredited Laboratory, as defined by the FIDO document authenticity verification requirements. This ensures that the biometric testing entity has the skills, experience and qualifications necessary to carry out the eIDVT testing and that this has been independently recognised and certified by the FIDO Alliance.

2.32 Subsection 2.7(3) sets out the testing requirements. Subparagraph(3)(a) ensures that the scope of the testing includes the eIDVT requirements in rule 5.20 of the Accreditation Rules. This is to ensure that the Digital ID Regulator has independent verification that the entity's eIDVT is configured in accordance with the Accreditation Rules.

2.33 Subparagraph 2.7(3)(b) provides that the eIDVT must be tested in accordance with subsection 2.7(4) in relation to paragraph 5.20(4)(b) of the Accreditation Rules. This helps ensure that an entity's eIDVT must be able to have determined that the photo ID processed through the eIDVT is physically present at the time of capture by testing for document liveness.

2.34 Subparagraphs 2.7(3)(c) and (d) provide that the testing of the eIDVT is to be conducted using the existing testing procedure as specified in FIDO document authenticity verification requirements and published by the FIDO Alliance. The additional requirements set out in the table must also be met. These additional requirements increase the overall assurance that the eIDVT testing provides, taking into account for the unique Australian context of documents which are eligible to be used for eIDVT (i.e., all states and territories issue different driver's licences and proof-of-age cards which contain different security features, font and colour settings and other information).

2.35 Subsection 2.7(4) sets out the standards for eIDVT testing for document liveness. The purpose of these requirements is to ensure that the testing involves reproduced documents which should be classified as fraudulent by the eIDVT, and test cases that are both physical and digital, to ensure that the eIDVT can detect live presentations of a fraudulent document (document liveness). Currently, testing for document liveness testing is out-of-scope for the published version of the FIDO document authenticity verification requirements. Ensuring that any eIDVT used for identity proofing is able to ensure that a real version of the document is present at the time the individual was conducting a biometric match using eIDVT is critical to eIDVT being included as a biometric matching process for identity proofing by accredited entities. Therefore, the bespoke requirements for document liveness testing in subsection 2.7(4) were developed by subject matter experts and provided in the Accreditation Data Standards to ensure the high assurance of eIDVT used in the identity proofing process. Subsection 2.7(5) requires that the biometric testing entity provide a report to the ISP to ensure the eIDVT testing has been carried out in accordance with the requirements in this section, including the requirements set out in subsection 2.7(3) which includes references to the Accreditation Rules.

2.36 Subsections 2.7(6) and (7) set out the requirements for managing the kinds of documents and credentials accepted by the eIDVT for verification and the retesting requirements should the ISP add new types of documents or credentials that can be accepted by the eIDVT for verification. The intent of this requirement is to ensure that only the documents and credentials that have been tested in accordance with these requirements are accepted. This is particularly important where an ISP may not accept, for example, a driver's licence issued by one jurisdiction (for whatever reason) and therefore, has not completed the required testing for that document or credential in its initial eIDVT testing. This requirement is due to the Australian context having different states and territories issue driver's licences and proof-of-age cards with different security and other unique features that require an eIDVT to be trained in order to be able to detect tampering with the document.

Part 2—Authenticating to a digital ID

Division 1—Authentication levels

3.1 The authentication requirements in this Division are based on the authentication requirements set out in the NIST Special Publication 800-63b Digital Identity Guidelines for Authentication and Lifecycle Management (NIST 800-63b). NIST 800-63b is considered a world-leading standard for authentication. A version of these guidelines is publicly available at Digital Identity Guidelines: Authentication and Lifecycle Management (nist.gov).

3.2 NIST 800-63b has not been incorporated into these Accreditation Data Standards by reference due to the nature of the document and requirements being tailored for the United States Government services. However, the requirements in this Part have been adapted from NIST 800-63b to better suit the Australian digital ID context.

3.3 This Division defines authentication levels and the authenticator types that can be used (either individually or in combinations) to meet authentication levels.

Section 3.1 Authentication levels: AL Table

3.4 The ***AL Table*** defines the features of 3 authentication levels an ISP can provide for individuals. This includes defining which authentication levels can be used to authenticate a digital ID at each identity proofing level.

3.5 These authentication levels are designed to give assurance to entities that the individual remains in control of their digital ID and mitigate risks associated with unauthorised access to personal information and fraudulent activity. The AL Table is a structured framework that delineates authentication requirements across different authentication levels (AL1, AL2 and AL3). The AL Table is ranked from lowest assurance (AL1) to highest assurance (AL3), and specifies:

- Types of authenticators permissible for each AL;
- Reauthentication requirements for each AL;
- Mandatory security requirements for each AL; and
- Permitted combinations of authenticators and identity proofing levels.

3.6 The authentication levels are aligned to the risk tolerance of an ISP’s accredited services and IP levels, as required by the AL Table and the IP Levels Table (as specified in rule 5.10 of the Accreditation Rules). Additionally, the authentication levels correspond to the level of protection they afford, with higher authentication levels demanding advanced capabilities and significant resources for adversaries to exploit the authentication process. Authentication at higher ALs progressively reduces the risk of attacks that compromise a digital ID.

3.7 **Authenticator Level 1**: AL1 provides some assurance that the individual controls an authenticator bound to the ISP. Authentication at this level requires either single-factor or multi-factor authentication using a wide range of available authentication technologies. Successful authentication necessitates the individual proving possession and control of the authenticator via a secure authentication protocol.

3.8 **Authenticator Level 2**: AL2 provides high confidence that the individual controls an authenticator(s) bound to the ISP. Authentication at this level requires proof of possession and control of 2 different authentication factors and is required through secure authentication protocol(s).

3.9 **Authenticator Level 3**: AL3 provides very high confidence that the individual controls authenticator(s) bound to the ISP. Authentication at AL3 is based on proof of possession of a key through a cryptographic protocol. AL3 authentication necessitates a hardware-based authenticator and an authenticator that offers phishing resistance. The same device may satisfy both requirements. For authentication at AL3, individuals are required to prove possession and control of 2 distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.

3.10 Item 2 of the AL Table prescribes the circumstances in which an individual must reauthenticate to their digital ID, or the authenticated session is to be terminated. This is an important security control to ensure that where an individual forgets to logout of their digital ID or a service, the session will automatically terminate after a period of time unless the individual reauthenticates according to the requirements in item 2. This reduces the risk of account takeover, for example, if an individual is using their digital ID via a publicly accessible computer and forgets to logout, or in situations where an attacker may steal an unlocked device.

Security requirements:

3.11 AL1, AL2 and AL3 authentication must have ***MitM (man-in-the-middle)*** resistance, protecting against an adversary intercepting communication between an individual and an ISP.

3.12 AL3 authentication must have "Phishing resistance", protecting against an adversary impersonating an ISP, which if not mitigated could lead to an individual revealing sensitive information (e.g., memorised secret) to an adversary.

3.13 AL3 authentication is required to have ***AE-compromise resistance***, as defined in section 1.5.

3.14 AL2 and AL3 authentication must have "Replay resistance", preventing adversaries from capturing transmitted authentication or access control information and using it to gain unauthorised access.

3.15 AL3 authentication must have "Authentication intent", which refers to preventing an adversary using malware with a directly-connected physical authenticator (e.g., multi-factor cryptographic device) without the individual's knowledge. An authentication process demonstrates intent when it requires the individual's explicit response to each authentication or reauthentication request.

Division 2—Binding authenticators to a digital ID

3.16 This Division provides data standards for binding an authenticator to a digital ID. Binding authenticators is required at the beginning of an account lifecycle and where an ISP is managing or maintaining a digital ID. An individual authenticating to a digital ID using an authenticator asserts ownership and control of their digital ID.

Section 3.2 Binding an authenticator when generating a digital ID

3.17 This section prescribes requirements for ISPs when binding an authenticator to a digital ID at the time the digital ID is created. This includes standards for the online context and the in-person context.

3.18 Binding an authenticator to a digital ID is the process of establishing an association between a specific authenticator and an individual's digital ID, enabling the authenticator to be used — possibly in conjunction with other authenticators — to authenticate for that digital ID.

3.19 If enrolment and binding cannot be completed in a single physical encounter or electronic transaction (i.e., within a single protected session), the prescribed methods must be used to ensure that the individual for whom the digital ID was created is the same person who initiated the binding process.

Division 3—Standards for kinds of authenticators

3.20 This Division prescribes requirements for the generation, binding, management and distribution of allowable authenticator types defined by the AL Table in section 3.1.

Section 3.3 Memorised secrets

3.21 The table in this section prescribes requirements for the generation, binding, management and distribution of memorised secrets. This includes standards for memorised secrets that are generated by the ISP and chosen by the user.

3.22 A ***memorised secret*** is defined in section 1.5. Memorised secrets need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value. A memorised secret is considered to be a type of authenticator that is *something you know*.

Section 3.4 Look-up secrets

3.23 The table in this section prescribes requirements for the generation, binding, management and distribution of ***look-up secrets***. This includes standards for how look-up secrets are delivered to a user, usage parameters for physical look-up secrets such as grid cards, and storage requirements for look-up secrets.

3.24 A ***look-up secret*** is defined in section 1.5. The individual uses the authenticator to look up the appropriate secret(s) needed to respond to a prompt from the ISP. For example, the ISP may ask an individual to provide a specific subset of the numeric or character strings printed on a card in table format. A common application of look-up secrets is the use of "recovery keys" stored by the individual for use in the event another authenticator is lost or malfunctions. A look-up secret is considered to be a type of authenticator that is *something you have*.

Section 3.5 Single-factor one-time password devices

3.25 The table in this section prescribes requirements for the generation, binding, management and distribution of single-factor one-time password (OTP) devices. This includes standards for the use of the cryptographic key, the generated nonce, and parameters for the use of the one-time password.

3.26 A ***single-factor one-time password device*** is defined in section 5.1. It generates OTPs. This category includes hardware devices and software-based OTP generators installed on devices such as mobile phones. These devices have an embedded secret that is used as the seed for generation of OTPs and does not require activation through a second factor. The OTP is displayed on the device and manually input for transmission to the verifier, thereby proving possession and control of the device. An OTP device may, for example, display 6 characters at a time. A single-factor OTP device is considered to be a type of authenticator that is something you have.

3.27 Single-factor OTP devices are similar to look-up secret authenticators, except that the secrets are cryptographically and independently generated and compared by the ISP. The secret is based on a nonce, which is a number or piece of data used only once. A nonce may be time-based or from a counter on the ISP.

Section 3.6 Multi-factor one-time password devices

3.28 The table in this section prescribes requirements for the generation, binding, management and distribution of multi-factor one-time password devices. This includes standards for the use of the cryptographic key, the generated nonce, parameters for the use of the one-time password, and specific rules about the activation factor for the authenticator.

3.29 A ***multi-factor one-time password device*** is defined in section 1.5. It includes hardware devices and software-based OTP generators installed on devices such as mobile phones. The second factor of authentication may be achieved through some kind of integral entry pad, an integral biometric reader, or a direct computer interface (e.g., USB port). The OTP is displayed on the device and manually input for transmission to the ISP. For example, an OTP device may display 6 characters at a time, thereby proving possession and control of the device. The multi-factor OTP device is considered to be a type of authenticator that is something you have, and it is activated by either something you know or something you are.

Section 3.7 Single-factor cryptographic software

3.30 The table in this section prescribes requirements for the generation, binding, management and distribution of single-factor cryptographic software. This includes standards for the use of the cryptographic key, the challenge nonce, and the use of the challenge key.

3.31 ***Single-factor software cryptographic software*** is defined in section 1.5. Authentication using single-factor software cryptographic software is accomplished by proving possession and control of the key. The authenticator output is highly dependent on the specific cryptographic protocol (i.e., AACP), but it is generally some type of signed message. The single-factor software cryptographic authenticator is considered to be a type of authenticator that is something you have.

3.32 Examples may include a digital certificate managed by an operating system keychain storage.

Section 3.8 Multi-factor cryptographic software

3.33 The table in this section prescribes requirements for the generation, binding, management and distribution of ***multi-factor cryptographic software***. This includes standards for the use of the cryptographic key, the challenge nonce, and specific rules about the activation factor for the authenticator.

3.34 A multi-factor software cryptographic software is defined in section 1.5. Authentication using multi-factor cryptographic software is accomplished by proving possession and control of the key. The authenticator output is highly dependent on the specific cryptographic protocol (i.e., AACP), but it is generally some type of signed message. The multi-factor cryptographic software authenticator is considered to be a type of authenticator that is *something you have* and is activated by either *something you know* or *something you are*.

3.35 Examples may include digital certificates issued by a Certification Authority, which is an entity that stores, signs, and issues digital certificates and acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate.

Section 3.9 Multi-factor cryptographic devices

3.36 The table in this section prescribes requirements for the generation, binding, management and distribution of ***multi-factor cryptographic devices***, as defined in section 1.5. This includes standards for the use of the cryptographic key, the challenge nonce, specific rules about the external hardware layer of the device, and specific rules about the activation factor for the authenticator.

3.37 Authentication using multi-factor cryptographic device is accomplished by proving possession of the device and control of the key. The authenticator output is provided by direct connection to the individual's endpoint and is highly dependent on the specific cryptographic device and protocol, but it is typically some type of cryptographically signed message. The multi-factor cryptographic device is considered to be a type of authenticator that is *something you have* and is activated by either *something you know* or *something you are*.

3.38 Examples of multi-factor cryptographic devices may include a smart card with an embedded digital certificate.

3.39 Although cryptographic devices (single-factor or multi-factor) contain software, they differ from cryptographic software authenticators in that all embedded software on the hardware device is under the control of the ISP or issuer.

Section 3.10 Single-factor cryptographic devices

3.40 The table in this section prescribes requirements for the generation, binding, management and distribution of ***single-factor cryptographic devices***, as defined in section 1.5. This includes standards for the use of the cryptographic key, the challenge nonce, and specific rules about the external hardware layer of the device.

3.41 The single-factor cryptographic device uses embedded symmetric or asymmetric cryptographic keys and does not require activation through a second factor of authentication. Authentication is accomplished by proving possession of the device via the authentication protocol. The authenticator output is provided by direct connection to the individual's endpoint and is highly dependent on the specific cryptographic device and protocol, but it is typically some type of signed message. A single-factor cryptographic device is considered to be a type of authenticator that is *something you have*.

3.42 Examples of single-factor cryptographic devices may include a USB key fob.

Section 3.11 Out-of-band devices

3.43 The table in this section prescribes requirements for the generation, binding, management and distribution of ***out-of-band devices***, as defined in section 1.4. This includes standards for how the out-of-band device must be authenticated by the ISP, specific rules for how the secret must be shared to the out-of-band device, and additional restrictions for when the out-of-band device uses the ***public switched telephone network (PSTN)***. The out-of-band device is possessed and controlled by an individual and supports private communication over a secondary channel, separate from the primary channel for e-authentication. An out-of-band device is considered to be a type of authenticator that is *something you have*.

3.44 An out-of-band authenticator must not use email or voice-over-IP (VOIP) telephone numbers, as these methods do not prove possession of a specific device, failing the requirement for an authenticator that is *something you have*.

3.45 Examples of out-of-band devices may be a mobile phone.

3.46 The use of the PSTN for out-of-band verification (i.e., sent over SMS) has additional restrictions as described in item 10. These additional requirements are needed due to the additional risk associated with PSTN delivery of an out-of-band authentication secret, such as device swap, SIM change, number porting, or other abnormal behaviour associated with PSTN.

Division 4—Standards for security requirements

Section 3.12 Standards for security requirements

3.47 The table in this section prescribes the standards for security requirements for authenticating an individual to their digital ID, as well as security requirements for:

- Phishing resistance (when authenticating to AL3)
- AE-compromise resistance (when authenticating to AL3)
- Authentication intent
- Rate limiting (throttling)
- Authenticator attestation where the authenticator attestation is signed

Phishing Resistance

3.48 Phishing resistance is the technique of recognising and avoiding deceptive attempts from an adversary to steal sensitive information through fraudulent interactions, often disguised as trustworthy entities. Item 1 of the table details the requirements for an accredited entity to implement phishing resistance when authenticating to AL3.

AE-Compromise Resistance

3.49 AE-compromise resistance refers to the use of authentication protocols designed to eliminate the need for accredited entities to store authentication secrets permanently, ensuring security by associating public keys with an Approved Authentication Credential Authority and requiring cryptographic keys with a minimum of 112 bits of security strength. The 112 bits of security strength refers to cryptography with 2^{112} possible combinations, making the key highly resistant to brute force attacks, where an attacker might try numerous combinations to guess the key. These requirements are designed to protect keys against compromise (e.g., an adversary stealing a cryptographic key) and ensuring the keys are managed and issued by a trusted authority.

Authentication Intent

3.50 Authentication intent refers to when an authenticator requires the individual's explicit response to each authentication or reauthentication request to demonstrate intent (e.g., the intent to authenticate must come directly from the authentication device itself). This is required when proving an identity at AL3, with these specifications detailed in item 3 of this table, ensuring that the individual is consciously participating in the authentication.

3.51 For example, the device might require the individual to perform a specific action, such as pressing a button or providing a biometric input (e.g., like a fingerprint), to confirm their intent to authenticate. This requirement helps to prevent unauthorised access, as it ensures that the authentication process cannot proceed without the individual's active involvement.

Rate Limiting (throttling)

3.52 Rate limiting (throttling) is the practice of restricting the number of logins attempts within a specific timeframe to prevent unauthorised access through brute force or guessing attacks. Item 4 of this table specifies which kinds of authenticators require rate limiting and outlines the specifications for implementing it. ISPs may consider whether to implement more restrictive throttling requirements than those in item 4 (c) depending on the security risks and the type of authenticators it implements.

Authenticator Attestation

3.53 Authenticator attestation is the process of proving the authenticity and integrity of an identity using a digital signature secured through cryptography. Item 5 of this table specifies that the attestation must be verified with a digital signature of at least 112 bits of effective security strength. The 112 bits of effective security refers to the high level of cryptographic protection, 2^{112} possible combinations or keys to generate that signature, making it difficult for an adversary to forge or tamper with the attestation's authenticity.

3.54 The attestation must be verified by the ISP to ensure it meets the security standards and that the identity being authenticated is genuine.

Division 5—Authentication using biometric information

Section 3.13 Standards for authentication using biometric information

3.55 The table in this section prescribes requirements for ISPs when binding or managing authenticators that use an individual's biometric information. This includes authentication that uses the biometric capability provided by the original equipment manufacturer of a smartphone (referred to as in-device biometric capability) and biometric authentication that is fully designed and implemented by the ISP (referred to as a custom biometric capability). This section also prescribes the requirements for how and when biometric information can be used for authentication and for testing the performance of the biometric capability for authentication, including the requirements relating to the use of a biometric matching algorithm and PAD algorithm.

3.56 Authentication using biometric information uses the measurement of physical characteristics, which are considered to be a type of authentication factor which is something you are. Common examples include fingerprint or facial characteristics. This section provides requirements for 2 key topics: how authentication using biometric information must operate, and how biometric technology used for authentication must be tested to ensure it meets minimum performance requirements.

3.57 In-device biometric capability and custom biometric capability provide differing levels of assurance.

3.58 Custom biometric systems are designed, implemented and tested by the ISP (or with a third-party technology provider). This includes enrolling and managing the biometric template. As a result, ISPs that use custom biometrics for authentication have greater assurance that the individual presenting the biometric for authentication is the same individual present at identity proofing.

3.59 In contrast, in-device biometrics relies on the smartphone's capabilities, and implicitly trusts the binary (match/no match) response from the smartphone's application programming interface. While smartphone biometric authentication is generally considered very secure, it is easy for users to enroll fingerprints from multiple individuals onto a single device. As a result, biometric authentication using in-device capability asserts device control, rather than *something you are.*

3.60 Among other reasons associated with hardware and software requirements for authenticators, in-device biometric capability is not eligible for use at AL3, and custom biometric capability is eligible.

3.61 Custom biometric capability and in-device biometric capability require differing levels of testing:

- Custom biometric systems are required to be tested. Because the ISP is in complete control of their biometric system, it is easy to engage a biometric testing entity to test the matching and PAD algorithms.
- In-device systems cannot feasibly be tested. Because of the reliance on the capability of individual smartphones, ISPs cannot reasonably be expected to

test all (or even a meaningful subset) of devices that could be used by individuals.

3.62 Testing requirements for biometric authentication systems are similar to those for biometric systems used for identity proofing (e.g., testing the biometric matching algorithm performance is identical) but PAD testing differs slightly. Notably, PAD systems for authentication are allowed a higher error rate than that of PAD being used for identity proofing.

3.63 Identity proofing (i.e., often a first-time visit) and authentication (i.e., a return visit) represent 2 differing contexts, which is why the requirements for testing in this section differ from the testing requirements specified in section 2.3 of the Accreditation Data Standards. Identity proofing:

- takes longer,
- requires higher levels of assurance to be met, and
- has greater impact if a fraudulent transaction occurs.

This can be contrasted with authentication, which:

- usually occurs relatively quickly, and
- generally, involves fewer checks than identity proofing.

3.64 Subsequently, PAD testing requirements for custom biometric capability systems allow for a lower accuracy rate than PAD testing requirements for PAD technology used during online biometric binding for *identity proofing*. This reflects the differing use contexts and risk profiles between identity proofing and authentication, as well as the limitations of the current state PAD technology which needs to balance the demands of accuracy and usability.

3.65 The 10% APCER metric used in item 4(k) of this table aligns with the metrics for PAD technology operation for authentication in the current version of NIST 800-63b.

ATTACHMENT B

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

3.1 Digital ID (Accreditation) Data Standards 2024

4.1

The *Digital ID (Accreditation) Data Standards 2024* (the Accreditation Data Standards) are compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Accreditation Data Standards

The Accreditation Data Standards set out requirements for ISPs which:

- support the operation of the accreditation scheme and the *Digital ID (Accreditation) Rules 2024* (the Accreditation Rules), which aim to provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity for use in online transactions with government and businesses;
- provide a robust technical framework of requirements to provide assurance that biometric technology has been tested and operates to a high standard; and
- provide technical configuration requirements for authentication services to facilitate and promote trust in these kinds of digital ID services accredited under the accreditation scheme.

Human rights implications

The Accreditation Data Standards engage the following rights:

- The right to protection from arbitrary or unlawful interference with privacy contained in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR), and also referred to in Article 16 of the *Convention on the Rights of the Child* (CROC) and Article 22 of the *Convention on the Rights of Persons with Disabilities* (CRPD).
- The rights to equality and non-discrimination, contained in Article 26 of the ICCPR and Article 2 of the CROC.

PROTECTION FROM ARBITRARY OR UNLAWFUL INTERFERENCE WITH PRIVACY

Article 17 of the ICCPR prohibits arbitrary or unlawful interference with privacy. It provides that:

- No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
- Everyone has the right to the protection of the law against such interference or attacks.

Article 16 of the CROC and Article 22 of the CRPD contain similar rights.

The *Digital ID Act 2024* (the Digital ID Act) requires that accredited entities continue to comply with existing privacy protections in the Privacy Act or, for State or Territory entities, their local privacy law. Where a State or Territory accredited entity is not subject to a local privacy law, and wishes to become an accredited provider, the Digital ID Act prescribes that the entity must enter into a binding agreement that would require them to comply with the APPs. Australian Government agencies that are subject to the Privacy Act are also subject to the privacy governance code. In the context of the Rules, if an accredited entity is not an agency within the meaning of the Privacy Act, it must still comply with the privacy governance code in respect of its DI data environment and accredited services as if it were an agency for the purposes of the code.

The Accreditation Data Standards engage with the right to protection from arbitrary or unlawful interference with privacy to the extent that they prescribe the standards for authentication to a digital ID using biometric information. This authentication may be conducted via in-device capability or custom capability. Using custom capability, the accredited entity collects, holds and uses an individual's biometric information for the purpose of authentication. Due to the options for authentication set by the Accreditation Data Standards, not all ISPs will use a custom biometric capability to authenticate individuals to their digital ID. If an ISP includes the use of a custom biometric capability to satisfy the authentication requirements for a reusable digital ID, the Accreditation Data Standards set the requirements for ensuring that the biometric information is stored and protected appropriately through the use of encryption. These protections complement the protections set out in the Digital ID Act, which sets out the requirements for the retention of biometric information for authentication purposes and its destruction once an individual withdraws their consent.

For completeness, the Accreditation Data Standards do not engage with the right to protection from arbitrary or unlawful interference with privacy to the extent that they prescribe the testing procedures for the testing of biometric information. This is because the testing must be conducted by a biometric testing entity that is external to the accredited entity and/or its corporate group, and the testing sample need not be individuals who use the accredited entity's services (i.e. users of the digital ID service).

This means that the biometric testing entity and the individuals whose biometric information is tested as per the testing requirements in the Accreditation Data Standards may not be regulated by the Digital ID Act, the rules or the Accreditation Data Standards. The Accreditation Data Standards prescribe the requirements for a biometric testing entity, which the accredited entity must ensure their chosen testing entity meets. However, the Accreditation Data Standards do not affect or involve the privacy of persons any more so than already takes place for biometric testing undertaken by entities as part of other regulatory frameworks.

MEASURES TO ENSURE LIMITATIONS ON A PERSON'S PRIVACY ARE NOT ARBITRARY NOR UNLAWFUL

The Act sets out restrictions on collecting, using and disclosing biometric information, which apply to accredited entities, including entities which use custom capability to authenticate individuals to their digital ID or who are required to complete biometric testing in accordance with the Accreditation Data Standards.

The privacy of individuals engaged by the biometric testing entity as part of the testing requirements are also protected by existing regulatory frameworks, such as the *Privacy Act 1988*.

CONCLUSION

The Accreditation Data Standards engage with Article 17 of the ICCPR in a direct manner but with limited scope. This is because an accredited entity may choose to authenticate individuals using other options for authentication that do not require the accredited entity to collect, hold or use an individual's biometric information.

In instances when the right is engaged, the protections and safeguards set out in the Digital ID Act and the Accreditation Rules apply to ensure that individuals are informed that their privacy may have been interfered with and are therefore able to make decisions to protect their personal information.

The limitations on privacy are permissible as they are reasonable, necessary and proportionate to give effect the objectives of the Digital ID Act.

THE RIGHTS OF EQUALITY AND NON-DISCRIMINATION

Article 26 of the ICCPR states:

> *All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.*

Article 2 of the CROC contains a similar right.

The Accreditation Data Standards build on the protections provided for by the Digital ID Act and the Accreditation Rules to promote the rights of equality and non-discrimination.

The test procedures set out requirements relating to testing a diverse range of individuals. Subparagraph 2.5(2)(c)(iii) of the Accreditation Data Standards prescribes that an ISP that conducts biometric testing must test the biometric testing algorithm using representatives from a diverse range of individuals, having regard to the range of individuals who may be potential users of the ISP's accredited services.

Further, for eIDVT testing for document liveness requirements, both the images used and the test set conditions include requirements relating to the representation of a diverse range of individuals, including individuals with disability and individuals with a diverse range of age, gender, ability and ethnicity.

As a result of these standards, one of the outcomes of testing is assurance that the biometric matching algorithm or eIDVT does not selectively disadvantage or discriminate against any group (i.e. the test is not limited to only include people with similar physical appearance, gender or age).

These standards affirm the protections provided for under the Digital ID Act and the Accreditation Rules. This ensures that systems are tested across a wide range of people so any technical issues, including for different groups, are identified and then able to be rectified.

Conclusion on overall compatibility with human rights

The Standards are compatible with human rights and, to the extent that they may limit human rights, those limitations are reasonable, necessary and proportionate.

Senator the Hon Katy Gallagher, Minister for Finance