# Digital ID rules and data standards – feedback template

## Digital ID Bill 2024

The Digital IDBill 2024 and the Digital ID (Transitional and Consequential Provisions) Bill 2024 were passed on 16 May 2024. The Bills are expected to receive Royal Assent in the coming weeks with the Acts expected to commence by November 2024.

This legislation authorises a package of multiple legislative instruments which govern the Accreditation Scheme and the Australian Government Digital ID System. The Digital ID Act 2024 will be the primary legislation for the Accreditation Scheme and the Australian Government Digital ID System. The Act will allow for legislative rules and data standards to be made. This public consultation focuses on three of these rules and standards:

* the draft Digital ID Rules 2024(Digital ID Rules),
* the draft Digital ID (Accreditation) Rules 2024 (Accreditation Rules), and
* the draft Digital ID (Accreditation) Data Standards 2024 (Accreditation Data Standards).

Copies of these rules and data standards can be found on the Digital ID website.

Copies of the Digital ID Bill can be found on the [Parliament of Australia website](https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/bills/s1404_third-senate/0000%22).

## Have your say

Using this template for your feedback is optional. It is provided for your convenience and contains consultation questions that you may wish to use to direct your feedback. You may fill out as little or as much of the template as you want.

The consultation is directed towards the changes made to the Digital ID Rules, Digital ID (Accreditation) Rules and (Accreditation) Data Standards since the first public consultation in September 2023 and for matters regarding Digital ID that are critical for your organisation.

Please ensure that your consultation feedback is submitted by 5:00pm 25 June 2024 via the submissions page on the Digital ID website. There is an attachment option for you to upload and submit your feedback via a word or pdf document.

## Consultation questions

The following tables contain consultation questions that you may wish to use to direct your feedback. These questions are for issues or policy that may change in response to the consultation feedback.

## Template navigation

* [Attachment A – General comments](#_Attachment_A:_General)
* [Attachment B – Digital ID Rules feedback](#_Attachment_B:_Digital)
* [Attachment C – Digital ID (Accreditation) Rules feedback](#_Attachment_C:_Digital)
* [Attachment D – Digital ID (Accreditation) Data Standards feedback](#_Attachment_D:_Digital)

# Your details

|  |  |
| --- | --- |
| **Organisation or agency Name** |  |
| **Contact email** |  |

# Attachment A: General comments

|  |  |  |
| --- | --- | --- |
| **Rules or Standards that the feedback relates to?** | **Rule/Section/Part no.** | **Your feedback** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Attachment B: Digital ID Rules feedback

| Rule | Amended since Sept 2023 | Explanation | Your feedback |
| --- | --- | --- | --- |
| Chapter 1—Preliminary | | | |
| 1.1 Name | No |  |  |
| 1.2 Commencement | Yes | Drafting simplified. |  |
| 1.3 Authority | Yes | Drafting clarified. |  |
| 1.4 Definitions | Yes | Updated to reflect other amendments; drafting simplified and clarified; new definitions (e.g., ‘material change’, ‘material effect’, ‘pairwise identifier’). |  |
| Chapter 2—Fit and proper person considerations | | | |
| 2.1 Application of this Chapter | N/a | New application provision. |  |
| 2.2 Mandatory relevant matters | Yes | Formerly rule 5; paragraph (c) amended to add new s 52(1A)(ba) of the Privacy Act; paragraph (f) amended to clarify references to external dispute resolution schemes; new paragraphs (1)(g) (whether prior application for accreditation was refused) and (j) (whether approval to participate is or has been suspended or revoked). |  |
| Chapter 3—Participation in the Australian Government Digital ID System | | | |
| Part 1—Applications for approval to participate | | | |
| 3.1 Application of this Part | N/a | New application provision. |  |
| 3.2 Applications for approval to participate—all entities | Yes | Formerly rule 6; process and drafting clarified. |  |
| Consultation question for Rule 3.3 – The requirements included in this rule 3.3 are based on existing requirements applicable to Government entities seeking to onboard to the Australian Government Digital ID System. They are designed to ensure that the System Administrator and the government relying parties reach an agreement prior to onboarding on how different types of incidents relating to the AGDIS are managed, so that if an incident occurs these can be resolved effectively. We are seeking feedback on how to achieve this coordinated response in future phases of the AGDIS rollout, where non-Government organisations who may not have large fraud and security teams may find these requirements difficult to meet.  How would you consider clarifying these rules for non-government organisations while still maintaining strong minimum security and fraud protections for individuals who may use their digital ID to access that relying party service? | | |  |
| 3.3 Applications for approval to participate—relying parties | Yes | Formerly rule 7; process and drafting clarified; requirement for continuity procedures for critical functions of its information technology system omitted |  |
| Part 2—Approval to participate | | | |
| 3.4 Conditions on approval to participate | Yes | Formerly rule 8; item 1 (notification of change of contact details timeframe reduced from 28 to 7 days).  New conditions: item 2 (participating relying parties to report proposed changes to IT systems and outages to the System Administrator); item 3 (participating relying parties to collect and store the pairwise identifier); item 4 (participating relying parties to notify the digital ID Regulator regarding ‘reporting entity’ status under AML/CTF laws); item 5 (participating relying parties may collect/disclose certain restricted attributes for the purpose of complying with AML/CTF obligations); item 6 (accredited identity service providers may collect/disclose certain restricted attributes for the purpose of participating relying parties to comply with their AML/CTF obligations); item 7 (IP rights warranty condition for accredited entities to complement rule 3.5). |  |
| Part 3—Statutory contract | | | |
| 3.5 Intellectual property rights | Yes | Formerly rule 9; redrafted. |  |
| Chapter 4—Reportable incidents | | | |
| 4.1 Application of this Chapter | N/a | New application provision. |  |
| Consultation question for rule 4.2 – This rule is based on reporting requirements that are currently used in the Australian Government Digital ID System. Do you have any suggested changes to this rule supporting the relevant regulator in accessing the necessary information to undertake investigations into cyber security or fraud incidents that could occur within the Australian Government Digital ID System? | | |  |
| 4.2 Cyber security incidents and digital ID fraud incidents | Yes | Formerly rules 12 and 13; incident reportable to System Administrator; former paragraph (4)(f) omitted; drafting clarified (including to refer to law enforcement agency and pairwise identifier). |  |
| 4.3 Changes in control of corporations | Yes | Drafting clarified, including to replace ‘proposed change’ with ‘future change’ in control and permit Commonwealth, State and Territory governments to change control of their corporations within their government structures without notifying the Digital ID Regulator. |  |
| 4.4 Change in contractor | Yes | Drafting clarified; new exception to reporting a change in contractor within 28 days before an engagement is proposed to start where it is necessary to manage a material change in circumstances (so long as the engagement and material change in circumstances are reported under rule 4.5). |  |
| 4.5 Other incidents | Yes | Drafting clarified; new requirement for accredited entities to report proposed changes to IT systems and outages to the System Administrator. |  |
| 4.6 Other digital ID systems | Yes | Drafting clarified; paragraph 3(g) amended to require information held by the entity for the purposes of the Australian Government Digital ID System to be located and distinguished from other digital ID system information. |  |
| 4.7 System Administrator may disclose information | Yes | Formerly rule 19; redrafted consistent with other amendments including change from Digital ID Regulator to System Administrator; notes inserted to clarify Digital ID Regulator and System Administrator functions are not limited. |  |
| Chapter 5—Trustmarks | | | |
| 5.1 Application of this Chapter | N/a | New application provision. |  |
| 5.2 Digital ID trustmark | Yes | Drafting simplified and clarified. |  |
| 5.3 Conditions in relation to use or display of digital ID trustmark | N/a | New rule prescribing conditions in relation to use or display of digital ID trustmark. |  |
| Chapter 6—Record-keeping | | | |
| Consultation question for rule 6.2 – The record keeping provisions required for the logging of information in relation to Australian Government Digital ID System transactions and other system information required by rule 6.2 in the proposed Digital ID Rules has been amended to 6 years. This is different from the proposed Accreditation Rules requirement for logging the same information under rule 4.20. Rule 4.20 in the proposed Accreditation Rules maintains that logs required for that rule are required to be kept for 3 years.   * Is 6 years an appropriate timeframe to retain the logging and transaction information required by rule 6.2 in the proposed Digital ID Rules in relation to transactions and personal information on the Australian Government Digital ID System? * What do you consider an appropriate minimum timeframe for the retention of this type of information?   Note: other kinds of personal information such as an individual’s name or restricted attributes collected for the purpose of a Digital ID are not required to be kept under the logging requirements in rule 4.20 of the proposed Accreditation Rules. | | |  |
| 6.1 Application of this Chapter | N/a | New application provision. |  |
| 6.2 Record keeping requirements for accredited entities | Yes | Formerly rule 22; drafting simplified; record-keeping requirement standardised from 7/3 years to 6 years; additional requirement to not destroy/de-identify personal information in specified circumstances. |  |
| Chapter 7—Interim liability arrangements | | | |
| Consultation question for Chapter 7 – The interim liability arrangements in Chapter 7 are prescribed for the initial phases of the Australian Government Digital ID System, where participants are Australian or state and territory government entities.  The liability arrangements in the proposed Digital ID Rules will be reviewed prior to the expansion of the Australian Government Digital ID System to the private sector.   * What kinds of liability arrangements would your organisation expect to see operational on Australian Government Digital ID System? * Are there any existing liability frameworks that the Digital ID Rules could draw from? | | |  |
| 7.1 Simplified outline of this Chapter | N/a | New outline provision confirming interim liability arrangements for commencement phase of the legislated Australian Government Digital ID System. |  |
| 7.2 Breaches of the statutory contract | N/a | New interim rule prescribing conduct that does not, and circumstances that do not, constitute a breach of the statutory contract. |  |
| 7.3 Limits on the kinds of losses or damages and amount of compensation | N/a | New interim rule limiting kinds of losses or damages, and limiting amount of compensation, in relation to non-compliance with the statutory contract. |  |

# Attachment C: Digital ID (Accreditation) Rules feedback

| Rule | Amended since Sept 2023 | Explanation | Your feedback |
| --- | --- | --- | --- |
| General questions – Accreditation Rules and data retention periods for personal information:  Retention of personal information collected from an individual is managed through an accredited entity’s own policies and requirements of its services as well as its tolerance for security and fraud risks associated with the retention of that information (e.g. the longer it is retained, the more at risk that information may be of being breached).   * Should the Accreditation Rules set out a maximum data retention period for an individual’s personal information? For example, that an accredited entity must delete personal information after a period of time if an account becomes dormant. What should that period of time be? | | |  |
| General questions – Accreditation Rules and barriers to entry for the accreditation scheme:  The Accreditation Rules are a set of minimum controls that are designed to address Digital ID specific risks to individuals and relying parties. Some previous feedback has indicated that because of the technical nature and complexity of the Accreditation Rules and Accreditation Data Standards, that there is a high cost of entry to the accreditation scheme due to the kinds of controls accredited entities are expected to implement.   * If the Accreditation Rules were to be simplified, which rules would you suggest be removed?   + If you are suggesting removal of a rule, how would you recommend mitigating the risk that rule was designed to address? * Are there any other standards that are not already incorporated into the rules that you suggest should be considered? | | |  |
| Chapter 1—Preliminary | | | |
| 1.1 Name | No |  |  |
| 1.2 Commencement | No |  |  |
| 1.3 Authority | No |  |  |
| 1.4 Definitions | Yes | Clarification of various definitions. |  |
| 1.5 Incorporated instruments | Yes | Addition of (b) to ensure that legislative instruments such as the Accreditation Data Standards are not captured by this requirement. |  |
| 1.6 Taking reasonable steps | No |  |  |
| Chapter 2—Applying for accreditation | | | |
| 2.1 DI data environment | Yes | Minor clarifications to ensure that references to contracted service providers are consistent. |  |
| 2.2 Documents to accompany application | Yes | New – This requirement is to support annual review requirements for the documents mentioned in the rule. All other documentation required for accreditation will be set out in the application for accreditation form required under section 141 of the Digital ID Bill. |  |
| 2.3 Criteria to be met | No |  |  |
| 2.4 Privacy impact assessment | Yes | Minor clarification to capture Chapter 5 rules as part of the PIA. |  |
| 2.5 Technical Testing | Yes | Addition of data minimisation mechanism to be tested (see rule 4.42 (2)). |  |
| 2.6 Matters to which the Digital ID Regulator must have regard | No |  |  |
| 2.7 Matters to which the Digital ID Regulator must be satisfied | No |  |  |
| Chapter 3—Assurance assessments and systems testing | | | |
| Part 3.1—General | | | |
| 3.1 Entity’s obligation | No | No |  |
| 3.2 Assessors | No | No |  |
| Part 3.2—Assurance assessments | | | |
| Division 1—Protective security assessment | | | |
| 3.3 Requirements | Yes | Minor drafting clarifications |  |
| 3.4 Essential strategies review and report | No |  |  |
| 3.5 Where a control is not relevant to an entity | Yes | Minor drafting clarifications |  |
| Division 2—Fraud assessment | | | |
| 3.6 Requirement | No |  |  |
| Division 3—Accessibility and useability assessment | | | |
| 3.7 Requirements | No |  |  |
| Part 3.3—Systems testing | | | |
| Division 1—Penetration testing | | | |
| Consultation Question for Rule 3.8 – The penetration testing rule has been updated to better clarify the scope and requirements of a penetration test, including what is required to be tested and what kind of testing must be included in a penetration test. Do you have any feedback regarding this requirement? | | |  |
| 3.8 Penetration testing requirements | Yes | Requirements have been added to better clarify what the scope of the penetration testing must include as well as what the penetration testing applies to in the accredited entity’s information technology system. New requirements to clarify penetration testing requirements where an accredited entity uses a cloud service provider. |  |
| 3.9 Penetration testing assessor | No |  |  |
| 3.10 Penetration testing report | No |  |  |
| Division 2—Useability testing | | | |
| 3.11 Accessible and inclusive services | Yes | Minor drafting clarification to align with section 30 of the Digital ID Bill and rules that were updated in Part 4.4 in the Accreditation Rules. |  |
| 3.12 Useability testing requirements | Yes | Minor drafting clarification to align with section 30 of the Digital ID Bill and rules that were updated in Part 4.4 in the Accreditation Rules. |  |
| 3.13 Useability testing report | No |  |  |
| Division 3—WCAG testing | | | |
| 3.14 Accessible and inclusive services | Yes | Minor drafting clarification to align with section 30 of the Digital ID Bill and rules that were updated in Part 4.4 in the Accreditation Rules. |  |
| 3.15 WCAG testing requirements | Yes | Minor drafting clarification to align with section 30 of the Digital ID Bill and rules that were updated in Part 4.4 in the Accreditation Rules. |  |
| 3.16 WCAG testing report | No |  |  |
| Part 3.4—Reports | | | |
| 3.17 Assessor’s report | No |  |  |
| 3.18 Entity’s response to an assessor’s report | No |  |  |
| Chapter 4—Requirements for maintaining accreditation | | | |
| Part 4.1—Protective security controls | | | |
| Division 1—Capability | | | |
| 4.1 Protective security capability | No |  |  |
| Division 2—Protective security frameworks | | | |
| 4.2 Accredited entities must implement a security framework | Yes | Minor drafting clarification to address structure and clarity of interpretation |  |
| 4.3 Compliance with the PSPF | Yes | Minor drafting clarification to address structure and clarity of interpretation |  |
| 4.4 Compliance with ISO/IEC 27001 | Yes | Minor drafting clarification to address structure and clarity of interpretation |  |
| 4.5 Implementation and compliance with an alternative framework | Yes | Minor drafting clarification. Guide note: this rule is in the wrong place and will be moved to Division 2 (above) prior to public consultation. |  |
| 4.6 Where a control is not relevant to an entity | Yes | Minor drafting clarification to address structure and clarity of interpretation |  |
| Division 3—Additional protective security controls | | | |
| 4.7 Cyber security risk assessment | No |  |  |
| 4.8 Sharing information about risks | No |  |  |
| 4.9 Eligibility and suitability of personnel | No |  |  |
| 4.10 Advice to individuals | Yes | Requirement changed to implement consultation feedback. Adopted the use of "serious harm" to align with Privacy Act and OAIC advice wording and requirement now ensures that entities must "promptly" inform individuals of the risk or incident. |  |
| 4.11 Support to individuals | No |  |  |
| Subdivision 1—System security plan | | | |
| 4.12 Requirement | Yes | Now includes security goals and strategic objectives and addition of requirements for entities to record their biometric information destruction process (TDIF requirements that were not in the September 2023 draft Accreditation Rules). |  |
| 4.13 Review of the system security plan | Yes | Now includes review of security goals and strategic objectives. |  |
| Subdivision 2—Cloud service management | | | |
| 4.14 Selection, use and management of cloud services | No |  |  |
| Subdivision 3—Incident detection, investigation, response and reporting | | | |
| 4.15 Incident monitoring and detection | No |  |  |
| 4.16 Incident investigation, management and response | No |  |  |
| 4.17 Disaster recovery and business continuity management | No |  |  |
| 4.18 Record keeping | Yes | Minor adjustments to improve clarity. |  |
| Subdivision 4—Information technology system controls | | |  |
| 4.19 Essential Eight | No |  |  |
| 4.20 Logging requirements | Yes | Minor adjustments to improve clarity. Requirements for logging consent explicitly included (previous TDIF requirement that was not in the September 2023 draft Accreditation Rules). |  |
| 4.21 Cryptography | No |  |  |
| 4.22 Cryptographic standards | No |  |  |
| 4.23 Cryptographic key management processes and procedures | No |  |  |
| Part 4.2—Fraud control requirements | | | |
| Division 1—Capability | | | |
| 4.24 Fraud management capability | No |  |  |
| Division 2—Fraud controls | | | |
| 4.25 Fraud risk assessment | No |  |  |
| 4.26 Sharing information about risks | No |  |  |
| 4.27 Fraud controller | No |  |  |
| 4.28 Fraud awareness training | No |  |  |
| 4.29 Advice to individuals | Yes | Requirement adjusted to address consultation feedback. Adopted the use of "serious harm" to align with Privacy Act and OAIC advice wording and requirement now ensures that entities must "promptly" inform individuals of the risk or incident. |  |
| 4.30 Support to individuals | No |  |  |
| Division 3—Fraud control plan | | | |
| 4.31 Fraud control plan | Yes | Minor adjustments to improve clarity |  |
| 4.32 Review of entity’s fraud control plan | No |  |  |
| Division 4—Incident detection, investigation, response and reporting | | | |
| 4.33 Incident monitoring and detection | No |  |  |
| 4.34 Incident investigation, management and response | No |  |  |
| 4.35 Record keeping | No |  |  |
| Part 4.3—Privacy | | | |
| 4.36 Privacy governance code | No |  |  |
| 4.37 Compliance with privacy governance code | No |  |  |
| 4.38 Privacy policy | No |  |  |
| 4.39 Review | No |  |  |
| 4.40 Providing information about express consent | Yes | Requirement included to address feedback about the intersection of privacy and usability. This requirement was previously a TDIF requirement that was not in the draft September 2023 Accreditation Rules |  |
| Consultation question for Rule 4.41 – Some feedback has indicated that the rules should not set a timeframe for enduring consent to expire and instead allow accredited entities to set their own policies for the expiry of enduring consent dependent on the service that is being provided. Do you think the rules should set a timeframe for enduring consent to expire? What should that timeframe be? | | |  |
| 4.41 Enduring consent | Yes | New. Added to address consultation feedback noting the gap in assurance about the timing and duration of consent. Wording and policy for the duration period aligns with similar CDR provisions. Supporting requirements for enduring consent related to usability and accessibility have been added. These requirements were previously in the TDIF but were not in the draft September 2023 Accreditation Rules |  |
| 4.42 Data minimisation principle | Yes | Major change. Consultation feedback indicated the data minimisation principle was overly burdensome in regulating what kind of data relying parties required. The requirement has been amended to now ensure accredited entities can allow relying parties to select only the information they require to offer their services (e.g., a surname only instead of a bundle of first name, middle name, and surname). |  |
| 4.43 Use of DVS and FVS for providing accredited services | Yes | New. Included to ensure alignment and legality of use of the DVS and FVS. |  |
| 4.44 Disclosure of personal information for fraud activities | No |  |  |
| 4.45 Privacy awareness training | No |  |  |
| 4.46 Data breach response plan | No |  |  |
| 4.47 Record keeping | No |  |  |
| Part 4.4—Accessible and inclusive accredited services | | | |
| 4.48 Application | Yes | Aligned with Digital ID Act provisions. |  |
| 4.49 Reporting on accessibility | Yes | New. Requirement added to ensure alignment with section 30 of the Digital ID Act and address consultation feedback encouraging the use of inclusion strategies and goals for accredited entities. |  |
| 4.50 Accessibility requirements | Yes | Requirement wording has been adjusted to ensure alignment with section 30 of the Digital ID Act. |  |
| 4.51 Journey map | Yes | Minor clarifications to address consultation feedback and to fold the journey map into the usability testing rules to better scope usability testing. |  |
| Part 4.5—Retention and use of biometric information for testing and fraud activities | | | |
| 4.52 Requirements where biometric information is used for testing activities | Yes | Changes made to align with Section 49 (6A) and (7) of the Digital ID Act and to address consultation feedback. Additionally, changes to testing requirements include that accredited entities must only carry out testing of biometric information where the testing is unable to be conducted effectively by processing synthetic or anonymised data rather than by using biometric information of an individual. This aligns to international best-practice standards and requirements when using biometric information for secondary purposes. |  |
| 4.53 Requirements where biometric information is used for fraud activities | No |  |  |
| Part 4.6—Review of DI data environment and statement of scope and applicability | | | |
| 4.54 DI data environment | Yes | New – requirement added to support the structure of the Accreditation Rules and annual review requirements for these documents in Chapter 6. |  |
| 4.55 Statement of scope and applicability | Yes | New – requirement added to support the structure of the Accreditation Rules annual review requirements for these documents in Chapter 6. |  |
| Part 4.6—Review of DI data environment and statement of scope and applicability | | | |
| Chapter 5—Requirements when providing accredited services | | | |
| Part 5.1—Preliminary | | | |
| 5.1 Definitions | Yes | Majority of definitions moved to Chapter 1 of the Rules or into the Accreditation Data Standards where appropriate |  |
| Part 5.2—Accredited identity service providers | | | |
| Division 1—Generating, managing, maintaining or verifying a digital ID | | | |
| 5.2 General requirements | Yes | Yes. The rule has been rewritten for clarity and scope of ISP services to address consultation feedback. |  |
| 5.3 Digital IDs and children | Yes | The age an individual can get a digital ID will remain at 15 years old to align with OAIC guidance regarding the age that individuals have the capacity to give express consent. Additionally, a new subrule was added to address IP1 services that cannot effectively verify an individual's age because an individual is not required to present any documents for verification at IP1. |  |
| 5.4 One-off digital IDs | No |  |  |
| 5.5 Expiry of a reusable digital ID | Yes | Amended for clarity. |  |
| 5.6 Step-up of an identity proofing level | Yes | Amended for clarity. |  |
| 5.7 Updating and correcting attributes | Yes | Amended for clarity. |  |
| 5.8 Suspension of a digital ID | Yes | Amended for clarity. |  |
| 5.9 Digital IDs affected by a fraud or cyber security incident | Yes | Amended for clarity. |  |
| 5.10 Reactivating a suspended digital ID | Yes | Amended for clarity. |  |
| Division 2—Identity proofing and verification of credentials | | | |
| Subdivision A—Identity proofing | | | |
| 5.11 IP Levels Table | Yes | Amended for clarity. |  |
| 5.12 Verification using an Australian passport or Australian ePassport | Yes | Amended for clarity. |  |
| 5.13 Technical verification of credentials | Yes | This requirement has been amended to be scoped only to ePassport verification. This is because ePassports have a clear standard and way to be verified using Public Key Infrastructure technology and issued by the Internation Civil Aviation Organization (ICAO). As new standards and issuance processes for other kinds of credentials emerge, this rule will be updated. |  |
| 5.14 Source verification using a government credential | Yes | Minor amendments and drafting clarification. |  |
| 5.15 Visual verification | Yes | Minor amendments and drafting clarification to align with feedback and amendments made to Schedules 1-4. |  |
| Subdivision B—Verification using biometric information | | | |
| 5.16 Application | No |  |  |
| 5.17 Requirements for biometric binding | No |  |  |
| 5.18 Requirements for online biometric binding | Yes | Minor drafting clarification. |  |
| 5.19 Requirements for local biometric binding | Yes | Minor clarification to address consultation feedback. |  |
| 5.20 Requirements for technical biometric matching | No |  |  |
| 5.21 eIDVT biometric matching | Yes | Moved some requirements from the previous eIDVT testing rules to here as they structurally belonged in this section. The eIDVT testing requirements are now located in the Accreditation Data Standards. |  |
| 5.22 Requirements for manual face comparison | No |  |  |
| Subdivision C—Alternative proofing processes | | |  |
| 5.23 Accessible and inclusive services | No |  |  |
| 5.24 Exceptional use case | No |  |  |
| 5.25 Requirements for an alternative proofing process | Yes | Minor drafting clarification. |  |
| Division 3—Generating, binding, managing or distributing authenticators | | | |
| 5.26 General requirements | Yes | Amended for clarity. Note that any other requirements related to authenticators are located in the Accreditation Data Standards. |  |
| 5.27 Physical authenticators | Yes | Amended for clarity. Note that any other requirements related to authenticators are located in the Accreditation Data Standards. |  |
| 5.28 Authenticator that has been compromised | Yes | Amended for clarity. Note that any other requirements related to authenticators are located in the Accreditation Data Standards. |  |
| 5.29 Step-up of an authentication level | Yes | Amended for clarity. Note that any other requirements related to authenticators are located in the Accreditation Data Standards. |  |
| 5.30 Expired and renewed authenticators | Yes | Amended for clarity. Note that any other requirements related to authenticators are located in the Accreditation Data Standards. |  |
| 5.31 Revocation and termination of an authenticator | Yes | Amended for clarity. Note that any other requirements related to authenticators are located in the Accreditation Data Standards. |  |
| Division 4—Accessibility and useability | | | |
| 5.32 Application | No |  |  |
| 5.33 Verification services | No |  |  |
| 5.34 Authentication services | No |  |  |
| Part 5.4—Accredited attribute service providers | | | |
| 5.35 Verifying and managing a special attribute | Yes | Amended to address consultation feedback and Digital ID policy about the scope of an ASP service. |  |
| 5.36 Requirements when verifying a special attribute | Yes | Amended to address consultation feedback and Digital ID policy about the scope of an ASP service. |  |
| 5.37 Special attributes that are self-asserted | Yes | Amended to address consultation feedback and Digital ID policy about the scope of an ASP service. |  |
| 5.38 Special attributes affected by a fraud or cyber security incident | Yes | Amended to address consultation feedback and Digital ID policy about the scope of an ASP service. |  |
| Chapter 6—Annual reviews | | | |
| Part 6.1— Accredited entities to conduct annual reviews | | | |
| 6.1 General requirements | Yes | Minor amendment to address consultation feedback by allowing entities an additional month past the anniversary of their accreditation date to submit their annual review report and supporting evidence. |  |
| 6.2 Reporting periods for transitioned accredited entities | Yes | New. Required for entities transitioning their accreditation from TDIF to the legislation. This table will completed post-consultation. |  |
| 6.3 Reporting periods for other accredited entities | Yes | New. Required for entities that will be accredited under the legislation. |  |
| 6.4 Scope of annual review | Yes | Minor clarifications to include notes about the privacy impact assessment (PIA) and other drafting clarifications. |  |
| 6.5 Assurance assessments | No |  |  |
| 6.6 Penetration and presentation attack detection testing | No |  |  |
| Part 6.2— Accredited entities to provide annual reports | | | |
| 6.7 Content of report | No |  |  |
| 6.8 Where previous timeframes to address risks and recommendations not met | Yes | Minor clarification to include PIA in this rule. |  |
| 6.9 Information and documents | No |  |  |
| 6.10 Attestation statement | No |  |  |
| Chapter 7—Other matters relating to accreditation | | | |
| Part 7.1—Matters related to attributes | | | |
| 7.1 Individuals must expressly consent to disclosure of certain attributes of individuals to relying parties | Yes | New. Requirement included to ensure accredited entities collect express consent for attributes that are not covered in section 45 of the Digital ID Act. |  |
| 7.2 Meaning of *restricted attribute* of an individual | Yes | New. Requirement included ensure that card numbers are included as a restricted attribute. |  |
| Part 7.2—Accreditation conditions | | | |
| 7.3 Table of accreditation conditions | Yes | New. Included to align with Digital ID Act requirements for accreditation of entities. |  |
| Part 7.3—Reportable incidents | | | |
| 7.4 General | No |  |  |
| 7.5 Reportable incidents | No |  |  |
| 7.6 Change of control for corporations | No |  |  |
| 7.7 Entity no longer providing accredited services | Yes | New requirement to address gap in reporting information to the Regulator. |  |
| Part 7.4—Data standards relating to accreditation | | | |
| 7.8 Digital ID Data Standards Chair to make standards | Yes | New. Included to accommodate the Accreditation Data Standards (see below). |  |
| Schedules | | | |
| Schedule 1— Documents or other credentials that are a commencement of identity credential | Yes | Minor changes to support changes to verification rules and supporting requirements. |  |
| Schedule 2—Documents or other credentials that are a linking credential | Yes | Minor changes to support changes to verification rules and supporting requirements. |  |
| Schedule 3—Documents or other credentials that are a UitC credential | Yes | Minor changes to support changes to verification rules and supporting requirements. |  |
| Schedule 4—Documents or other credentials that are a photo ID | Yes | Minor changes to support changes to verification rules and supporting requirements. |  |
| Schedule 5—PSPF controls | No | This schedule will be consolidated with any updates of the PSPF published prior to commencement. |  |

# Attachment D: Digital ID (Accreditation) Data Standards

| Standard | Amended since Sept 2023 | Explanation | Your feedback |
| --- | --- | --- | --- |
| Chapter 1 —Preliminary | | |  |
| 1 Name | NA |  |  |
| 2 Commencement | NA |  |  |
| 3 Authority | NA |  |  |
| 4 Schedules | NA |  |  |
| 5 Definitions | Yes | Clarification of various definitions to align with the Accreditation Rules |  |
| Schedule 1—Data standards for accredited identity service providers | | |  |
| Part 1—Biometric testing | | |  |
| 1.1 Definitions | Yes | Minor clarifications |  |
| 1.2 Biometric testing entity | Yes | Minor clarification to rule 1.2(1)(b) to ensure that the laboratory certified by ISO/IEC 17025 includes that the certification is for the assessment of biometric technology testing standards. |  |
| 1.3 Testing of presentation attack detection technology | Yes | Minor clarifications to allow an accredited entity to have a minor failure in the PAD testing (as opposed to meeting a 0% failure rate) and address that failure through implementing a treatment or recommendation. |  |
| 1.4 ISP’s response to testing report | Yes | New. Added to support changes to section 1.3 and address feedback related to PAD testing metrics and outcomes for rule 5.28 (7) in draft September 2023 Accreditation Rules |  |
| 1.5 Testing of biometric matching algorithm for technical biometric matching | No |  |  |
| 1.6 Testing of source biometric matching | Yes | Minor drafting clarifications |  |
| 1.7 Testing of eIDVT | Yes | Some rules were moved from the testing section to the eIDVT rules in the Accreditation Rules as they related to configuration settings and requirements for eIDVT rather than testing requirements. |  |
| Part 2—Authenticating to a digital ID | | |  |
| Division 1—Authentication levels |  |  |  |
| 2.1 Authentication levels: AL Table | Yes | Minor drafting clarifications for table readability. Amendments to item 2 Reauthentication requirements have been made for readability and alignment with NIST 800-63b. |  |
| Division 2—Binding authenticators to a digital ID |  |  |  |
| 2.2 Binding an authenticator when generating a digital ID | No |  |  |
| Division 3—Standards for kinds of authenticators | | |  |
| 2.3 Memorised secrets | Yes | Minor drafting clarifications |  |
| 2.4 Look-up secrets | Yes | Minor drafting clarifications |  |
| 2.5 Single-factor one-time password devices | Yes | Minor drafting clarifications |  |
| 2.6 Multi-factor one-time password devices | Yes | Minor drafting clarifications |  |
| 2.7 Single-factor cryptographic software | Yes | Minor drafting clarifications |  |
| 2.8 Multi-factor cryptographic software | Yes | Minor drafting clarifications |  |
| 2.9 Multi-factor cryptographic devices | Yes | Minor drafting clarifications |  |
| 2.10 Single-factor cryptographic devices | Yes | Minor drafting clarifications |  |
| 2.11 Out-of-band devices | Yes | Additional requirements added for out-of-band devices that use the PSTN to address security concerns. These requirements align to the NIST 800-63b framework. |  |
| Division 4—Standards for security requirements | | |  |
| 2.12 Standards for security requirements | No |  |  |
| Division 5—Authentication using biometric information | | |  |
| 2.13 Standards for authentication using biometric information | Yes | Changes made to in-device biometric capability requirements—requirement to record in-device capability risks in the fraud control plan have been moved to the fraud control plan rules in the Accreditation Rules (see rule 4.31) |  |