Australian Government
Digital Transformation Agency

Stakeholder and community feedback

Trusted Digital Identity Framework

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (http://www.itsanhonour.gov.au)

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties with accessing this document, or have questions or comments regarding this document please email the Director, Trusted Digital Identity Framework at identity@dta.gov.au.

Contents

1 Summary of changes

The Trusted Digital Identity Framework (TDIF) has been developed in conjunction with government agencies and the private sector. The DTA met regularly with stakeholders while drafting the TDIF which was then released for public consultation in November and December 2017.

Thank you to everyone who provided feedback. More than 1,000 comments were received. In this document we have summarised the broad changes made to the TDIF in response to this feedback.

There were a number of suggestions made which have resulted in changes to all of the documents that make up version 1.0 of the TDIF. These changes include the following:

- Duplication between the documents has been removed as much as practicable.
- Documents have been merged together where there was a logical reason to do so (e.g. risk requirements and risk guidance) which has reduced the number of TDIF documents from 14 to 10.
- All defined terms have been removed from documents and added to the *Overview and Glossary*.
- Inconsistencies that existed between defined terms have been resolved.
- The relationship and linkages section has been removed from each document and added to the *Overview and Glossary*.
- The document introductions have been tailored to the specific documents.
- All documents that were either '*Core Requirements'* documents or '*Standards'* have been retitled as '*Requirements'* documents. This change was needed to remove confusion between the TDIF document hierarchy and suggested reading order.
- Changes that have been made to individual documents are summarised below. The terms and definitions used in this document are defined in the *Trust Framework Overview and Glossary*.

1.1 Overview and Glossary

- Additional context of what a trust framework is has been added.

- A section to explain why the DTA is developing a trust framework and what benefits this will bring the public, government and stakeholders has been added.
- A conceptual model for the identity federation including descriptions of the various federation actors (e.g. Identity Service Provider, Exchange) has been provided.
- The TDIF schedule, including anticipated documents and content for subsequent releases has been added.
- The governance roles and responsibilities and the issues the governance body will be required to manage has been updated. (TDIF governance will be covered as part of TDIF release 2).
- The concept of 'Attribute Providers' which will be covered as part of TDIF release 3 has been added.

1.2 Accreditation Process

- Context about how long accreditation should take and why the TDIF does not specify timeframes has been added.
- Information about likely costs for Applicants undergoing accreditation has been added.
- The accreditation process now supports identity services being developed.
- The accreditation workflow now supports the iteration of activities.
- An annex which maps accreditation activities to TDIF documents has been added.

1.3 Authentication Credential Requirements

- Digital Authentication Credential Standard has been renamed Authentication Credential Requirements.
- Changes have been made to the description of each Authentication Credential Level (ACL) to better reflect the identity verification requirements per ACL.
- The document now aligns with National Institute of Standards and Technology (NIST)guidance regarding out-of-band device requirements.
- The requirement to change memorised secrets (e.g. a password) every 90 days is now subject to a risk assessment by the Relying Party.
- Credential levels and authentication factors now align with NIST.

- Phishing resistant factors are now required at CL3.
- Specific security requirements for some authentication credential types have been removed and replaced with references to the Australian Government Information Security Manual (ISM) for those credential types.

1.4 Fraud Control Requirements

- Core Fraud Control Requirements has been renamed Fraud Control Requirements.
- Fraud control requirements updated to apply to all Applicants.
- Fraud control examples added.
- The document now aligns to national fraud control standards.

1.5 Identity Proofing Standard

- Digital Identity Proofing Standard has been renamed Identity Proofing Requirements.
- The document has been updated to better align with the Council of Australian Governments National Identity Proofing Guidelines.

1.6 Protective Security Requirements

- Core Protective Security Requirements has been renamed Protective Security Requirements.
- The document formally known as Information Security Documentation Guide has been merged with the Protective Security Requirements.
- The Trust Framework Accreditation Authority position on information security waivers and the issues to be considered before waivers will be accepted has been explained.
- The document has been updated to reflect that protective security requirements apply equally to organisations or agencies seeking accreditation.
- The document has been updated to make it clear that only applicable UNCLASSIFIED ISM controls (i.e. those listed as ‘UD’ in the ISM) need to be implemented.

- All ISM statements have been removed. Applicable ISM controls now defined by their respective control numbers only.

1.7 Privacy Requirements

- The document Core Privacy Requirements has been renamed Privacy Requirements.
- The document formally titled Privacy Audit has been merged with the Privacy Requirements.
- The document now aligns with the Australian Government Agency Privacy Code for conducting Privacy Impact Assessments.
- Privacy Impact Assessments are now required where an Applicant identifies a high privacy risk.
- The Office of the Australian Information Commissioner (OAIC) has been removed as a stakeholder to whom data breaches are to be reported. This change was required as the OAIC may not be able to action some data breaches where the Applicant is not operating with the jurisdiction of the OAIC.
- The uses and disclosures section of the document now makes a distinction between verification events (i.e. where consent is required), direct marketing (not allowed) and other uses and disclosures (which must comply with the Privacy Act).
- The document now aligns with the Privacy Act 1988 in relation to access and correction.
- It is now clearer in the document that the Approved Assessor undertaking the privacy audit is required to be independent of the identity service under review.

1.8 Risk Management Requirements

- Core Risk Management Requirements has been renamed Risk Management Requirements.
- The previously titled Core Risk Management Requirements and Risk Management Guide together have been merged.
- The document now supports any internationally-recognised risk management methodology.

- Where possible, identity-specific context to the risk management guidance has been provided.
- Likelihood and consequence ratings have been collapsed into a 5x6 risk event matrix. The 'Significant' risk rating as these risks need the same management approaches as 'High' risks have been removed.

1.9 User Experience Requirements

- Core Usability and Accessibility Requirements has been renamed Usability and Accessibility Requirements.
- Some of the 'SHOULDs' have been changed to 'MUSTs'.
- The exemption from the contrast requirement of Web Content Accessibility Guideline (WCAG) 2.0 has been removed. The requirement changed to a 'SHOULD' which means an Applicant is required to justify why they don't comply with the requirement.

1.10 Protective Security Reviews

- IRAP Assessment has been renamed Protective Security Reviews.
- All ISM control numbers have been moved to Protective Security Requirements.
- The document now focuses on the IRAP process, rather than the controls that need to be tested.
- A placeholder section for the penetration testing requirements which will be developed as part of TDIF release 2 has been added.

2 Feedback under consideration

We have also received some suggestions that we are unable to address in this current version of the TDIF but will be considered for future versions. These include the following:

- Governance roles and responsibilities for the identity federation, including warranties, liability allocation and dispute resolution.
- How the TDIF manages the requirement to obtain user consent multiple times within the identity proofing process.
- The applicability of Transparency Reports to Identity Service Providers and Attribute Providers.
- The technical aspects of the TDIF, including data models, identity federation architecture and profiles for the use of Security Assertion Markup Language (SAML) and OpenID Connect.
- The TDIF vulnerability and penetration testing requirements.
- The TDIF annual audit requirements.
- Offline or alternative identity proofing processes.
- Complex identity proofing requirements where individuals do not have the required identity documents.
- Individuals operating with multiple yet legitimately acquired identities - marriages, change-of-name or gender.
- Managing identity proofing that may require completion offline i.e. in a shopfront or face to face.
- The appropriateness of using a Commencement of Identity document at identity proofing level 2 (IP2).
- Options to verify identity data with alternatives to Authoritative Sources.
- Greater detail on the implementation of biometric face-matching requirements and secondary assurance measures such as the social-footprint check.