Australian Government
Digital Transformation Agency

Stakeholder and community feedback

Trusted Digital Identity Framework (Component 2)

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 have difficulties 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. There have been two components of TDIF released, with the first being published in February 2018 and the second in August 2018. The second component includes a combination of new documents and updates to existing documents from the first TDIF component. Both components are available on the DTA website[1].

The DTA met regularly with stakeholders while drafting the second component of the TDIF which was then released for public consultation through May and June 2018.

Thank you to everyone who provided feedback. More than 900 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 the second release of the TDIF. These changes include the following:

- Moved the document conventions (how to interpret MUST, SHOULD, etc) to the inside cover of each document.
- Changed the document management section of each document to show the Trust Framework Accreditation Authority as the body who endorses the document.
- References to the Trust Framework have been replaced with TDIF.
- References to individuals, users, end users and subscribers have been replaced with person or people.

Changes that have been made to individual documents are summarised below.
The terms and definitions used in this document are defined in the *TDIF: Overview and Glossary*.

[1] Both TDIF components are available on the DTA website, https://www.dta.gov.au/what-we-do/policies-and-programs/identity/

1.1 Attribute Profile

- Core attributes have been separated from the attributes that describe validated contact details.
- The descriptions of core attributes have been updated. This includes noting that where a person has only one name, it should be recorded as the family name.
- Description of attribute sets has been updated to note that the attributes may be requested individually.
- Revised the terminology that describes the types of consent. Added the “Every Change” consent type to support the need for requiring consent whenever an attribute value is changed.
- Added additional timestamp attributes to the attribute sets to enable an Identity Exchange to detect a change in attributes so that the appropriate consent policy can be applied. All timestamps are in UTC format.
- Clarified the use of different OIDC scopes for Relying Parties and Identity Providers, Relying Parties may also use the same OIDC scopes specified for Identity Providers.
- Added a paragraph describing support for computed attributes.
- Added examples of attributes that may be supported in the future releases.

1.2 Authentication Credential Requirements

- Complete re-write of the document to align with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63B
- Amended the wording to reflect consistency of terminology throughout the document.
- Updated Table 1 proof of possession requirements highlighting the alignment with NIST SP 800-63B requirements.
- Clarified Credential Service Provider specific requirements to remove ambiguity.

1.3 Fraud Control Requirements

- Terminology and reporting requirements have been clarified.
- Requirement for real-time fraud monitoring added.
- Fraud Risk Assessment now forms a component of the overall risk assessment.

1.4 Identity Proofing Requirements

- Inclusion of referee checks (attestation) for individuals without photo identity documentation.
- Expansion and clarification for IP4 (including in-person interviews).
- Introduced Transitional Arrangements that are a temporary alternative for identity proofing.
- Updated the list of allowable identity sources.
- Clarified and updated the Identity Service Provider requirements.
- Provided clarity around the objectives and their application within the identity proofing processes for each identity proofing level.
- Aligned terminology with the Glossary
- Re-ordered the document to improve readability

1.5 Interim Accreditation Governance

- Merged with the Interim Memorandum of Agreement

1.6 Interim Memorandum of Agreement

- The System Governance Interim MOU (MOU) consolidates the Federation Deed and MOU, and the Interim Accreditation Governance document, into one document. (The Federation Deed and MOU, and the Interim Accreditation Governance document, were each included in TDIF release two). This approach streamlines the governance arrangements for the System ('System Governance') during the roll-out of pilot services from October.
- The MOU provides for the DTA to act as an 'Oversight Authority' for the System and outlines the rights, powers and obligations of that Oversight Authority to ensure the safe, reliable and effective operation of the System. The TDIF MOU document previously referred to an 'Accreditation Authority', which was a body that had responsibility for accrediting participants within the System – the Oversight Authority has broader responsibility for administration and enforcement of arrangements for the System.

- The MOU sets out the roles and responsibilities of each participant within the System to ensure accountability and certainty within the System, and to ensure that use of the System is consistent with the requirements of the TDIF.
- The MOU is an interim arrangement which is designed to 'fall away' as the scope of the System expands and other non-Commonwealth participants seek to use the System (the MOU will be replaced by 'Operating Rules' in due course). In the meantime, it has flexibility for other Commonwealth entities to participate in the system (for example, as a Relying Party as new services are on-boarded).
- The MOU requires the Identity Exchange to maintain the privacy of the System through the 'double-blind' mechanism and the legal structure of this document (including the obligations of the participants) reflects the double blind technical architecture. The MOU also enshrines other privacy requirements – for example, the Oversight Authority must notify the Privacy Commissioner of proposed changes to the TDIF and invite comment on those changes.

1.7 Interim Federation Deed

- Merged with the Interim Memorandum of Agreement.

1.8 Overview and Glossary

- Provided greater clarity as what TDIF success will look like, including how success will be publicly reported.
- Redrafted the TDIF guiding principles to make them clearer.
- Added a description of 'double blind' in the objectives and how this will be achieved.
- Redrafted the sections about the functions performed by participants in the identity federation and how the relate to the various federation roles.
- Removed ambiguity about the number of identity exchanges that will operate in the identity federation over time (there will likely be several).
- Updated the section about the TDIF documents and development schedule. Moved this section closer to the front of the document and removed the pictures that showed the linkages between the TDIF policies as several people found these pictures confusing.

- Added a new section which describes how to interpret the document conventions (e.g. MUST, SHOULD, etc) and the impacts if these conventions are not followed.
- Added a new section which describes the initial accreditation process and the ongoing accreditation obligations.
- Introduced the concepts of the Oversight Authority and Operating Rules and added some of their roles and responsibilities.
- Added and updated a number of glossary terms that were missed from the first TDIF release.

1.9 OpenID Connect 1.0 Profile

- Corrections made to trust broker diagram and descriptions as requested.
- Corrections to examples as requested.
- Updated the diagram on Interactions (Appendix A) to highlight the interactions that are occurring via the user's web browser.
- Minor corrections and amendments identified in feedback.

1.10 Protective Security Reviews

- Minor changes have been made to a number of requirements to make them clearer.
- Provided additional information about the likely costs of an IRAP Assessment.
- Provided greater clarity regarding how failed IRAP Assessments will be handled by the Trust Framework Accreditation Authority.
- Removed references to the unclassified controls listed in the Australian Government Information Security Manual.
- Aligned the vulnerability management requirements with the *TDIF: Protective Security Requirements*.
- Added provisions to allow penetration testing to be conducted by internal teams.
- Added the definitions of 'black box' and 'white box' system testing to the *TDIF: Overview and Glossary*.

1.11 SAML 2.0 Profile

- Corrections to trust broker diagram and descriptions as requested, consistent with those included in the OIDC Profile.
- Updated diagram on Interactions (Appendix A) to highlight the interactions that are occurring via the user's web browser, consistent with those included in the OIDC Profile.
- Corrected section on "Common Profile Requirements" to clarify that a SAML Service Provider is only required to support either the Http-Redirect or Http-POST
- This profile requires support for the SAML metadata specifications to ensure support for static configuration of SAML requests. The relevant section will be revised to make this clearer in the next release.

1.12 Service Operations Requirements

- Clarification to include applicable outsourced services as part of Service Operations testing activities.
- Removed definitions specific to the document and added them to the *TDIF: Overview and Glossary*.

1.13 Technical Integration Testing Requirements

- Provided clarity regarding the scope of the Integration Testing to include demonstrating that the components of the system interface correctly and fulfil the functions specified for them.
- Included requirement for the Applicant to provide the Trust Framework Accreditation Authority with evidence that demonstrated achievement of the Technical Integration requirements.
- Removed definitions specific to the document and added them to the *TDIF: Overview and Glossary*.

2 Feedback under consideration

We have also received some suggestions that we are unable to address in this TDIF component 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.
- The TDIF annual audit requirements.
- How an individual can reuse a digital identity to act on behalf of a business.
- Details on the implementation of biometric face-matching requirements.
- Alignment with private sector requirement.