Australian Government

Digital Transformation Agency

Stakeholder and community feedback (component 3)

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 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 are three components of the TDIF. The first was published in February 2018, the second in August 2018 and the third due for release in April 2019. The third TDIF component includes a combination of new documents and updates to existing documents from the first and second components. All TDIF components are available on the DTA website[1].

The DTA met regularly with stakeholders while drafting the third component of the TDIF which was then released for public consultation through January and February 2019. Thank you to everyone who provided feedback. More than 230 comments were received. In this document we have summarised the broad changes made to the TDIF in response to this feedback.

A change that has been made to all TDIF documents is all references that were previously listed in individual TDIF documents have been moved to the *TDIF: Overview and Glossary*.

Changes that have been made to individual documents are summarised below.

1.1 Architecture Overview

- This is a new document.
- Added additional content to clarify boundaries of a Relying Party and the use of persistent pairwise identifiers.
- Corrected content included from *TDIF: Authentication Credential Requirements*.

1.2 Attribute Provider Requirements

- This is a new document.
- Use of common language terms open to misinterpretation removed

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

- Requirement to notify attribute holder and Relying Parties upon deactivation of attribute removed.
- Language for requirement to keep Attribute Provider database separate from other TDIF functions clarified.
- Reference to notifications to Relying Parties removed.

1.3 Technical Requirements

- This is a new document.
- Added guidance on use of persistent pairwise identifiers.

1.4 Accreditation Process

- Updated the requirements to be met by Applicants for initial accreditation.
- Added the ongoing accreditation and re-accreditation obligations for Accredited Providers.
- Added numerous appendixes which provide supplementary information for Applicants and Accredited Providers, including new requirements to be met when an Identity Service Provider or Attribute Provider providers services both within the TDIF federation and also outside it.

1.5 Attribute Profile

- Added attributes for other verified names that a person may have used.
- Added attributes to enable sharing of details of verified documents used in identity verification.
- Expanded section on Computed Attributes to note that they are synonymous with the term "*Attribute References*".

1.6 OpenID Connect 1.0 Profile

- Minor edits and corrections based on feedback.

1.7 Overview and Glossary

- Updated the section about the TDIF documents and development schedule.
- Updated the concepts of the Oversight Authority and Operating Rules and added their roles and responsibilities.
- Updated the glossary terms to include additional terms that were missed from previous TDIF components.
- Removed all references from TDIF documents and added them to section 6 of the Overview and Glossary.

1.8 Privacy Requirements

- Added a section on limitation of use and disclosure of behavioural information to Identity Service Providers so they do not use data collected from the services beyond providing and improving the service and detection and investigation of fraud.
- Streamlined consent section so not to duplicate common law requirements.
- Revision of overseas and contractor disclosure section so it better maps to APP 8.

1.9 Protective Security Requirements

- Updated the document to reflect the requirements in the recently released Australian Government Protective Security Policy Framework and Information Security Manual.
- Removed approximately 120 controls as part of the update.

1.10 Risk Management Requirements

- Removed the guidance section of the document (formally section 3). The Australian Government Protective Security Policy Framework has an excellent summary of how to plan for and manage risk within an agency or organisation[2].
- Removed approximately 180 requirements as part of the update.
- Changed two MUST requirements to objective statements.

1.11 SAML 2.0 Profile

- No changes occurred.

1.12 User Experience Requirements

- Added greater clarity for the reporting obligations for Applicants.
- Added requirements for Applicants to support multiple accessibility formats.

[22] See the PSPF *GOVSEC-3 Security planning and risk management* for further information.

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:

- Feedback on TDIF documents not part of this component (e.g. Identity Proofing Requirements, Fraud Control, Authentication Credential Requirements). All feedback on these documents has been saved and will be addressed as part of the next update.
- Governance roles and responsibilities for the identity federation, including warranties, liability allocation and dispute resolution.
- The commercial model that underpins the TDIF and identity federation.
- Requirements for biometric face-matching and presentation attack detection.
- Interactions between the identity federation and other initiatives (e.g. Open Banking, Consumer Data Right, etc).
- Interactions between the TDIFand other policy frameworks (e.g. Gatekeeper Public Key Infrastructure Framework and the National eAuthentication Framework).