Australian Government
Digital Transformation Agency

Overview and Glossary

Trusted Digital Identity Framework
February 2018, version 1.0

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

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.

Document Management

This document has been reviewed and endorsed by the following groups.

Endorsement

Group	Endorsement date
Director, Trusted Digital Identity Framework	Jan 2018
Commonwealth GovPass Design Authority	Feb 2018

Change log

Version	Date	Author	Description of the changes
0.01	Jul 2016	SJP	Initial version
0.02	Aug 2016	SJP	Minor updates and Alpha release
0.03	Jul 2017	DA & DR	Minor updates
0.04	Jan 2018	SJP	Major content review and feedback incorporated from stakeholders
1.0	Feb 2018		Endorsed by the Commonwealth GovPass Authority

Contents

1 Introduction

The Digital Transformation Agency (DTA), in collaboration with other government agencies and key private sector bodies, is leading the development of a national federated digital identity system (the ‘identity federation’). Implementation and operation of the identity federation is underpinned by the Trusted Digital Identity Framework (TDIF). This document provides a high-level overview of the TDIF including its scope and objectives, the relationship between its various documents and the definition of key terms.

The intended audience for this document includes:

- Accredited Providers.
- Applicants.
- Authorised Assessors.
- Relying Parties.
- Trust Framework Accreditation Authority.

2 Context

The United Nations Commission on International Trade Law (UNCITRAL[1]) has defined an identity system as follows:

“Identity system” means an online environment for identity management transactions governed by a set of system rules (also referred to as a trust framework) where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their identities. An identity system involves:

- A set of rules, methods, procedures and routines, technology, standards, policies and processes.
- Applicable to a group of participating entities.
- Governing the collection, verification, storage, exchange, authentication and reliance on identity attribute information about an individual person, legal entity, device or digital object.
- For the purpose of facilitating identity transactions.

Identity systems can be broadly characterised as either “Syndicated” or “Federated”. Under a syndicated system a single identity credential is issued, typically by government, to provide single sign-on access to public and private sector services. A federated system is a decentralised model enabling individuals to access public and private sector services through a choice of identity providers.

Traditional identity systems have often been based on a collection of bilateral agreements or loosely-coupled Service Level Agreements (SLAs). These frequently lack transparency and do not readily scale on a national basis. In contrast, a trust framework provides an efficient and scalable approach that readily facilitates the operation of a federated identity system.

A “trust framework” describes a legally binding and agreed set of specifications, rules, and agreements for the governance of a federated identity system established to achieve common outcomes among participants. Examples of federated identity systems that employ trust frameworks include electronic bill payment systems (such

[1] See *References* for further information on UNCITRAL

as BPAY or Post bill pay), electronic point of sale systems (such as EFTPOS) and credit card systems (such as MasterCard or Visa). Although these systems are functionally different, participants that operate within these environments share common characteristics, including the need for, and assurance that, other participants within the federated identity system follow the rules applicable to their role. A trust framework therefore enables participants to have confidence in the functionality and trustworthiness of federated identity systems.

3 Characteristics of a trust framework

The OIX[2] defines a trust framework as having the following characteristics:

Scope: a trust framework governs a specific federated identity system to enable the digital verification of an individual's identity, the binding of individuals to authentication credentials and the reuse of those credentials to access relying party's services.

Purpose: to define and govern the operation of a federated identity system and the obligations of its participants in order to ensure both the **functionality** and **trustworthiness** of the system. From a trustworthiness perspective a trust framework addresses:

- Functionality: the trust framework facilitates the functionality of the federated identity system it governs through the use of specifications, rules, and agreements designed to ensure that it operates properly in two respects:
    - Proper operation: it governs the federated identity system in a manner designed to ensure that the system functions properly for its intended purpose (so that it works).
    - Compliance: it is also designed to ensure that the system and its participants operate in accordance with legislative and regulatory requirements.
- Trustworthiness: the trust framework facilitates the trustworthiness of the federated identity system it governs through the use of specifications, rules, and agreements designed to ensure that it functions in a way that is sufficiently trustworthy to meet the needs of the participants (so the various parties are willing to participate). To that end:
    - Risk Management: it addresses and manages the various risks inherent in participating in the identity federation, and the requirements designed to address those risks.
    - Legal Certainty and Predictability: the legal rights, responsibilities, and liabilities of the participants, within broader legislative and regulatory requirements.
    - Transparency: the trust framework specifications, rules, and agreements are accessible to and agreed by all participants.

[2] See *References* for further information on OIX

- Content: The trust framework:
  - Defines Roles and Functions: the functions and operational roles needed to maintain the identity federation and the participant roles of those that engage in identity transactions within the federated identity system.
  - Addresses Key Issues: the specifications, rules, and agreements for the key business, technical, operational, and legal issues of importance for the governed identity federation to ensure both the functionality and trustworthiness of the system.
- Binding: the trust framework legally binds participating entities in the identity federation with role-specific sets of duties and liabilities. It is implemented and made legally binding on participating entities either by contract or legislation/regulation.

4 Trusted Digital Identity Framework

4.1 Meeting the Government's Financial System Inquiry commitment

The Australian Government established the Financial System Inquiry[3] ('the Inquiry') in 2013 to examine the positioning of the financial system to meet evolving needs and support economic growth for Australia. In 2014, the Inquiry concluded that a federated digital identity model would best meet cost, innovation, efficiency and flexibility requirements of the broader Australian digital economy. In accepting the recommendations of the Inquiry, the Australian Government agreed that a national digital identity strategy would streamline people's interactions with government and provide efficiency improvements. The Government also agreed to work with State and Territory jurisdictions and with the private sector to develop a Trusted Digital Identity Framework to support the Government's Digital Transformation Agenda.

The TDIF responds directly to the Inquiry and provides the rules for a federated digital identity system by which providers of identity services need to be accredited. The TDIF is being developed in consultation with government agencies and key private sector, privacy and consumer advocates by the Digital Transformation Agency.

The TDIF contains the tools, rules and accreditation criteria to govern the identity federation. It provides the required structure and controls to deliver confidence that all participants in the identity federation have met their accreditation obligations and as such may be considered trustworthy.

4.2 What success will look like

Successful implementation of the TDIF will be evident when people are able to simply and securely establish a digital identity through an identity provider of their choice, and safely reuse that identity to transact across all tiers of government and with the private sector, with their privacy assured. This will make it easy for people and

[3] See *References* for further information on the FSI

businesses in choosing their identity provider, as all providers will be required to independently demonstrate their compliance with the requirements of the TDIF.

Success will also be measured by the number of people that can complete the digital identity verification process to access services without the need to visit a shop front or call a help desk for support. A dashboard will be developed to report transparency on this, along with measuring user satisfaction.

Participants will judge the federated digital identity system by broad acceptance of the requirements and protocols established through the TDIF.

4.3 Guiding Principles

The TDIF will operate to the following principles:

User Centric:

- Accessing digital services must be easy, convenient and simple.
- Users can choose their digital identity and credential service providers from a range of accredited government and private sector providers.
- Users can choose to maintain multiple digital identities and credentials.
- Personal and business digital identities can be combined or kept separate.

Voluntary and Transparent:

- Users choose whether or not to participate.
- Users control their digital identities.
- Credential use records are accessible to users.

Service Delivery:

- Highly reputable identity and credential providers provide choice and convenience for users.
- Participation is cost effective for public and private sectors.

Privacy Enhancing:

- Personal information is collected, used and disclosed in accordance with privacy laws and good privacy practices.

- Privacy enhancing technology, policy and processes are applied to all personal information.
- Personal information is only collected with the consent of the user.
- Users have an informed understanding of how their personal information will be used and protected.

Collaborative:

- Active collaboration between the public and private sectors and the broader community will draw on the respective strengths and expertise of government and business and reflect the strengths and other characteristics of Australia’s federated identity system.

Interoperable:

- Develop robust policies and technologies which facilitate interconnectedness with other identity services nationally and internationally.
- Relevant standards, frameworks and common approaches are used wherever appropriate.

Innovative:

- Promote flexibility and innovation in technology and business models.
- The digital identity framework must be adaptable to ensure it can evolve in line with changing technology trends.
- The identity system is architected to support secure transactions across the digital economy, including transactions ranging from anonymous to fully authenticated and from low to high value.

Service Delivery:

- Highly reputable identity and credential providers provide choice and convenience for users.
- Participation is cost effective for public and private sectors.

Secure and Resilient:

- Apply minimum standards and accreditation and certification processes to identity providers, credential service providers and identity exchanges.
- Threats and risks are identified and actively managed for identity services.

4.4 Objectives

Based on the above principles, the TDIF will facilitate the following outcomes:

Simple:

- A digital end-to-end identity service that people want to use.

Accessible:

- Digital identity services that are accessible to all people regardless of their abilities or environment.

Secure:

- Digital identity services are security and privacy preserving.
- There is no single digital credential or centralised database of personal information.
- Users are given greater control of their personal information.

Standards based:

- Digital identity services are based on open standards to facilitate interoperability.

4.5 Roles and functions

The TDIF roles and functions can be grouped into two general categories:

- Operational functions, which relate to defining, governing and operating the identity federation.
- Participating functions, which relate to the participating entities within the identity federation.

4.5.1 Operational functions

The DTA will be responsible for developing and maintaining the TDIF, and amending it when changes are required or when new issues arise. The operational functions performed by the DTA in relation to the TDIF include:

- Governance and Policy Development: Developing and amending policies; decision making; stakeholder-facilitation; managing standards and procedures; accountability mechanisms.
- Policy Binding: Ensuring compliance with Trust Framework requirements; binding mechanisms; performing assessments or audits; managing policy changes and releases.
- Participating Entity Management: Administration and enrolment of participating entities; accreditation/on-boarding; support; dispute resolution.
- Network Evolvement: Growing and supporting the federated digital identity system; marketing; communication and strategy developing.
- Trust Framework Operations: Offering central services to the participating entities and/or public, e.g. information and discovery services.

4.5.2 Participating functions

The functions performed by participants within the federated digital identity system will include the following:

- Identity issuing: registration of identities and related attributes, issuing identity credentials, binding identities and credentials to end users.
- Identity verification: verifying identity information and credentials, proving or verifying additional attributes and assertions.
- Authentication management: requesting verification of attributes, claims and attributes, providing the results of verification.
- Authorisation management: managing user consent, managing identity verification and authentication policies.
- Attribute, claims, or assertion management: registration of attributes and credentials, binding attributes and credentials to identities, verification of claims based on registered attributes and credentials.

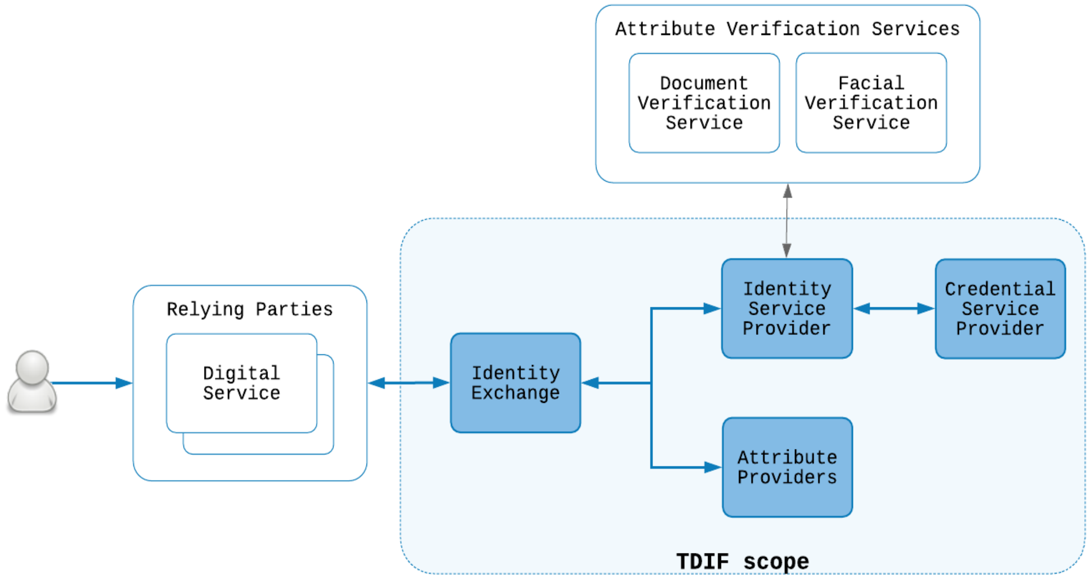
The TDIF accommodates the following roles to undertake these functions:

- Identity Service Providers undertake the function of verifying the identity of end-users.
- Credential Service Providers generate and manage authentication credentials which are provided to individuals. This function may be internalised within an IdP.

- Attribute Providers generate and manage attributes and claims which are provided to Relying Parties to support their decision-making process
- Identity Exchanges convey, manage and coordinate the flow of identity attributes, claims and assertions between members of the identity federation. The Identity Exchange will function in double-blind mode and must operate independently from all other participants within the identity federation.
- Relying Parties (also referred to as service providers) across both the public and private sectors.
- End users - initially individuals acting in their own capacity, but in time extended to business (a generic term for non-individual entities) and also to individuals acting on behalf of other individuals (authorisation)
- Attribute Verification Services - electronic means of verifying identity information against records held in the databases of government agencies.

Figure 1 below, outlines one instance of each role within the federated digital identity system, the scope of the TDIF and the roles to which it applies. The figure is merely to show how the roles relate to each other, and should not be interpreted as a complete model of the Australian federated digital identity system. The DTA envisages an identity federation that includes several Identity Service Providers, Credential Service Providers, Attribute Providers and Exchange Platforms operating across tiers of government and the private sector. Regardless of whether the participant is a government agency or commercial entity, if the participant operates within the TDIF scope it is required to achieve and maintain accreditation.

Figure 1: roles within the federated digital identity system


Attribute Verification Services
Document Verification Service
Facial Verification Service
Relying Parties
Digital Service
Identity Exchange
Identity Service Provider
Credential Service Provider
Attribute Providers
TDIF scope

4.6 Identity federation governance model

Central to the successful implementation of the federated digital identity system is an effective and representative governance model. Figure 2 below, outlines the proposed identity federation governance model.

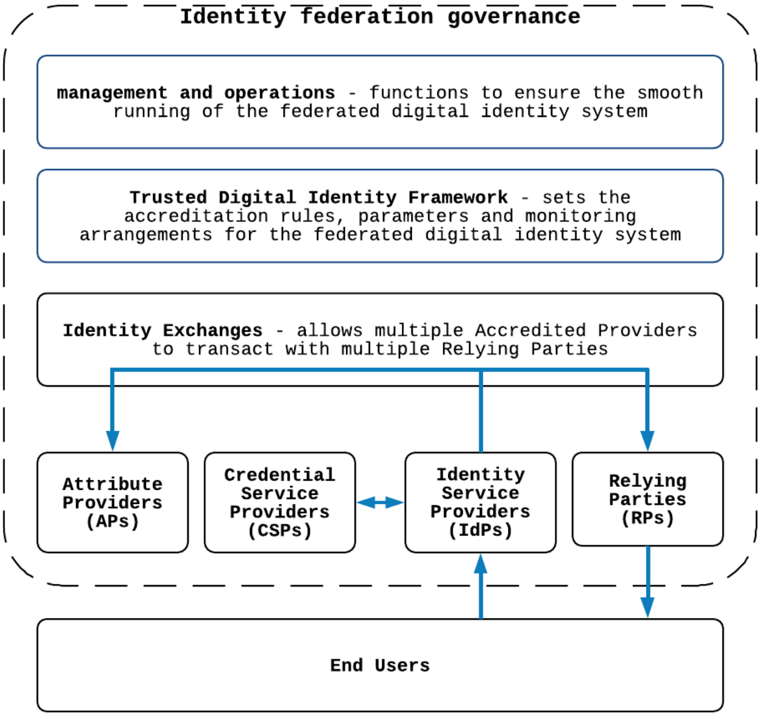
The governance model will ensure:

- Adequate representation of all affected and interested parties in decision making.
- High standards of usability, accessibility, privacy and security.
- Effective risk management and fraud controls.
- Effective mechanisms operate for redress and service support for users and relying parties.
- Robust change management that involves all parties.
- An equitable allocation of risk across participants in the identity federation (users, the governance body, Exchange Platforms, Identity Service Providers, Attribute Providers, Credential Service Providers and Relying Parties).
- A competitive cost and risk environment, including prevention of a monopsony among Identity Service Providers and subsequent rent-seeking.
- Transparency and accountability to government and all participants.

Issues that the identity federation governance body will need to address include:

- Rights and obligations of each participant role.
- Accountability mechanisms.
- Applicant appeal processes.
- Warranties, liability allocation, dispute resolution, and governing law.
- Remediation of breaches by Accredited Providers against TDIF requirements.
- Failure or exit of one or more Accredited Providers.
- Likely cost models for the provision of identity services.
- Management responsibility for shared risks across identity federation participants.
- Managing cyber security incidents, remediation actions and any potential ongoing risks to the identity federation.
- Managing identity fraud incidents and providing victim support services.
- Complaints handling.
- Determining the suitability of Authorised Assessors and other entities that support the operation of the identity federation.

Figure 2: identity federation governance model


Identity federation governance
management and operations - functions to ensure the smooth running of the federated digital identity system
Trusted Digital Identity Framework - sets the accreditation rules, parameters and monitoring arrangements for the federated digital identity system
Identity Exchanges - allows multiple Accredited Providers to transact with multiple Relying Parties
Attribute Providers (APs)
Credential Service Providers (CSPs)
Identity Service Providers (IdPs)
Relying Parties (RPs)
End Users

The TDIF establish the agreed criteria against which all accredited participants must operate.

The Framework envisages a single representative governance body operating within a legislative framework. Australia's federated system of government will mean that any such legislative framework will likely require approval from the Council of Australian Governments (COAG).

The governance body will be supported by a secretariat and a series of working groups that provide specialist advice to the governance body in areas such as technology, privacy, security, usability, etc. The governance body will also operate as the Trust Framework Accreditation Authority[4] - responsible for decisions in relation to the initial accreditation of Identity Service Providers, Credential Service Providers, Attribute Providers and Identity Exchanges, as well as the ongoing maintenance of that accreditation. The governance body would also be responsible for decisions relating to the entry of Relying Parties to the federation.

While the governance body has responsibility for the efficient and effective operation of the identity federation on a day to day basis, there is a need for it to be accountable to Government. In this regard scope exists for the COAG to provide directions to the governance body, and there is an expectation that COAG would receive regular reports from the governance body.

4.7 Accreditation

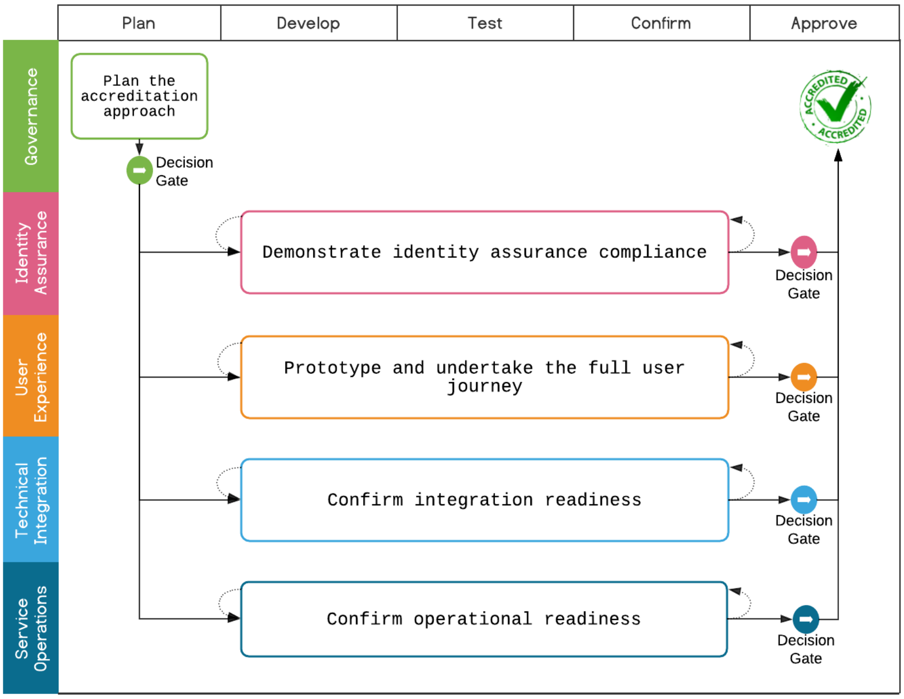
Accreditation of the Applicants is fundamental to the trustworthiness of the identity federation and also to its functional effectiveness. The accreditation process includes a number of accreditation activities and involves a combination of documentation, third party evaluations and operational testing that the Applicants are required to complete in order to be accredited.

As per Figure 3 below, the accreditation activities are linked by a series of work streams that cover governance, identity assurance (including privacy and security), user experience, technical integration and service operations. Progress through the

[4] Regardless of whether the governance body performs the accreditation function or it is delegated to a specialist sub-group the governance body will be accountable for the function

accreditation process is managed by a series of decision gates. The decision gates are used by the Trust Framework Accreditation Authority to evaluate the Applicant's progress towards accreditation. Arrows show the relationships between accreditation activities. The activities in all workstreams can be iterated and worked on in parallel. This approach supports participants that are still developing their identity service who don't meet all the requirements of a particular workstream and are not yet ready to pass a decision gate. See the *Trust Framework: Accreditation Approach* for further information on the Trust Framework Accreditation Process.

Figure 3: Trust Framework Accreditation Process



Each Applicant must be able to demonstrate to the Trust Framework Accreditation Authority their identity service is:

- Able to achieve accreditation in accordance with the Trust Framework Accreditation Process (above).
- Compliant with the TDIF requirements (see '*TDIF development schedule*').
- Able to pass independent assessments by Authorised Assessors.

The accreditation process provides the mechanism to draw the Trust Framework together as a coherent whole.

4.8 TDIF development schedule

There are three releases of TDIF documents proposed for the first half of 2018; the first two need to be completed before accreditation work can commence.

- Release one is now available on the DTA website[5], having been published in Feb 2018 and covers approximately half of the accreditation requirements.
- Release two is currently being drafted and will be available for public consultation in Apr 2018. This release broadly focuses on the second half of the accreditation requirements, ongoing accreditation requirements and governance.
- Drafting will commence shortly for release three and will be available for public consultation by July 2018. Release three will focus on business identity, including authorisations and Attribute Provider accreditation requirements.

Below is a summary of what is included in the first two TDIF releases and how each document will be incorporated into the TDIF.

4.8.1 Release one

the Release one includes ten documents, including:

1. *Overview and Glossary* (this document), which provides a high-level overview of the Trust Framework including its scope and objectives, the relationship between various documents and the definition of key terms.

2. *Accreditation Process,* which defines the requirements to be met by Applicants in order to achieve Trust Framework accreditation.

3. *Fraud Control Requirements*, which sets out the requirements for fraud control.

4. *Privacy Requirements*, which sets out requirements for maintaining user privacy.

5. *Usability and Accessibility Requirements,* which sets out the requirements for prototyping and testing the accessibility and usability of identity services.

[5] See www.dta.gov.au for further information

6. *Risk Management Requirements,* which sets out the risk management responsibilities of Applicants.

7. *Authentication Credential Requirements*, which sets out the requirements which relate to authentication credential management

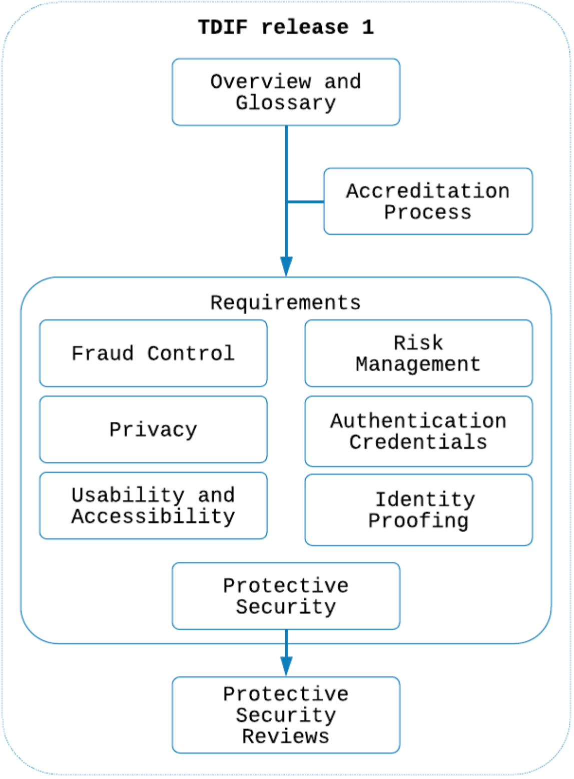
8. *Identity Proofing Requirements*, which sets out requirements relating to the verification of an individual's identity.

9. *Protective Security Requirements*, which sets out the requirements for maintaining security identity services.

10. *Protective Security Reviews*, which sets out the requirements for Authorised Assessors when evaluating the security of identity services.

Figure 4 below, shows the functional relationships between these documents and a suggested reading order.

Figure 4: release one of TDIF documents



4.8.2 Release two

The TDIF release two will include approximately nine new documents and updates to at least two documents from release one. This will include:

1. *Governance Model*, which will how the TDIF and broader identity federation will be governed. It will include roles and responsibilities and cover the governance issues listed above.

2. *Federation Agreement/MOU*, which will be the legally binding agreement that participants sign once accredited. The agreements will specifies arrangements in relation the maintenance of accreditation.

3. *Annual Review,* which will define the annual compliance assessment that participants will need to complete in order to remain accredited.

4. *Technical Integration Requirements*, which will define the technical standards for participants to meet in order to connect identity services into an Identity Exchange.

5. *Conceptual Architecture*, which will describe in detail, the components that make up the identity federation.

6. *Attribute Profile*, which will describe the permissible attribute and data flows between participants within the identity federation.

7. *OpenID Connect 1.0 Profile*, which will describe a profile for the use of OpenID Connect assertions and messages between participants within the identity federation.

8. *SAML 2.0 Profile*, which will describe a profile for the use of SAML assertions and messages between participants within the identity federation.

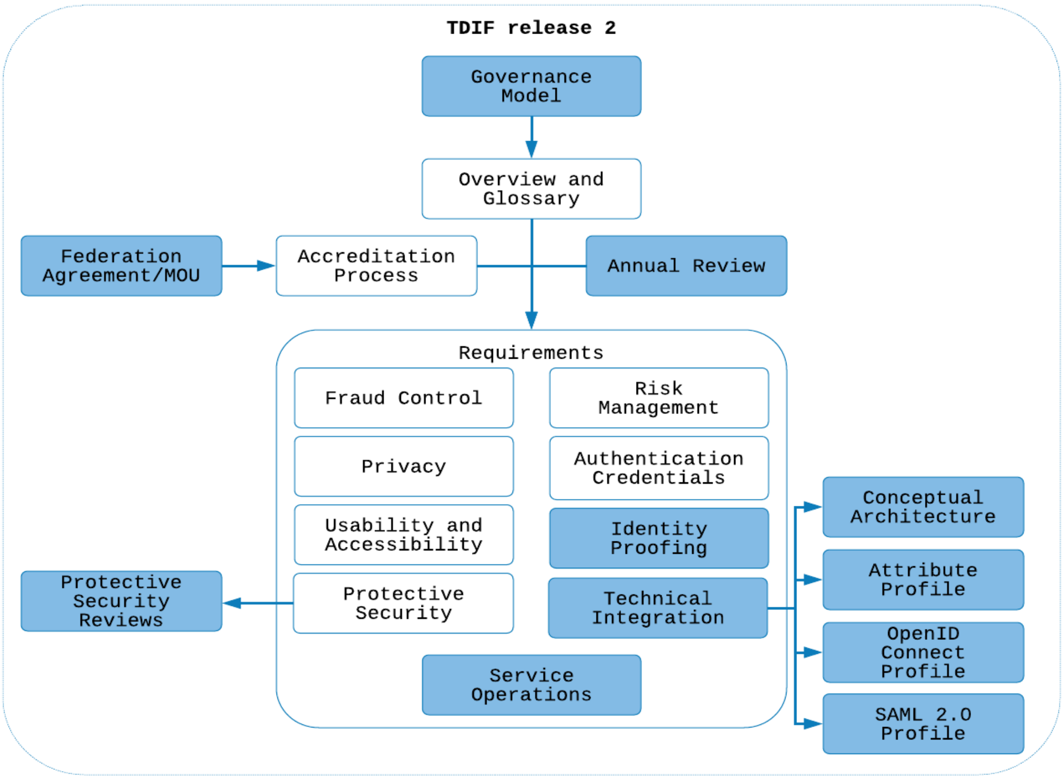
9. *Service Operations Requirements*, which will define the operational requirements that identity services are required to meet.

10. *Identity Proofing Requirements* will be updated to support offline and supported identity proofing processes.

11. *Protective Security Review* will be updated to include guidance to participants and Authorised Assessors when performing information security penetration testing.

Figure 5 below, shows the functional relationships between these documents and a suggested reading order. The labels in blue indicate new or updated TDIF documents added as part of release two.

Figure 5: release two of TDIF documents



5 Glossary of terms

Accreditation. The procedure by which an authoritative body gives independent attestation conveying formal demonstration of a Service Provider's competence to provide services of the kind specified in an assurance framework.

Accredited Providers are organisations and government agencies that have achieved Trust Framework accreditation.

APP. Australian Privacy Principles.

Applicants are organisations and government agencies that undergo the Trust Framework Accreditation Process as either an:

- Attribute Provider,
- Credential Service Provider,
- Identity Exchange,
- Identity Service Provider, or
- a combination of the above.

Attribute Provider (AP) are organisations and government agencies that undergo the Trust Framework Accreditation Process. They generate and manage attributes which are provided to Relying Parties to support their decision-making process. Whereas an Identity Provider verifies the identity of an individual (e.g. I am Joe Bloggs), an Attribute Provider verifies specific entitlements, qualifications or characteristics of an individual (e.g. this Joe Bloggs is authorised to act on behalf of business xyz in a particular capacity).

Australian Government Information Security Manual (ISM) is designed to assist Australian government agencies in applying a risk-based approach to protecting their information and systems. The ISM includes a set of information security controls that, when implemented, will help agencies meet their compliance requirements for mitigating security risks to their information and systems.

Australian Government Protective Security Policy Framework (PSPF) defines a series of core policies and mandatory requirements with which applicable Commonwealth agencies and bodies must demonstrate their compliance. These requirements cover protective security governance, personnel security, information security and physical security.

Australian Institute of Criminology (AIC). Australia's national research and knowledge centre on crime and justice

Authentication. a function for establishing the validity and assurance of a claimed identity of an individual, device or another entity by testing the credentials supplied by the entity making the claim.

Authentication Credential Level (CL) is the level of assurance or confidence in the authentication process, ranked from lowest to highest based on the consequence of incorrectly determining that an individual is who they say they are.

Authentication Factor is an object used in authenticating the identity of an individual. Authentication factors may be something you know (a password or PIN), something you have (a card or device) or something you are (a facial image or fingerprint).

Authorised Assessor are consultants or independent evaluators of products, processes and systems who have the required skills, experience and qualifications to determine whether an Applicant has met specific requirements of the Trust Framework.

Authoritative Source. An electronic database maintained by a Document Issuer that is able to be queried via the DVS.

Binding is the establishment of an association between a claimed identity and a specific authentication factor enabling the authenticator to be used, possibly in conjunction with others, to authenticate a claimant's identity.

Binding Document. An Australian government issued document that has been:

- Verified using the DVS.
- Bound to the document holder with a biometric quality facial image. (e.g. Australian passport).

Biometric. A measurable physical characteristic, a set of characteristics or behavioural traits of a person, which have had a template applied to them so that they can be recognised and matched using an automated system.

Claimant. an individual whose identity is to be authenticated using one or more authentication protocols.

Council of Australian Governments (COAG). The peak intergovernmental forum in Australia. The members of COAG are the Prime Minister, state and territory First Ministers and the President of the Australian Local Government Association (ALGA).

Commencement of Identity (CoI) document is an Australian government issued document which provides document which provides evidence of the establishment or creation of an identity in Australia, either through immigration or birth.

Control. Any process, policy, device, practice or other actions within the internal environment of an organisation which modifies the likelihood or consequences of a risk.

Core Privacy Requirements (CPRs). See the *Trust Framework: Privacy Requirements* for further information.

Credential. the 'technology' used by a claimant for authentication (e.g. user-ID and password, shared information, smartcard.)

Credential Management. the 'lifecycle' approach associated with a credential including creation, initialisation, personalisation, issue, maintenance, recovery, cancellation, verification and event logging.

Credential Service Provider (CSP) are organisations and government agencies that undergo the Trust Framework Accreditation Process. They generate and manage authentication credentials which are provided to individuals. This function may be internalised within an IdP.

Cyber security incident is an occurrence or activity of a system, service or network state indicating a possible breach of protective security policy or failure of safeguards, or a previously unknown situation that may be security relevant. Examples include:

- Receiving suspicious or seemingly targeted emails with attachments or links,
- Any compromise or corruption of information,
- Unauthorised access or intrusion into an identity service,
- Data spill,
- Intentional or accidental introduction of viruses to a network,
- Denial of service attacks, and
- Suspicious or unauthorised network activity.

DFAT. Department of Foreign Affairs and Trade.

DOHA. Department of Home Affairs.

DIBP. Department of Immigration and Border Protection.

Document Issuer. An Australian government agency which issues identity documents.

DTA. Digital Transformation Agency

Document Verification Service (DVS) is a national online system that allows organisations to compare a customer's identifying information with a government record. The DVS matches key details contained on Australian-issued identity documents.

EU GDPR. European Union General Data Protection Regulations.

Family Name. A person’s last name or surname. The ordering of family name and given names varies among cultures. Some cultures do not recognise a ‘family’ name; In Australia the last name is usually adopted as the family name.

Fraud is dishonestly obtaining a benefit, or causing a loss, by deception or other means.

Face Verification Service (FVS). The FVS will allow an IdP to biometrically verify facial images of individuals against biometric records held in the databases of government agencies such as DFAT, DOHA & RTAs.

Given Name. Given names include a combinations of first name/s, forename, Christian name/s, middle name/s and second name/s.

Identity. A combination of identity attributes which uniquely distinguishes a person within a specific context.

Identity Attribute. A piece of information relating to identity. (e.g. full name or date of birth).

Identity Exchange (also called an ‘Exchange Platform’) are organisations and government agencies that undergo the Trust Framework Accreditation Process. They convey, manage and coordinate the flow of identity attributes and assertions between members of the identity federation. Once an Identity Exchange has been granted accreditation it becomes a trusted core element of the identity federation.

Identity Proofing Level (IP). level of assurance or confidence in the identity proofing process ranked from lowest to highest based on the consequence of incorrectly identifying a person.

Identity Service Provider (IdP) are organisations and government agencies that undergo the Trust Framework Accreditation Process. They verify the identity of individuals, bind an identity to an authentication credential and assert identity to other members of the identity federation.

Information Security Registered Assessors Program (IRAP) is an ASD initiative to provide high quality information security services to government. The IRAP provides a framework to endorse individuals from the private and public sectors to provide information security assessment services to Australian governments.

Internal system user is an employee, secondee or third party authorised by the Applicant’s organisation or agency to access and perform functions on the identity service. E.g. a system administrator. See also ‘Personnel’.

IRAP assessment is a review by an IRAP Assessor of the implementation, appropriateness and effectiveness of the information security controls within a computing environment.

IRAP Assessor is an ASD certified information security professional endorsed to provide information security services to Australian governments who can provide an independent assessment of information security, suggest mitigations and highlight residual risks.

Knowledge Based Authentication - see Shared Secrets.

Linking Document. A document that provides linking evidence between two names resulting from a name change. (e.g. change of name certificate or marriage certificate).

Liveness Detection. Liveness detection refers to a functionality in a biometric system or process which checks whether an entity presenting is a live person.

Memorised Secret - commonly referred to as a password or, if numeric, a PIN - is a secret value intended to be chosen and memorised by the user.

Multi-factor Authentication - an authentication protocol that relies on more than one authentication factor for successful authentication.

Multi-factor Cryptographic (device) - is a hardware device that performs cryptographic operations using one or more protected cryptographic keys and requires activation through a second authentication factor (either something the claimant knows or something the claimant is).

Multi-factor Cryptographic (software) - a multi-factor software cryptographic authenticator is a cryptographic key stored on disk or some other "soft" media that requires activation through a second authentication factor (either something the claimant knows or something the claimant is).

Multi-factor Cryptographic (trusted device) - is a Multi-factor Cryptographic device that has been evaluated by ASD and is on the ASD Evaluated Products List.

Multi-factor One-Time Password - is a trusted device that generates OTPs for use in authentication after activation through an additional authentication factor (either something the claimant knows or something the claimant is). This includes hardware devices and software-based OTP generators installed on devices such as mobile phones. The OTP is displayed on the device and input or transmitted by the claimant, proving possession and control of the device.

One-Time Password (OTP) - is a password that is changed each time it is required.

Out-of-Band Device - is a physical device that uses an alternative channel for transmitting information - eg SMS to send a PIN or one-time password.

National Identity Proofing Guidelines (NIPGs). the Council of Australian Government's national guidelines for identity proofing.

Personnel refers to officials, employees, contractors and agents working on behalf of the Applicant.

Presentation attack. Attempt to gain access by spoofing a biometrics-based security measure by manipulating the image/s collected for biometric verification purposes, so that it represents the account holder.

Privacy audit criteria is the criteria against which a privacy audit is evaluated.

Privacy audit objective is the objective of the privacy audit.

Privacy audit scope are the Applicant’s activities that will and will not be subject to the privacy audit.

Privacy Impact Assessment (PIA) is a systematic assessment of an identity service that identifies the impact that the identity service might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.

Protective Security Documentation is the minimum set of protective security documents that an Applicant is required to develop in order to satisfy the requirements of the *Trust Framework: Protective Security Requirements*.

RBDM. Australian State and Territories based Registry of Births, Deaths and Marriages

Relying Party is an organisation or government agency that relies on verified attributes or assertions provided by an Applicant through an Identity Exchange to enable the provision of a digital service.

Risk. The effect of uncertainty on objectives. An effect is a deviation from the expected - positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances or knowledge) and the associated likelihood of occurrence.

Risk appetite. The amount and type of risk an entity is willing to accept or retain in order to achieve its objectives. It is a statement or series of statements that describes the organisation's attitude toward risk taking.

Risk assessment. The process of risk identification, risk analysis and risk evaluation.

Risk management framework. A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

Risk management. Are the coordinated activities and actions taken to ensure that an organisation is conscious of the risks it faces, makes coordinated and informed decisions in managing those risks and identifies potential opportunities.

Risk profile. A description of any set of risks. The set of risks can contain those that relate to the whole organisation, part of the organisation or as otherwise defined.

Risk tolerance. The levels of risk taking that are acceptable in order to achieve a specific objective or manage a category of risk.

Risk. The effect of uncertainty on objectives. An effect is a deviation from the expected. positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances or knowledge) and the associated likelihood of occurrence.

RTA. A state-based Australian Road and Transport Authority.

Serious and complex fraud is fraud which due to its size or nature, is considered too complex for Applicants and Accredited Providers to investigate. Complex fraud may involve collusion between officials and external parties.

Shared risk. A risk with no single owner, where more than one entity is exposed to or can significantly influence the risk. The responsibility for managing a shared risk is shared by all relevant identity federation participants and will benefit from a coordinated response where one identity federation participant takes a lead role.

Session - once authentication has taken place a session may be established to allow the claimant to continue accessing the service across multiple subsequent interactions without requiring repeated authentication.

Shared Secret - a secret used in authentication that is known to the subscriber and the verifier. Shared Secrets are frequently used to implement knowledge-based authentication.

Single-factor Authentication. An authentication protocol that relies on only one authentication factor for successful authentication.

Single-factor Cryptographic (software) - is a cryptographic key stored in some form of ‘soft’ media. Authentication is accomplished by proving possession and control of the key.

Single-factor One-Time Password (device) - a device that generates OTPs, including hardware devices (e.g. a dongle), SMS or software-based OTP generators installed on devices such as mobile phones. The OTP is displayed on the device and input or transmitted by the claimant.

SMS One-Time Password - an OTP that is delivered via SMS.

Social Footprint check (SFC). A check that confirms whether an identity has been operating in the community for five or more years. For this check, a minimum of three distinct data points evidencing a history of transactions over a minimum five year period are validated. These data points may be from a common transaction history or a number of independent sources, however all such sources should be reliable and there should be reasonable confidence that they cannot be modified after the fact. Examples of such data sources include tax records, health records, postal records, telephone records, and banking and other financial records. Such evidence should provide evidence of activity over time (e.g. an account transaction, not just the creation of an account). A SFC does not include access to an individual's social media accounts or information.

Something the individual has - see Authentication Factor.

Something the individual is - see Authentication Factor.

Something the individual knows - see Authentication Factor.

Step up. A process where the level of assurance of a person's identity is increased from one IP level to the next IP level.

TDIF. Abbreviated form of the Trusted Digital Identity Framework.

Trust Framework Accreditation Authority is the Government entity which manages the Trust Framework Accreditation Process and makes decisions in relation to the accreditation of Applicants and Accredited Providers.

Trust Framework Accreditation Process includes a number of activities and involve a combination of documentation requirements, third party evaluations and operational testing that Applicants must complete to the satisfaction of the Trust Framework Accreditation Authority in order to achieve Trust Framework accreditation.

Trusted Device. a device for facilitating authentication that an individual controls and that is enrolled as part of the creation of the credential.

Trust Framework describes a legally binding and agreed set of specifications, rules, and agreements for the governance of a federated identity system established to achieve common outcomes among participants.

Trusted Digital Identity Framework. The TDIF contains the tools, rules and accreditation criteria to govern the identity federation. It provides the required structure and controls to deliver confidence to participants that all Accredited Providers in the identity federation have met their accreditation obligations and as such may be considered trustworthy. These obligations cover privacy, protective security, accessibility and usability, risk management, fraud control, technical integration, service operations, identity proofing and authentication credential management.

Unique in context. Unique in the context of an IdP. While individuals can choose to sign up with multiple IdPs, each individual should have only one identity within the same IdP.

Use in the Community (UitC) document is a government issued document or a document issued by a reliable and independent source used to demonstrate the use of an individual’s identity in the community over time. (e.g. a Medicare card).

User is an individual who uses the identity service in order to access a Relying Party service. (e.g. the general public).

User Experience for the purpose of the Trusted Digital Identity Framework this covers the accessibility, usability and inclusive design aspects of solution design to ensure identity services are straightforward and easy to use.

User Researcher. A person who focuses on understanding user behaviours, needs, and motivations through observation techniques, task analysis, and other feedback methodologies.

Validation. A check that the attribute exists and is under the control of the individual. (e.g. SMS activation code being sent to the number to confirm control).

Verification. The act of confirming that information presented matches information held by the Authoritative Source.

6 References

The following information sources have been used in developing this document.

1. Commonwealth of Australia, 2015, ‘Financial System Inquiry’, Commonwealth of Australia. http://fsi.gov.au/
2. Makaay, E. Smedinghoff, T. & Thibeau, D, 2017, ‘Trust Frameworks for Identity Systems’, Open Identity Exchange (OIX). http://www.openidentityexchange.org/trust-frameworks-for-identity-systems-2/
3. United Nations Commission on International Trade Law (UNCITRAL), 2017, ‘Legal issues related to identity management and trust services – terms and concepts relevant to identity management and trust services’, United Nations. https://documents-dds-ny.un.org/doc/UNDOC/LTD/V17/008/31/PDF/V1700831.pdf?OpenElement