Australian Government
Digital Transformation Agency

Overview and Glossary

Trusted Digital Identity Framework
August 2018, version 1.2

dta

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.

Document Management

The Trust Framework Accreditation Authority has reviewed and endorsed this document for release.

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
1.1	Mar 2018	PH & SJP	Updates to the TDIF schedule and glossary of terms.
1.2	Aug 2018	SJP	Feedback incorporated from stakeholders

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, and the definition of key terms.

The intended audience for this document includes:

- Accredited Providers.
- Applicants.
- 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 people, 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 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 people 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[2]" 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

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

[2] The term 'Trust Framework' is defined by the Open Identity Exchange in their whitepaper, titled '*Trust Frameworks for Identity Systems*'. See *References* for further information on this whitepaper.

systems that employ trust frameworks include electronic bill payment systems (such 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 Open Identity Exchange[3] 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 a person's identity, the binding of a person to authentication credentials and the reuse of those credentials to access relying party 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.

[3] See *References* for further information on the Open Identity Exchange

    - Transparency: the trust framework specifications, rules, and agreements are accessible to and agreed by all participants.
- 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[4] ('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 (TDIF) 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 will be accredited. The TDIF is being developed by the DTA in consultation with government agencies and key private sector, privacy and consumer advocates.

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

Success will also be measured by the number of people that can complete the digital identity verification process to access services. A public dashboard will be developed to report transparency on this, along with measuring user satisfaction, digital take-up

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

and identity verification completion rates. This dashboard will form part of the DTA's performance dashboard.

Participants will judge the federated digital identity system a success by broad acceptance of the requirements established through the TDIF, and when the identity federation's governance body executes its roles and responsibilities in an effective and transparent manner.

4.3 Guiding Principles

The TDIF will operate to the following principles:

User centric:

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

Voluntary and transparent:

- People choose whether or not to participate.
- People control their digital identities in an easy and straightforward manner.
- Records of authentication credential use are maintained and easily accessible.

Service delivery focused:

- Accredited identity and credential service providers offer choice and convenience for people.
- Participation is cost neutral for people to use.
- The supporting business model encourages private sector participation.

Privacy enhancing:

- Personal information is only collected, used and disclosed with the consent of the person and in accordance with privacy laws and good privacy practices.

- Privacy enhancing technology, policy and processes are applied to all personal information.
- People have an informed understanding of how their personal information will be used and protected.
- People can view and manage their personal information, correct errors and revoke their consent.

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:

- Use relevant open standards, frameworks and common approaches to facilitate interconnectedness with other identity services nationally and internationally.

Adaptable:

- Promote flexibility and innovation in technology and business models.
- The TDIF is flexible to evolve in line to meet community expectations and changing business, technology and social needs.
- The identity system is architected to support secure transactions ranging from low to high value and from anonymous to fully verified.

Secure and resilient:

- Accreditation requirements apply to identity service providers, credential service providers, attribute providers and identity exchanges. Relying parties also need to meet minimum standards to participate in the federated digital identity system.
- The same accreditation requirements apply to government and public-sector identity systems.
- Cyber security threats and risks are identified and actively managed by accredited providers and relying parties
- Effective fraud management controls are implemented and maintained.

4.4 Objectives

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

Simple and easy to use: 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.

Security and privacy preserving: digital identity services are security and privacy preserving. People can interact with any relying party without an identity service provider knowing the identity of the relying party and vice versa (this is known as 'double blind'). The identity service provider and relying party are prevented from tracking people using policy and technical means. There is no single digital authentication credential or centralised database of personal information. People are given greater control over their personal information and who their personal information is shared with.

Standards based: digital identity services support 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 participants 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 issues arise. The operational functions performed by the DTA in relation to the TDIF include:

- **Governance and policy development:** Developing and amending TDIF policies; decision making; stakeholder-facilitation; managing standards and procedures; accountability mechanisms.
- **Policy binding:** Ensuring compliance with TDIF requirements; binding mechanisms; performing assessments or audits; managing policy changes and releases.
- **Participant management:** Administration and enrolment of participating entities; evaluating accreditation plans and the associated timeframes; approving exceptions and exclusions; participant on-boarding and support; dispute resolution; participant off-boarding and penalising persistent non-compliant participants.
- **Network evolvement:** Growing and supporting the federated digital identity system; marketing; communication and strategy developing.
- **Trust Framework operations:** Offering central services to the participants 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 management**: registration, collection, verification, disclosure, modification and deletion of identity information and related attributes, claims and assertions.
- **Authentication credential management:** registration, creation, binding, acceptance, renewal, modification, suspension, revocation and deletion of authentication credentials.
- **Attribute management**: application, collection, verification, disclosure, modification and deletion of attributes relating to specific entitlements, qualifications, relationships or characterises of people and non-person entities.
- **Authentication management**: requesting verification of identity information, attributes, claims, assertions, authentication credentials and providing the results of verification.
- **Authorisation management**: managing user consent. Both in the context of a person who consents for their own personal information to be shared with an

authorised third party, as well as when a person authorises someone to act on their behalf.

- **Records management:** All participants will be required to use efficient and effective controls for the creation, maintenance, use, disposal and receipt of records in an accountable manner.

The TDIF accommodates the following roles to undertake these functions:

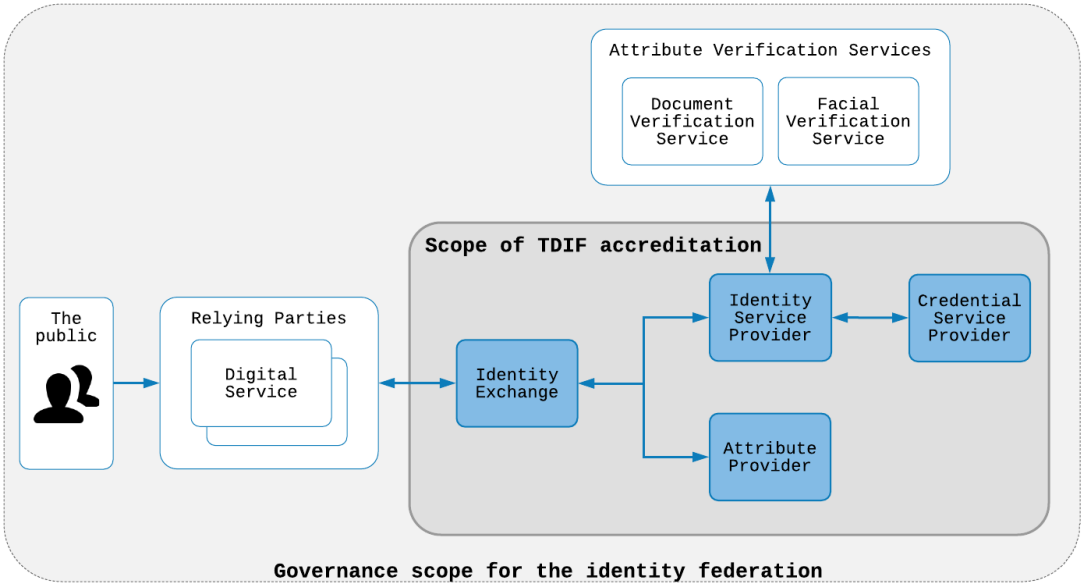
- **Identity Service Providers** (IdP) are accredited to undertake the functions of identity management, authorisation management and records management.
- **Credential Service Providers** (CSP) are accredited to undertake the functions of authentication credential management and records management. This includes generating, binding and distributing authentication credentials to people or can including the binding and management of authentication credentials generated by people. This function may be internalised within an IdP. Depending on the implementation of the IdP, the CSP and their relationship, authentication credentials may be bound to a 'empty' IdP account prior to identity verification, or bound to a digital identity as part of the identity verification process.
- **Attribute Providers** are accredited to undertake the functions of attribute management and records management. Attribute providers generate and manage attributes and claims that are provided to Relying Parties (through Identity Exchanges) to support their decision-making processes.
- **Identity Exchanges** are accredited to undertaken the functions of authentication management and records management. Identity exchanges convey, manage and coordinate the flow of attributes, claims and assertions between members of the identity federation. Over time the identity federation will support multiple identity exchanges. The Commonwealth government identity exchange will function in double-blind mode[5] and operate independently from other participants in the identity federation.
- **Relying Parties** (also referred to as digital services) are the organisations and government agencies that rely on verified identity information, attributes or assertions provided by identity service providers and attribute providers through an identity exchange to enable the provision of a digital service.

[5] Double blind is described in the '*Security and privacy preserving'* objective listed above.

- **The public**. People who establish and use a digital identity within the identity federation. This includes people acting in their own capacity and also people who act on behalf of others (authorisations).
- **Attribute Verification Services** (also known as Authoritative Sources) are repositories connected to the identity federation recognised by the Trust Framework Accreditation Authority that confirm the veracity of identity attributes and associated information. Attribute Verification Services can refer to either the repositories themselves, or the methods used to access them (e.g. Document Verification Service).

Figure 1 below, outlines one instance of each role within the federated digital identity system, the scope of the TDIF accreditation and the governance scope for the broader identity federation. 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 over time the identity federation includes several identity service providers, credential service providers, attribute providers and identity exchange platforms operating across multiple tiers of government and the private sector. TDIF accreditation applies equally to these providers, regardless of whether they are a government agency, department or private sector entity.

Figure 1: roles within the federated digital identity system



TDIF documents and development schedule

Three releases of TDIF documents are scheduled for 2018. The first two releases have now been delivered and the third release will be available for public comment before the end of the 2018 calendar year.

TDIF release one was published in February 2018, is now available on the DTA website[6] and includes the following ten documents:

1. ***Overview and Glossary*** (this document), which provides a high-level overview of the Trust Framework including its scope and objectives, and the definition of key terms.
2. ***Accreditation Process****,* which describes the process and 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 privacy.
5. ***Usability and Accessibility Requirements****,* which sets out the requirements for prototyping and testing the accessibility and usability of identity services.
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 a person'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 evaluating the security of identity services.

[6] See http://www.dta.gov.au/ for further information

TDIF release two was published in August 2018, is now available on the DTA website[7] and includes the following 11 documents. This includes a combination of new and updates to TDIF release one documents.

New documents:

1. ***Attribute Profile***, which describes the technical specification of the attributes that can be shared between Identity Providers and Relying Parties via an Identity Exchange.
2. ***Interim Memorandum of Agreement***, is an agreement signed by participants once accredited. The MOU also outlines how accreditation will be maintained. Commencing in calendar year 2019, the MOU will be replaced with a set of legally binding Operating Rules. Further information on the Operating Rules will be publicly available before the end of 2018.
3. ***OpenID Connect 1.0 Profile***, which describes how OpenID Connect is used within the identity federation.
4. ***SAML 2.0 Profile***, which describes how SAML is used within the identity federation.
5. ***Service Operations Requirements***, which sets out the operational requirements that identity services are required to meet.
6. ***Technical Integration Testing Requirements***, which defines the technical standards to be met to connect identity services and relying parties to identity exchanges.

Updates to TDIF release one documents:

7. ***Authentication Credential Requirements***, this is an update of the Authentication Credential Requirements published in February 2018. This document now aligns with the National Institute of Standards and Technology (NIST) guidelines for authentication and lifecycle management and includes revised implementation guidance. Document content has also been restructured to improve readability.

[7] See http://www.dta.gov.au/ for further information

8. ***Fraud Control Requirements*** this is an update of the fraud control requirements published in February 2018. It has been updated with structural changes and content updates.

9. ***Identity Proofing Requirements*** this is an update of the Identity Proofing Requirements published in February 2018. The document now supports offline and supported identity proofing processes.

10. ***Overview and Glossary*** this is an update of the Overview and Glossary published in February 2018. The document has undergone significant change based on feedback received from stakeholders and the public.

11. ***Protective Security Reviews*** this is an update of the Protective Security Review document published in February 2018. It has been updated to include penetration testing and vulnerability management requirements.

Development for TDIF release three has now commenced will focus on business authorisations, core technical requirements and attribute provider requirements.

4.6 Conventions used across TDIF documents

Specific conventions are used across the TDIF documents to signify requirements. The following section defines these words and how they should be interpreted[8]. TDIF documents that include these conventions will include this phrase at the beginning of the document under the title "Conventions":

> The key words "**MUST**", "**MUST NOT**", "**SHOULD**", "**SHOULD NOT**", and "**MAY**" in this document are to be interpreted as described in the current version of the *Trusted Digital Identity Framework: Overview and Glossary*.

The force of these words is determined by the convention used.

- **MUST** – means an absolute requirement of this document. Failure to meet this requirement will impact the Applicant's ability to achieve and maintain TDIF accreditation.
- **MUST NOT** – means an absolute prohibition of this document. Failure to prevent this prohibition from occurring will impact the Applicant's ability to achieve and maintain TDIF accreditation.

[8] These conventions are taken from Request for Comments 2119 (RFC2119) – Keywords for use in RFCs to indicate requirements levels

- **SHOULD** – means an Applicant is required to meet this requirement unless there is a valid reason for them to ignore it. The Applicant must seek agreement from and provide evidence to the Trust Framework Accreditation Authority before it can ignore this requirement. Failure to meet this requirement will impact the Applicant's ability to achieve and maintain TDIF accreditation.
- **SHOULD NOT** – means an Applicant is required to prevent this prohibition from occurring unless there is a valid reason for them not to do so. The Applicant must seek agreement from and provide evidence to the Trust Framework Accreditation Authority before it can ignore this requirement. Failure to meet this requirement will impact the Applicant's ability to achieve and maintain TDIF accreditation.
- **MAY** – means truly optional. This requirement has no impact on the Applicant's ability to achieve and maintain TDIF accreditation if it is implemented or ignored.

4.7 TDIF Accreditation Process

TDIF accreditation is a formal process through which applicants demonstrate their ability to meet specific requirements of the TDIF to the satisfaction of the Trust Framework Accreditation Authority. TDIF accreditation covers the initial accreditation and ongoing accreditation obligations.

Initial accreditation: – The accreditation of the IdPs, CSPs, attribute providers and identity exchanges is fundamental to the trustworthiness of the identity federation and also to its functional effectiveness. Initial accreditation is achieved by applicants that satisfy the requirements of the TDIF Accreditation Process[9]. The TDIF Accreditation Process includes a number of accreditation activities and involves a combination of documentation, third party evaluations and operational testing that applicants are required to complete in order to be accredited and thus suitable to join the identity federation.

Ongoing accreditation obligations: once accredited, Accredited Providers are required to complete annual compliance assessments against the TDIF and remediate any adverse findings in timeframes agreed with the Trust Framework Accreditation Authority. These assessments ensure Accredited Providers continue to offer straightforward and easy to use identity services in a security and privacy preserving manner.

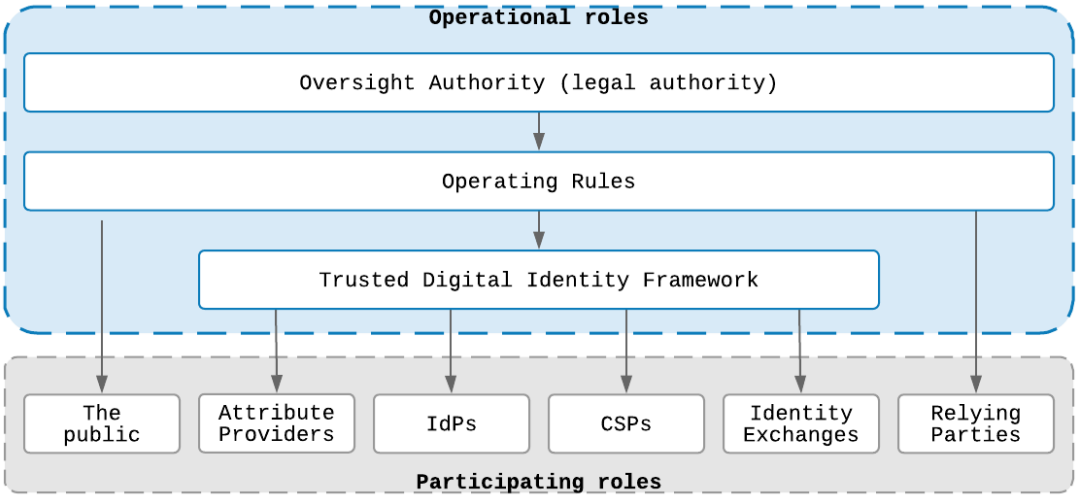
[9] For further information see the *Trust Framework: Accreditation Process*

4.8 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 identity federation governance model that is currently being developed. The arrows indicate how the various roles relate.

Further information regarding the federated governance model will be publicly available before the end of 2018. For the remainder of the 2018 calendar year, the DTA will fulfil the role of Trust Framework Accreditation Authority (TFAA). Commencing in calendar year 2019, the TFAA role will likely merge into the broader Oversight Authority role.

Figure 2: identity federation governance model



The Oversight Authority will be responsible to ensure participants operating in the identity federation:

- Are adequately represented in decision-making processes which impact themselves of the identity federation.
- Maintain fair and equitable use and availability of their identity services.
- Implement and maintain high standards of usability, accessibility, privacy and security for their identity services.

- Implement and maintain effective risk management and fraud prevention controls for their identity services.
- Formally manage and approve all exceptions that impact the operation of the identity federation.
- Implement and maintain effective mechanisms for redress, reporting privacy breaches and service support for people and relying parties.
- Implement and maintain robust change management processes for their identity service, which involves all relevant stakeholders.

The Oversight Authority will also be responsible to ensure:

- An equitable allocation of risk across the participating roles.
- A competitive and commercially viable business model underpins the identity federation.
- The prevention of a monopsony among IdPs and subsequent rent-seeking behaviours.
- Transparency and accountability to government and all participants.

Issues that the Oversight Authority will be responsible to address include:

- Enforcement of the participating rules (i.e. Operating Rules and TDIF)
- Rights and obligations of each participating role.
- Accountability mechanisms.
- Applicant and participant 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.
- Cost models for the provision of identity services.
- Management responsibility for shared risks across identity federation participants.
- Investigating and managing cyber security incidents, remediation actions and potential ongoing risks to the identity federation.
- Managing identity fraud incidents (including privacy breaches) and providing victim support services.
- Complaints handling.
- Maintenance of the Operating Rules and documents that form the TDIF.
- The definition of cross recognition requirements to enable other identity systems to join the identity federation (e.g. international governments).

The Oversight Authority will be supported by a secretariat and a series of working groups that provide specialist advice in areas such as technology, privacy, security, service design, etc.

The Oversight Authority will be responsible for all decisions in relation to the initial accreditation of IdPs, CSPs, Attribute Providers and Identity Exchanges, as well as the ongoing maintenance of their accreditations. The Oversight Authority will also be responsible for decisions relating to the entry of Relying Parties to the identity federation.

5 Glossary of terms

Accreditation. The process 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. Source: TDIF defined Term.

Accredited Providers. Organisations and government agencies that have achieved Trust Framework accreditation. Source: TDIF defined term.

Active Attack. An attack on the authentication protocol where the attacker transmits data to a User, Identity Service Provider, Credential Service Provider, Attribute Provider, Identity Exchange or Relying Party. Examples of active attacks include man-in-the-middle (MitM), impersonation, and session hijacking. Source: NIST 800-63

APP. Australian Privacy Principles.

Applicants. Organisations and government agencies that undergo the Trust Framework Accreditation Process as either an:

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

Source: TDIF defined term.

ASD. Australian Signals Directorate

Assertion. An Assertion Statement made by an entity without accompanying evidence of its validity. Source: Source: ISO/IEC 29003:2013, ITU-T X.1252

Assessing Officer. A person who is assessing applications and making a decision about whether a person meets the specified identity proofing requirements. The assessing officer may be an employee of the organisation or contracted to assess applications. Source: TDIF defined term.

Assisted Digital. Assistance and interaction between a person and a service provider aimed at successfully completing a transaction, which can include support provided to a person during an identity proofing process or registration interview. This could be face-to-face shopfront assistance or include any secure online process that provides the person with assistance including chat bot, web-chat, call-centre or other live session-based 'dial-in' assistance. Assisted Digital processes will be assessed as part of an IdP's accreditation by the Accreditation Authority. Source: TDIF defined term.

Attribute. An item of information or data associated with a subject. Examples of attributes include information such as name, address, age, gender, title, salary, net worth, driver's license number, e-mail address, mobile number, and data such as the subject's network presence, the device used by the subject, the subject's usual home location as known by a network, etc. (for a human being); corporate name, principal office address, registration name, jurisdiction of registration, etc. (for a legal entity); make and model, serial number, location, capacity, device type, etc. (for a device). Source: UNCITRL

Attribute Provider (AP). Organisations and government agencies that undergo the Trust Framework Accreditation Process. They generate and manage attributes relating to people and Non-Person Entities which are provided to Relying Parties to support their decision-making processes. Whereas an Identity Provider verifies the identity of a person (e.g. I am Joe Bloggs), an Attribute Provider verifies specific attributes relating to entitlements, qualifications or characteristics of that person (e.g. this Joe Bloggs is authorised to act on behalf of business xyz in a particular capacity). Source: TDIF defined term.

Attribute Verification Service. See Authoritative Source.

Australian Government Information Security Manual (ISM). A manual 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. Source: ASD.

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 a person, device or another entity by testing the credentials supplied by the entity making the claim. Source: NIPGs

Authentication Credential. See Credential.

Authentication Credential Level (CL). The level of assurance or confidence in the authentication process, ranked from lowest to highest based on the consequence of incorrectly determining that a person is who they say they are. Source: TDIF defined term.

Authentication Factor. A piece of information and process used to authenticate or verify the identity of an entity. Source: ISO/IEC 19790. Note: authentication factors are divided into four categories: (a) something an entity has (e.g., device signature, passport, hardware device containing a credential, private key); (b) something an entity knows (e.g., password, PIN); (c) something an entity is (e.g., biometric characteristic); or (d) something an entity typically does (e.g., behaviour pattern). Source: Rec. ITU-T X.1254.

Authorised Assessor 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. Source: TDIF defined term.

Authoritative Source. Repositories connected to the identity federation recognised by the Trust Framework Accreditation Authority that confirm the veracity of identity attributes and associated information. Source: TDIF defined term.

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 claimed identity. Source: TDIF defined term.

Biometric Information (Biometrics). Information about any measurable biological or behavioural characteristics of a natural person that can be used to identify them or verify their identity, such as face, fingerprints and voice. (Under the Privacy Act 1988 biometric information is considered as sensitive information, which provides additional obligations on organisations.). Source: NIPGs.

Biometric Verification. The automated Verification of a person based on their biological and behavioural characteristics. E.g. the facial matching conducted by the FVS. Source: ISO/IEC 2382-37:2017.

Black box system testing. A security testing and examination technique performed by a protective security specialist. Black box techniques are performed against an application's binary executable without source code knowledge. Black box techniques are used to assess the security of individual compiled components, interactions between components, applications, users, other systems and the external environment. Black box techniques are also used to determine how effective an application or system can handle threats. Source: NIST SP 800-115.

Claimant. A person whose identity is to be authenticated using one or more authentication protocols. Source: TDIF defined term.

Commencement of Identity (CoI). The first registration by a government agency in Australia and includes RBDM birth registrations and issuance of Home Affairs immigration documents and records. Source: NIPGs

Community Footprint Check. The trail of information recorded in information systems or other types of evidence (such as testimonial from a referee) as a result of normal social, living and employment activities during a person's lifetime. In the context of the TDIF, this means a check that confirms whether an identity has been operating in the community over time. Source: TDIF defined term.

Consent. Means express consent or implied consent. The four key elements of consent are:

- the individual is adequately informed before giving consent.
- The individual gives consent voluntarily.
- The consent is current and specific, and
- The individual has the capacity to understand and communicate their consent.

Source: OAIC and Privacy Act 1988, Section 6

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. Source: ISO 31000

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).

Credential. A Credential is the technology used to authenticate a user's identity (also referred to as an authentication credential). The user possesses the Credential and controls its use through one or other authentication protocols. A Credential may incorporate a password, cryptographic key or other form of secret. To use a digital identity in requesting access to a resource, a subject presents an authentication credential. The Credentials (once authenticated) are taken as proof that the subject owns the digital identity being presented, and that the subject is permitted to access the resources/services which are associated with their digital identity. Source: NIPGs.

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

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 people. This function may be internalised within an IdP. Source: TDIF defined term.

Cryptographically Secure Verification. Verifying the integrity of the information on a credential using an Approved cryptographic process such as the RFID chip in an e-passport or the signature on a pdf. Source: TDIF defined term.

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.

Source: ISM.

Department of Home Affairs. Government Agency responsible for Australia's federal law enforcement, national and transport security, criminal justice, emergency management, multicultural affairs and immigration and border-related functions and agencies.

DFAT. Department of Foreign Affairs and Trade.

Digital Identity. A set of the attributes about a person that uniquely describes the person engaged in an online transaction under the Trust Framework identity eco-system. Source: TDIF defined term.

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.

Entity. Something that has separate and distinct existence and that can be identified in a context. Note: an entity can be a physical person, an animal, a juridical person, an organization, an active or passive thing, a device, a software application, a service, etc., or a group of these entities. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc. Source: Rec. ITU-T X.1252. An entity may have multiple identifiers.

EU GDPR. European Union General Data Protection Regulations.

Evidence of Identity (EoI). The types of evidence that, when combined, provide confidence that a person is who they say they are. In the context of the TDIF it refers to information that a person may present to support assertions or claims to a

particular identity. This evidence may be provided in the form of identity documents or other card-based credentials that contain key attributes (such as name, date of birth, unique identifier) or provide information on a person's 'pattern of life' or 'community footprint'. Source: TDIF defined term.

Express Consent. Express consent is given explicitly, either orally or in writing. This could include a handwritten signature, or oral statement, or use of an electronic medium or voice signature to signify agreement. Source: OAIC.

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

Fact of Death File (FoD). A database of deaths registered in Australia, managed by the Queensland Registry of Births, Deaths and Marriages and available to approved applicants for administrative data cleansing purposes.

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. Source: Improving the integrity of Identity Data: Recording of a Name to Establish Identity: Better Practice Guidelines for Commonwealth Agencies – June 2011.

Federation. A group of identity providers, relying parties, subjects and others that agree to operate under compatible policies, standards, and technologies specified in system rules (or a trust framework) in order that people's identity information provided by identity providers can be understood and trusted by relying parties. Synonyms: identity federation, multi-party identity system. Source: TDIF defined term.

Fraud. Dishonestly obtaining a benefit, or causing a loss, by deception or other means. Source: Commonwealth Fraud Control Policy.

Gatekeeper. The Australian Government's policy and accreditation framework for the use of PKI by Australian Government agencies. Source: Gatekeeper.

Given Name. Given names include a combinations of first name/s, forename, Christian name/s, middle name/s and second name/s. Source: Improving the integrity

of Identity Data: Recording of a Name to Establish Identity: Better Practice Guidelines for Commonwealth Agencies – June 2011

Identity. A set of the attributes about a person that uniquely describes the person within a given context. Source: UNCITRL.

Identity Attribute. A piece of information relating to identity. (e.g. full name or date of birth). Source: TDIF defined term.

Identity Credential Issuer. An Australian government entity or approved entity that issues identity documents or identity credentials, such as Passports, Driver's Licences or Proof of Age credentials. Source: TDIF defined term.

Identity Crime. Activities or offences in which a perpetrator uses a fabricated, manipulated, stolen or otherwise fraudulently assumed identity to facilitate the commission of crime. Source: NIPGs

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. Source: TDIF defined term.

Identity Fraud. The gaining of money, goods, services or other benefits or the avoidance of obligations through the use of a fabricated, manipulated, stolen or otherwise fraudulently assumed identity. Source: NIPGs.

Identity Proofing Level (IP). Identity proofing refers to the process of collecting, verifying, and validating sufficient identity attributes about a specific person to define and confirm their identity. An IP describes the level of assurance or confidence in the identity proofing process ranked from lowest to highest based on the consequence of incorrectly identifying a person. Source: TDIF defined term.

Identity Service Provider (IdP). Organisations or government agencies that undergo the Trust Framework Accreditation Process to create, maintain and manage trusted identity information of other entities and offer identity-based services. In the context of

the TDIF, an Identity Service Provider carries out identity proofing and/or identity information verification. Source: TDIF defined term.

Identity theft. The fraudulent use of a person's identity (or a significant part thereof) without consent, whether the person is living or deceased. Source: NIPGs

Implied consent. Implied consent arises when consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity. Source: OAIC

Individual – see person.

In-person Interaction. An interaction in which the subject and/or applicant must be physically present with, and sighted by, an officer or contractor from the organisation. Source: NIPGs.

Information Security Registered Assessors Program (IRAP). An Australian Signals Directorate initiative to provide high quality information and communications technology services to government in support of Australia's security. The IRAP provides a framework to endorse people from the private and public sectors to provide information security assessment services to Australian governments. Source: ASD

Internal system user. 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'. Source: TDIF defined term.

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

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. Source: ASD

ISM. See Australian Government Information Security Manual (ISM)

Key. A string of characters used with a cryptographic algorithm to encrypt and decrypt. Source: Gatekeeper.

Knowledge Based Authentication – see Shared Secrets.

Linking Document. A document which provides a link demonstrating the continuity of the claimed identity where identity attributes, such as name or date of birth, have changed. e.g. change of name certificate, marriage certificate, or in some cases a birth certificate. Source: TDIF defined term.

Liveness Detection. The measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture. Note 1 to entry: Liveness detection methods are a subset of presentation attack detection methods. Source: ISO/IEC 30107-1:2016

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. Source: TDIF defined term.

Multi-factor Authentication – An authentication protocol that relies on more than one authentication factor for successful authentication. Source: TDIF defined term.

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 a person knows or something a person is). Source: TDIF defined term.

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 a person knows or something a person is). Source: TDIF defined term.

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. Source: TDIF defined term.

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 a person knows or something a person 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 a person, proving possession and control of the device. Source: TDIF defined term.

Non-Person Entity (NPE) – An entity with a digital identity that acts in the digital environment, but is not a human actor. This can include organisations, hardware devices, software applications, and information artefacts. Source: NIST

One-Time Password (OTP) – is a password that is changed each time it is required. Source: TDIF defined term.

Operating Rules – set out the legal framework for the operation of the identity federation, including key rights, obligations and liabilities of participants.

Oversight Authority – the entity responsible for the administration and oversight of the identity federation in accordance with the Operating Rules and TDIF.

Out-of-Band Device – is a physical device that uses an alternative channel for transmitting information – e.g. an SMS to send a PIN or one-time password. Source: TDIF defined term.

National e-Authentication Framework (NeAF). The NeAF applies a risk-based approach to identify and authenticate people to a desired level of assurance for online interactions. Source: NeAF.

National Identity Proofing Guidelines (NIPGs). The Council of Australian Government's national guidelines for identity proofing. Source: CoAG

Participant. Any person or legal entity that participates in the Identity eco-system or an identity transaction using this system. Participants include Users, Applicants, Accredited Providers and Relying Parties. Source: TDIF defined term.

Person – An entity with a digital identity that acts in the digital environment and is a human actor. May also be referred to as an individual. Source: TDIF defined term.

Personnel. Any member of an agency's staff or contracted service provider's staff used to service agency contracts, or other people who provide services to the agency or access agency information or assets as part of agency sharing initiatives. Source: PSPF.

Photo ID. Photographic Identification (Photo ID). A trusted credential:

- with core attributes that are verifiable to an Authoritative Source, and
- that includes a facial image of the credential holder that is verifiable to an Authoritative Source.

Source: TDIF defined term.

Presentation attack. Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system. A Presentation attack can be implemented through a number of methods, e.g. artefact, mutilations, replay, etc. Presentation attacks may have a number of goals, e.g. impersonation or not being recognized. Biometric systems may not be able to differentiate between biometric presentation attacks with the goal of interfering with the systems operation and non-conformant presentations. Source: ISO/IEC 30107-1:2016.

Privacy audit criteria is the criteria against which a privacy audit is evaluated. Source: TDIF defined term.

Privacy audit objective is the objective of the privacy audit. Source: TDIF defined term.

Privacy audit scope are the Applicant's activities that will and will not be subject to the privacy audit. Source: TDIF defined term.

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 people, and sets out recommendations for managing, minimising or eliminating that impact. Source: OAIC.

Protective Security Documentation. 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*. Source: TDIF defined term.

Public Key Infrastructure. The combination of hardware, software, people, policies and procedures needed to create, manage, store and distribute Keys and Certificates based on public Key cryptography. Source: Gatekeeper.

RBDMs. Registries of Births, Deaths and Marriages maintained by the Australian States and Territories.

Relying Party. An organisation or government agency that relies on verified identity information, attributes or assertions provided by identity service providers and attribute providers through an identity exchange to enable the provision of a digital service. Source: TDIF defined term.

Repudiation. A denial by a Legal Entity that an act attributed to them was performed by them. Examples of such an act include an Assertion, a declaration and a transaction. Source: NeAF

Requirements Traceability Matrix (RTM) captures the output from requirements tracing, a process of documenting the links between the requirements and the Test Cases developed to verify and validate those requirements (see Verification and Validation). Source: the field of software engineering.

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. Source: ISO 31000.

Risk-based Testing, testing in which the management, control, priority is based upon the Risk Rating assigned to the requirement. Source: TDIF defined term.

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. Source: ISO 31000.

Risk assessment. The process of risk identification, risk analysis and risk evaluation. Source: ISO 31000.

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. Source: ISO 31000

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. Source: ISO 31000.

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. Source: ISO 31000.

Risk tolerance. The levels of risk taking that are acceptable in order to achieve a specific objective or manage a category of risk. Source: ISO 31000.

RTA. Road traffic and transport agencies. Source: AustRoads.

Serious and complex fraud. 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. Source: Commonwealth Fraud Control Policy.

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. Source: ISO 31000.

Service Operations Testing are the testing process that covers the testing required to validate that the testable aspects of operating an In-Service (Production) system demonstrate conformance to the Service Operations' requirements. Source: TDIF defined term.

Session. Once authentication has taken place a session may be established to allow a person to continue accessing the service across multiple subsequent interactions without requiring repeated authentication. Source: TDIF defined term.

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. Source: TDIF defined term.

Sighting. The examination of a document by a trained operator to confirm the accuracy of the information presented. Source: TDIF defined term.

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

Single-factor Cryptographic (software). A cryptographic key stored in some form of 'soft' media. Authentication is accomplished by proving possession and control of the key. Source: NeAF.

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 a person. Source: NeAF

Source Verification. The act of verifying identity attributes and information with an Authoritative Source**.** Source: TDIF defined term.

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. Source: TDIF defined term.

System testing is a way of validating systems through executing the User Flows, User Interactions and Component Interactions to ensure that the system has all the required functionality specified in the TDIF. Source: TDIF defined term.

TDIF. See Trusted Digital Identity Framework (TDIF).

Technical Integration Testing is a testing process used to validate the conformance to Technical Integration requirements included in the Trust Framework technical profiles. Source: TDIF defined term.

Technical Verification. The act of verifying documentation using a cryptographically secure technical mechanism of the document, such as a secure chip or a pdf document signature. Source: TDIF defined term.

Test Artefacts, the products developed in the different phases of the testing life cycle are known as Test Artefacts. These may be electronic documents or output from a Test Tool. Source: TDIF defined term.

Test Case, documents preconditions (including test data), expected results and post conditions, developed for a particular test scenario in order to verify compliance against a specific requirement. Source: TDIF defined term.

Test Condition, a testable aspect of a feature, requirement or attribute Source: TDIF defined term.

Test Sets, a group of Test Cases that belong to specific tasks or feature, or where there is some other reason for the Test Cases to be executed at the same time. Source: TDIF defined term.

Test Tool, a test management tool is software used to manage tests (automated or manual). Source: TDIF defined term.

Trust Framework is a generic term often used to describe a legally enforceable set of specifications, rules and agreements that govern a multi-party system established for a common purpose, designed for conducing specific types of transactions among a community of participants, and bound by a common set of requirements. Source: OIX

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. Source: TDIF defined term.

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. Source: TDIF defined term.

Trusted Device. A device for facilitating authentication that a person controls and that is enrolled as part of the creation of the credential. Source: TDIF defined term.

Trusted Digital Identity Framework (TDIF). 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. Source: TDIF defined term.

Trusted Referee. A trusted referee is a person or organisation that holds a position of trust in the community and does not have a conflict of interest, such as an Aboriginal elder or reputable organisation that the person is a customer, employee or contractor of, and is known and listed by the enrolling agency to perform the function of a referee. The Statutory Declarations Act 1959 provides a list of people who hold a position of trust in the community. Similar lists are also generally included in state and territory legislation. Trusted referees may also include guardians or other people nominated to act on a person's behalf whose identities have been verified. Source: NIPGs.

Unique in context. A digital identity is created with a unique combination of legitimate personal and contact information. Different combinations of personal and contact information can be used to create additional digital identities, each unique within the IdP's system. This enables people – if they choose to do so – to establish one or multiple digital identities with one or multiple IdPs.

Note: IdPs may choose to implement their service in a manner that prevents the IdP itself from accessing the person's personal or contact information or the digital identity, except when this information has been unlocked by the person. Under these circumstances the IdP will not know which combinations of personal and contact information have been used to create a digital identity. Therefore, in these instances 'unique in context' can also refer to the individually encrypted records held by the IdP. Source: TDIF defined term.

Use in the Community (UitC) document. 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). Source: TDIF defined term.

User. A person who uses the identity service in order to access a Relying Party service. (e.g. the general public). Source: TDIF defined term.

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. Source: TDIF defined term.

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

Validation (in an identity proofing context). A check that the attribute exists and is under the control of the individual. (e.g. SMS activation code being sent to a mobile phone number to confirm control of the associated phone number). Source: TDIF defined term.

Validation (in an integration testing context) is oriented towards testing a system under controlled conditions providing evidence that the system, satisfy Trust Framework requirements and satisfy intended use and user needs. Validation involves testing that functionality works as specified, designed and constructed, including intentionally making things go wrong when they should not and things happen when they should not [testing boundary conditions] to ensure that the system is robust when in production. TDIF defined term.

Verification (in an integration testing context) provides confirmation, through the provision of objective evidence, that Trust Framework requirements have been fulfilled. Verification involves the evaluation of whether or not a system complies with a regulation, requirement, specification, or imposed condition. TDIF defined term.

White box system testing. A security testing and examination technique performed by a protective security specialist. White box techniques involve direct analysis of an application's source code. White box techniques are generally more efficient and

cost-effective for finding security defects in custom applicants than black box techniques. Source: NIST SP 800-115.

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