Trusted Digital Identity Framework

Structure and Overview
(document 1 of 14)

Version 0.02
PUBLIC CONSULTATION DRAFT

dta.gov.au
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Management</td>
<td>3</td>
</tr>
<tr>
<td>Endorsement</td>
<td>3</td>
</tr>
<tr>
<td>Change log</td>
<td>3</td>
</tr>
<tr>
<td>Scope of this document</td>
<td>3</td>
</tr>
<tr>
<td>Intended audience</td>
<td>3</td>
</tr>
<tr>
<td>Conventions</td>
<td>3</td>
</tr>
<tr>
<td>Terms and their meaning</td>
<td>4</td>
</tr>
<tr>
<td>Context</td>
<td>4</td>
</tr>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Trust Framework Characteristics</td>
<td>6</td>
</tr>
<tr>
<td>Trusted Digital Identity Framework</td>
<td>6</td>
</tr>
<tr>
<td>Governance Framework</td>
<td>9</td>
</tr>
<tr>
<td>Accreditation</td>
<td>10</td>
</tr>
</tbody>
</table>

---

Digital Transformation Agency – Trusted Digital Identity Framework Structure and Overview
Public Consultation Draft

2
# Document Management

## Endorsement

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

<table>
<thead>
<tr>
<th>Group</th>
<th>Version</th>
<th>Endorsement Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Director, Trusted Digital Identity Framework</td>
<td>0.02</td>
<td>20 Sept 2017</td>
</tr>
</tbody>
</table>

## Change log

This is version 0.2 of the *Trusted Digital Identity Framework: Structure and Overview*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.01</td>
<td>Jul 17</td>
<td>DA &amp; DR</td>
<td>Initial draft</td>
</tr>
<tr>
<td>0.02</td>
<td>Sep 17</td>
<td>SJP</td>
<td>Minor updates to support the public consultation draft</td>
</tr>
</tbody>
</table>

## Scope of this document

This document provides a high level overview of the Trusted Digital Identity Framework - its structure and the relationships between the different policy components of the Framework.

## Intended audience

The intended audience for this document is senior executives in all organisations and agencies participating or seeking to participate in the national identity federation. The document should also be read by organisations and individuals undertaking privacy and security evaluations and audits.

## Conventions

The following terms and their meaning used within the Trust Framework documents and are taken from Request for Comments 2119 (RFC2119), ‘Keywords for use in RFCs to Indicate Requirements Levels’.

- **MUST** means an absolute requirement of this document.
- **SHOULD** means that there may exist valid reasons in particular circumstances to ignore a particular item of this document, but the full implications need to be understood and before choosing a different course.
- **MUST NOT** means an absolute prohibition of this document.
**Terms and their meaning**

Key terms used in this document are listed below. All terms used in the Trusted Digital Identity Framework are also defined in the *Trust Framework: Glossary of Terms.*

- **Applicants** are organisations and government agencies that undergo the Trust Framework Accreditation Process as either an:
  - Identity Service Provider,
  - Credential Service Provider,
  - Identity Exchange, or
  - A combination of the above.

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

- **Credential Service Provider** is an entity that undergoes the Trust Framework Accreditation Process. They generate and manage authentication credentials which are provided to individuals. This function may be internalised within an Identity Service Provider.

- **Identity Exchange** is an entity that undergoes the Trust Framework Accreditation Process. This entity conveys, manages and coordinates 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 Service Provider** is an entity that undergoes 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.

- **Relying Party** is an entity that relies on verified identity information and assertions provided by an Identity Service Provider (or a Credential Service Provider) through an Identity Exchange to enable the provision of a digital service.

**Context**

The Digital Transformation Agency (DTA), in collaboration with other government agencies and key private sector bodies, is leading the development of a national federated identity ‘eco-system’ (the ‘identity federation’). Implementation and operation of the identity federation is underpinned by the Trusted Digital Identity Framework (‘Trust Framework’).

The Trust Framework 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 protective security, privacy, accessibility, usability, risk management, fraud control, technical integration and service operations.

**Introduction**

Traditional identity systems have often been based on a network 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 approach provides an efficient and scalable approach that readily facilitates the operation of federated style identity systems.

A “trust framework” describes a legally enforceable and agreed set of specifications, rules, and agreements for the governance of a federated style identity system. Trust frameworks therefore enable all participants (including end users) to have confidence in the key components of identity verification and authentication and the security and privacy of people’s personal information.

The United Nations Commission on International Trade Law (UNCITRAL) 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.”

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 provider.

The Report of the Inquiry into Australia’s Financial System (the Murray Report) was released on 7 December 2014 and recommended the development of “a national strategy for a federated-style model of trusted digital identities.” The Report noted:

> “A national strategy based on a federated-style model best balances the attainment of network benefits with ongoing innovation in digital identity solutions, contributing to overall financial system efficiency. It draws on the strengths of the public and private sectors and facilitates the best use of technology. It enhances consumer choice and convenience and, with appropriate design, could enhance privacy and security.”

---

1 The term “trust framework” can be read as synonymous with terms such as “system rules,” “scheme rules,” “operating regulations,” or “common operating rules.”


Trust Framework Characteristics

**Scope**: a trust framework specific to an Australian identity federation.

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

- **Risk Management**: 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 the broader Australian legislative and regulatory environment;
- **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 (if any) necessary to maintain the identity federation and the participant roles of those that engage in identity transactions within the 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.

**Enforceable**: 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.

**Trusted Digital Identity Framework**

The Australian Government is firmly committed to the development of a national, federated style identity system as shown in Figure 1 below.
The Trust Framework adopts a risk-based approach to identity verification and authentication using commonly understood and accepted terminology. This approach is consistent with existing national and international standards and frameworks.

Consistent with the OIX Paper “Trust Frameworks for Identity Systems” published in June 2017 the Trust Framework addresses the following functional responsibilities:

- **Governance and Policy Development**: Developing and amending policies; decision making; stakeholder-facilitation; managing standards and procedures; accountability mechanisms.
- **Policy Enforcement**: Ensuring compliance with Trust Framework standards and requirements; enforcement 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 identity eco-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 Open Identity Exchange (OIX) is a leading industry NFP, driving digital identity industry. See www.openidentityexchange.org
As per Figure 2 above, the Trust Framework includes a number of documents which define minimum requirements (the rules) and recommended approaches (the tools) as follows. The items marked with a (TBD) will be developed in the coming months:

**Governance**
- Trust Framework Overview (this document)
- Federation Governance Model (TBD)
- Federation Agreement/MOU/MOA (TBD)
- Trust Framework Accreditation Process
- Trust Framework Glossary of Terms

**Assessment and Compliance**
- Privacy Assessment
- InfoSec Registered Assessor Program (IRAP) Assessment
- Interface and User Experience Testing Assessment
- Annual Compliance Assessment (TBD)

**Core Requirements**
- Core Privacy Requirements
- Core Security Requirements
- Core User Experience Requirements
- Core Risk Management Requirements
- Core Identity Fraud Control Requirements
Standards

- Digital Identity Verification Standard
- Digital Authentication Credential Standard
- Non-Digital Identity Verification Standard (TBD)
- OpenID Connect Profiles (TBD)
- SAML 2.0 Profiles (TBD)
- Business Identity Verification Standard (TBD)
- Business Authentication Credential Standard (TBD)

Guides

- Information Security Documentation Guide
- Penetration Testing Guide (TBD)
- Risk Management Guide
- Identity Fraud Control Guide (TBD)
- Integration Testing Guide (TBD)
- Service Operations Guide (TBD)
- Authority Management Guide (TBD)

Support

- Tools, checklists, etc

**Governance Framework**

Central to the successful implementation of the identity federation is an effective and representative governance framework.

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 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, the Identity Exchange, Identity Service 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;
- a low risk of failure and alternatives in case of failure or exit of one or more Identity Service Providers;
- transparency and accountability to government and all participants; and
- stability/predictability to protect significant investments by Identity Service Providers, Credential Service Providers and Relying Parties.

The Framework accommodates the following entities / roles and functions:

- Accredited Identity Service Providers that undertake the function of verifying the identity of end-users. Identity Service Providers may also issue authentication credentials to end users.
The Framework also supports independent accredited Credential Service Providers.

- An Identity Exchange - also referred to as a hub or trust broker. The Identity Exchange will function in double-blind mode\(^5\). The Identity Exchange must operate independently from all Identity Service Providers and Credential Service Providers and any other state and territory government or private sector Identity Exchanges.

- Multiple 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).

The Trust Framework Standards and Core Requirements establish the agreed criteria against which all accredited entities must operate.

The Framework envisions 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\(^6\)).

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 etc. The governance body will also operate as the Trust Framework Accreditation Authority\(^7\) - responsible for decisions in relation to the initial accreditation of Identity Service Providers, Credential Service Providers and Identity Exchanges, as well as the on-going 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 nonetheless 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.

**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 interoperability and service operations. Progress through the accreditation process is managed by a

\(^5\) In this model IdPs have no knowledge of which service an end-user is seeking to access and Relying Parties have no knowledge of which IdP was used to verify the person’s identity. The Exchange will only hold relevant meta-data for audit purposes.


\(^7\) 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.
series of decision gates. The decision gates are used by the Trust Framework Accreditation Authority to evaluate the Applicant’s progress towards accreditation.

**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:
  - Trust Framework: Accreditation Process
- compliant with the Trust Framework requirements set out in:
  - Trust Framework: Core Privacy Requirements
  - Trust Framework: Core Protective Security Requirements
  - Trust Framework: Core User Experience Requirements
  - Trust Framework: Core Risk Management Requirements
  - Trust Framework: Core Identity Fraud Control Requirements
  - Trust Framework: Digital Identity Verification Standard
  - Trust Framework: Digital Authentication Credential Standard
  - Trust Framework: Integration Testing
  - Trust Framework: SAML 2.0 Profile
  - Trust Framework: OpenID Connect Profile
- Trust Framework: Service Operations Testing
- Able to pass independent assessments in accordance with:
○ Trust Framework: Information Security Registered Assessors Program (IRAP) Assessment
○ Trust Framework: Privacy Assessment
○ Trust Framework: Annual Compliance Assessment

Applicants should consider the guidance material:
○ Trust Framework: Penetration Testing Guide
○ Trust Framework: Risk Management Guide
○ Trust Framework: Identity Fraud Control Guide

Through the coverage of each of the elements of the Trust Framework, the accreditation process within the broader governance framework provides the mechanism to draw the Trust Framework together as a coherent whole.