Trusted Digital Identity Framework

Core Fraud Control Requirements
(document 10 of 14)

version 0.2

PUBLIC CONSULTATION DRAFT

dta.gov.au
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 Sep 2017</td>
</tr>
</tbody>
</table>

Change log

This is version 0.1 of the Trust Framework: Core Fraud Control Requirements.

<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>Aug 17</td>
<td>PH</td>
<td>Initial draft</td>
</tr>
<tr>
<td>0.02</td>
<td>Sep 17</td>
<td>PH</td>
<td>Minor changes to support public consultation draft</td>
</tr>
</tbody>
</table>

Conventions

The following terms and their meaning 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.
- **SHOULD NOT** means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- **MAY** means that an item is truly optional.
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.

- **Australian Institute of Criminology (AIC)** - Australia’s national research and knowledge centre on crime and justice

- **Credential Service Provider (CSP)** 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.

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

- **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 (IdP)** 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.

- **Serious and complex fraud** is fraud which due to its size or nature, is too complex for Accredited Providers to investigate. Complex fraud may involve collusion between officials and external parties.
Scope of this document

This document lists the Core Fraud Control Requirements (CFCRs) of the Trusted Digital Identity Framework (Trust Framework).

These CFCRs apply to participants when functioning as an accredited Identity Service Provider of the identity federation under the Trust Framework. For example, this document applies to an organisation that is an Identity Service Provider but it does not apply to the other functions (e.g. banking, postal) carried out by that organisation.

This version of the Core Fraud Control Requirements is focussed on Commonwealth agencies. Future versions of the document will also contain requirements for agencies at State and Territory level and non-government entities.

Intended audience

The intended audience for this document includes:

- Applicants
- Accredited Providers
- The Trust Framework Accreditation Authority
- Relying Parties.

Relationship to other documents

Figure 1: Trust Framework document hierarchy and relationships
As per Figure 1 above, the Trust Framework includes a number of documents which define minimum requirements (the rules) and recommended approaches (the tools). The Core Requirements are a subset of the rules and define specific privacy, security, user experience, risk management and fraud control requirements to be met by Applicants and Accredited Providers. The core requirements are informed by compliance assessments and standards, and are supported by a series of guides.

This document should be read in conjunction with the:

- **Trust Framework: Fraud Control Guide**, which provides guidance relating to the implementation of the Core Fraud Control Requirements.
- **Trust Framework: Structure and Overview**, which provides a high level overview of the Trust Framework including the structure and relationship between the various components.
- **Trust Framework: Accreditation Process**, which defines the requirements to be met by Applicants in order to achieve Trust Framework accreditation.
- **Trust Framework: Core Security Requirements**, which sets out requirements for maintaining secure identity services.
- **Trust Framework: Core Risk Management Requirements**, which sets out the risk management responsibilities of Applicants and Accredited Providers.
- **Trust Framework: Core Privacy Requirements**, which sets out requirements for maintaining user privacy.
- **Trust Framework: Digital Authentication Credential Standard**, which sets out requirements relating to authentication credentials.
- **Trust Framework: Digital Identity Verification Standard**, which sets out requirements relating to the verification of an individual’s identity.

### 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 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.

These CFCRs define the Fraud control responsibilities for Accredited Providers to meet their accreditation obligations under the Trust Framework, which aligns with the requirements of existing National Legislation and guidance regarding Fraud Control including section 10 of the Public Governance Performance and Accountability Rule.

These CFCRs are underpinned by the following guiding fraud control principles:
1. Preventing Fraud
2. Detecting Fraud
3. Reporting Fraud
4. Investigating Fraud
5. Fraud Victim Support

Fraud Control Responsibilities

The table below identifies the responsibilities of entities in the Trust Framework

Note: There are mandatory compliance obligations for Fraud controls for IdPs, CSPs and the Exchange.

Table 1: Fraud control responsibilities

<table>
<thead>
<tr>
<th>Who</th>
<th>Responsibility</th>
</tr>
</thead>
</table>
| Identity Service Providers and Credential Service Providers | • Collects, verifies and stores appropriate user information  
• Ensures that information collected is accurate and up to date.  
• Issues digital identities and authentication credentials  
• When authorised by the user, enables verification of digital identity with relying party  
• Provides fraud reporting channels to users, Relying Parties and appropriate law enforcement agencies  
• Advises exchange of fraud-related transactions within the IdP  
• Investigates reports of identity fraud within its user base  
• Maintains records of identity fraud within its user base  
• Assists victims of digital identity theft to regain control of their digital identity |
| Exchange                                  | • Ensure the anonymity of the user within the identity eco-system  
• Advise Identity Service Providers of fraud-related transactions reported by the relying party  
• Advise Relying party of fraud-related transactions reported by the IdP and CP |
| Relying Party                             | • Verify user identity using services provided by the accredited provider  
• Ensure where necessary through their own means of information collection, that enrolling users are unique in the context of their system  
• Collect user information relating to determining eligibility for Relying Party Purposes.  
• Detect and Report Identity fraud and credential fraud-related transactions to the Exchange |
| User                                     | • Provide accurate identity information  
• Correct or update identity information with Document Issuers as identity information such as name changes  
• Does not share user name, password and other identity information with a third parties  
• Report unauthorised use of their digital Identity or authentication credential to both the Accredited Provider and the Relying Party as soon as they become aware of it. |
While effective fraud control requires the commitment of all officials, contractors and third-party providers and users of a service, the primary responsibility for fraud control rests with Accredited Providers.

Accredited Providers **MUST**:

- conduct fraud risk assessments annually, when there is a substantial change in their structure, functions or activities AND when there are significant changes in technological capabilities which impacts on the service or services provided. Further information on Risks that MUST be considered are listed at Annex A: Potential Sources of Risk, in the Trust Framework Core Risk Management Requirements.
- develop and implement a fraud control plan that clearly delineates between process based and technological risks as soon as practicable after conducting a risk assessment.
- ensure that identified fraud control arrangements are in place.
- develop governance that promotes the proper use and management of identity and related information, functions and the financial sustainability of their processes.
- Store and protect information in accordance with the Trust Framework Core Privacy Requirements and the Trust Framework Core Security Requirements.
- establish and maintain an appropriate system of fraud risk oversight and management for each Trust Framework-related identity service as described in the Trust Framework Risk Management Guide.
- Provide an appropriate system of internal controls, including implementation measures directed at officials and third party service providers in accordance with the Trust Framework Core Privacy Requirements and the Trust Framework Core Protective Security Requirements.
- not improperly use their position or the information they have access to.

**Fraud Prevention**

Accredited Providers **MUST**:

- have in place appropriate mechanisms for preventing fraud, ensuring that:
  - their officials are made aware of what constitutes fraud for the Applicant service; and
  - the risk of fraud is taken into account in accordance with the Sources of Risk tables at Annex A of the Trust Framework Core Risk Requirements;
  - document instructions and procedures to assist officials to prevent, detect and deal with fraud;
- conduct vetting of officials and systems as described in the Core Protective Security Requirements.

**Aptitude and Training**

Accredited Providers **MUST** ensure that all officials and third party service providers undertaking facial recognition and matching tasks have undertaken and passed:
● a range of facial recognition aptitude testing provided by recognised and reputable tertiary institutions recognised by the Trust Framework Accreditation Authority.
● Facial recognition and matching training and elearning approved by the Attorney General’s Department

Accredited Providers **MUST**:

● ensure officials primarily engaged in fraud control activities possess or attain relevant qualifications or training to effectively carry out their duties;
● use fraud information gathered to update and tighten security and fraud control capabilities based on fraud incidents, investigations, reports and analytical data.

Identity Service Providers **MUST** conduct identity proofing as required by the Trust Framework Identity Proofing Standard.

Credential Providers **MUST** meet the requirements of the Trust Framework Authentication Credential Standard.

The Exchange **MUST** protect information passed through it in accordance with the Trust Framework Core Privacy Requirements and the Trust Framework Core Security Requirements.

**Fraud Detection**

Fraud may be detected at a number of touchpoints throughout the identity life-cycle. The greatest opportunity to detect fraud arises during the initial enrollment of an individual with an IdP or through reporting by Relying Parties and Users

Accredited Providers **MUST** have in place appropriate mechanisms for detecting incidents of fraud or suspected fraud, including a process for officials of the IdP and other persons to report suspected fraud confidentially.

Where a suspected fraud incident is detected by or reported to an Accredited Provider, it **MUST** be assessed, actioned and the appropriate stakeholders notified as soon as possible.

**Fraud Investigation**

Accredited Providers are responsible for investigating instances of fraud or suspected fraud against it that are not serious or complex. This includes the investigating disciplinary matters, unless the matter is referred to and accepted by the Australian Federal Police (AFP) or another law enforcement agency. Accredited Providers **MAY** seek guidance on the criteria for serious and complex crimes from the AFP.

Accredited Providers **MUST**:

● have in place appropriate mechanisms for investigating or otherwise dealing with incidents of fraud or suspected fraud including appropriately trained and skilled identity fraud investigation
staff or service providers; This training should include protocols and training to ensure the safety of staff conducting investigations.

- have in place investigation and referral processes and procedures that are consistent with the Australian Government Investigations Standards (AGIS).
- resolve fraud matters in accordance with relevant internal and external requirements where a law enforcement agency has declined a referral.
- document decision criteria at critical stages in managing a suspected fraud incident.
- resolve fraud investigations when they occur and advise stakeholders (particularly affected individuals, TDIF exchanges and identity providers) of the investigation outcome.
- appropriately document decisions to use civil, administrative or disciplinary procedures, or to take no further action in response to a suspected fraud incident.

The acts and policies which set out requirements for entities conducting investigations include the Crimes Act, the Freedom of Information Act 1982, Privacy Act 1988, Archives Act 1983, Prosecution Policy of the Commonwealth, the Protective Security Policy Framework and the Fraud Control Framework 2017. Accredited providers MUST ensure that they are aware of their roles and responsibilities under these acts and policies in addition to Trust Framework requirements.

If criminal activity is identified in an investigation the Accredited Provider MUST notify the affected parties where allowable, ensuring that no information is shared inappropriately.

**Fraud Reporting**

Where a Fraud is found to have occurred, Accredited Providers MUST:

- have an appropriate mechanism for recording and reporting incidents of fraud or suspected fraud.
- Follow the fraud reporting requirements in AGD's Commonwealth Fraud Control Framework 2017.
- conduct Fraud reporting as required in annual compliance audits.

Where an investigation discloses potential criminal activity involving another entity’s activities or programs, Applicants and Accredited Providers MUST report the matter to that entity to the extent possible subject to relevant requirements of any Australian law.

**Fraud Victim Support**

Accredited Providers MUST:

- have in place processes and services including online, face to face and telephone services, to assist users whose identities or authentication credentials have been compromised.
- Lock a user account when fraud has been reported.
- Ensure that identities are re-proofed when a fraud victim is identified.
References

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

<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Crimes Act 1914</td>
</tr>
<tr>
<td>5.</td>
<td>Criminal Code 1995</td>
</tr>
<tr>
<td>6.</td>
<td>Public Service Act 1999</td>
</tr>
<tr>
<td>8.</td>
<td>Australian Government Investigations Standards</td>
</tr>
</tbody>
</table>