Trusted Digital Identity Framework

Core Privacy Requirements
(document 6 of 14)

version 0.4
PUBLIC CONSULTATION DRAFT

dta.gov.au
Contents

Document Management 3
Endorsement 3
Change log 3
Conventions 4
Scope of this document 4
Terms and their meaning 4
Intended audience 5
Relationship to other documents 5
Introduction 6

Core Privacy Requirements 7
General privacy requirements 7
Applicant responsibilities 7
Privacy governance 7
Privacy Impact Assessment 8
Data Breach Response Management 9
Privacy Policy 9
Notice of Collection 10
Collection and use limitation 10
  Identity Service Provider additional requirements 11
  Identity Exchange additional requirements 11
Consent 11
  Identity Service Provider additional requirements 12
Cross border and contractor disclosure 12
Government Identifiers 13
Access, correction and dashboard 13
  Identity Service Provider additional requirements 13
  Identity Exchange additional requirements 13
Quality of personal information 14
  Identity Service Provider additional requirements 14
Handling Privacy Complaints 14
Destruction and de-identification 14
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>0.4</td>
<td>20 September 2017</td>
</tr>
</tbody>
</table>

Change log

This is version 0.4 of the Trust Framework: Core Privacy 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>Mar 17</td>
<td>JS &amp; DA</td>
<td>Initial version</td>
</tr>
<tr>
<td>0.02</td>
<td>May 17</td>
<td>JS</td>
<td>Updates based on feedback from privacy stakeholders and internal feedback. Updates include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Changed headings and restructure of the order of content</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Requirements regarding opting into coverage of Privacy Act</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Addition of section on cross border and contractor disclosure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Refinement to sections on reporting data breaches, definition of personal information, use and disclosure, consent, Privacy Impact Assessments and government identifiers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Aligning Governance requirements to announcements about Australian Public Service Privacy Code</td>
</tr>
<tr>
<td>0.03</td>
<td>July 17</td>
<td>SJP</td>
<td>Minor updates to align with other Trust Framework documents</td>
</tr>
<tr>
<td>0.04</td>
<td>Sept 17</td>
<td>JS &amp; SJP</td>
<td>Removed annex regarding relying party obligations as that will be addressed in another document Removal of list of metadata retained by the exchange Removal of age of 15 as minimum for a digital identity as that will be covered by guidance and requirements for informed consent Removal of blanket requirement for identity service providers not to use personal information other than through the exchange Minor updates to support the 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.
- **MAY** means that an item is truly optional.

Scope of this document

This document lists the Core Privacy Requirements (CPRs) of the Trusted Digital Identity Framework (Trust Framework).

These CPRs apply to Applicants when functioning in their role in the identity federation (for example as Identity Provider or Credential Provider) but not its broader activity. For example, the CPRs will apply to a bank or postal company if it operates as an Identity Service Provider but it does not apply to the other functions such as post or banking.

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.

### 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: 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 User Experience Requirements, which sets out the requirements for usability and accessibility.
- Trust Framework: Core Risk Management Requirements, which sets out the risk management responsibilities of Applicants and Accredited Providers.
- Trust Framework: Core Fraud Control Requirements, which sets out requirements for fraud control.
- 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 CPRs are designed to apply whether an Applicant or Accredited Provider operates within the jurisdiction of the Privacy Act 1988 (Cth) (Privacy Act), state privacy legislation or not covered by privacy law. These CPRs rely heavily on the Australian Privacy Principles and other provisions in the Privacy Act but are intended to be more specific and provide the highest standard across Australian and state government privacy legislation.
Core Privacy Requirements

General privacy requirements

The Identity Exchange **MUST** be a separate entity\(^1\) from other identity federation participants and **MUST** establish and maintain its own privacy management arrangements.

If the Identity Service Provider is a small business operator as defined by the Privacy Act, and therefore exempt from the Privacy Act, it **MUST** opt-in to coverage of the Privacy Act. Any state government Identity Service Provider not covered by state privacy laws **MUST** comply with Australian Privacy Principles for the purpose of achieving Trust Framework accreditation.

The Identity Exchange and Identity Service Provider **MUST** protect the greater subset of:

- ‘personal information’ as defined by the Privacy Act
- information about an individual who has been dead for no more than 30 years
- personal information as defined by a relevant state jurisdiction where the Identity Service Provider is a state government agency
- the metadata created from the identity attributes collected by an Identity Exchange.

Applicant responsibilities

The following privacy responsibilities apply to all Applicants, unless explicitly stated otherwise.

Privacy governance

The Applicant **MUST**:

- appoint key roles and responsibilities for privacy management, including:
  - a senior official or ‘Privacy Champion’ with overall responsibility and accountability for privacy
  - a dedicated privacy contact officer responsible for handling internal and external privacy enquiries, complaints, and access and correction requests
  - ensuring that the privacy management function is adequately resourced.
    - The Privacy Officer and senior official **SHOULD** be separate individuals.
- include privacy training and awareness sessions in induction and regular staff training programs (including for short term staff, service providers and contractors).
  - These sessions **MUST** include information on privacy responsibilities of the Applicant in the context of the Trust Framework and its obligations under this document.
- develop and maintain a Privacy Management Plan that aligns business processes with these CPRs, including documented policies and processes:
  - for receiving and responding to privacy enquiries and complaints

\(^1\) For the purpose of this document entity means an Applicant.
○ for the assessment of unsolicited information as it arrives to ensure that, if the Identity Service Provider could not have collected the information itself, the information is destroyed
○ to allow individuals to promptly and easily access and correct their personal information
○ about what information the Applicant holds.

- document its compliance with these CPRs, including keeping records (consistent with relevant state or commonwealth government Archive Act requirements) on privacy process reviews, audits, breaches and complaints

- ensure that senior management and those with responsibility for privacy management are regularly briefed on privacy risks and issues identified in reviews and audits

- implement, as part of the broader Security Risk Management Plan, risk management processes to identify, assess and manage privacy risks across the organisation, including personal information security risks

- conduct regular (at least annual) privacy audits to ensure that privacy policies and practices are being implemented appropriately.

- notify the Trust Framework Accreditation Authority in writing and allow them to comment before changing a practice and procedure governed by the Trust Framework.

### Privacy Impact Assessment

The Applicant **MUST**:

- commission a PIA, by an independent and qualified assessor, when applying to join the Trust Framework
- undertake a PIA for each business project or corporate decision that involves new or changed personal information handling practices (including implementing new technologies)
- respond in writing, at a senior management level, to the recommendations outlined in the PIA including whether the recommendations are accepted, the reasons for any non-acceptance and the timeframe for implementation of the recommendations
- ensure that the recommendations are implemented in the timeframe specified
- keep a register of all PIAs conducted
- Provide a copy of the PIA to the Trust Framework Accreditation Authority.

A PIA **MUST** at a minimum:

- be conducted by a qualified assessor
- be in writing
- be conducted early enough to influence the design of a project or decision
- consult with relevant stakeholders
- include a description of the proposed project
- map the project’s information flows
- include an analysis of:
  ○ risks of non compliance with the law
  ○ whether privacy impacts are necessary or avoidable
  ○ the impact of the project on individuals
  ○ possible mitigation of risks

---

● provide recommendations
● be made public unless that would unreasonably reveal commercial secrets or undermine security.  

**Data Breach Response Management**

The Applicant **MUST:**

● have a documented Data Breach Response Plan and Data Breach Policy (see below)
● report serious data breaches to:
  ○ affected individual(s)
  ○ the Office of the Australian Information Commissioner
  ○ the Trust Framework Accreditation Authority, and
  ○ the Australian Signals Directorate.

A data breach must be reported if it is likely to result in serious harm to any of the individuals to whom the information relates as defined in section 26WE of the Privacy Act.

The information reported in a data breach, and the timeframe for reporting, **MUST** be consistent with the data breach reporting requirements in the Privacy Act.

The Data Breach Response Plan is a tool to help an organisation prepare for a data breach. It **MUST**, at a minimum, include:

● the actions to be taken if a breach is suspected, discovered or reported by a staff member, including a clear communications plan and information about when it is to be escalated to the data breach response team (response team)
● the members of the response team
● the actions the response team is expected to take
● information about how the actions and roles in the plan relates to the organisation’s Incident Response Plan.

A Data Breach Policy, or a similar document, **MUST** provide:

● a clear explanation of what constitutes a data breach
● more detailed steps and considerations for responding to an incident than the Data Breach Response Plan
● details about training relating to data breaches
● details about how data breaches are logged.

**Privacy Policy**

---

4 Or relevant state regulator
6 Or any relevant state government law or voluntary scheme.
8 See the Trust Framework: Information Security Documentation Guide for further information in developing an Incident Response Plan
The Applicant **MUST** publish a clearly expressed and up to date Privacy Policy\(^{10}\) about the management of personal information which **MUST** contain:

- the kinds of personal information that the entity collects and holds
- how the entity collects and holds personal information
- the purposes for which the entity collects, holds, uses and discloses personal information
- how an individual may access personal information about the individual that is held by the entity and seek the correction of such information
- how an individual may complain about a breach of the APPs\(^{11}\), registered code, and how the entity will deal with such a complaint
- whether the entity is likely to disclose personal information to overseas recipients and if so the countries in which such recipients are likely to be located (if it is practicable to do so).

### Notice of Collection

The Applicant **MUST** notify users of the following at the time the individual enrols for the first time and again when individuals log in to the service to manage their identities or make an enquiry:

- its identity and contact details
- any collections from third parties
- where relevant, that a collection is required by law and the relevant law
- the purposes of collection
- the main consequences for the individual if all or some of the personal information is not collected
- any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected
- the privacy policy contains information about how the individual may access their personal information and seek the correction of such information
- the privacy policy contains information about how the individual may lodge a complaint
- whether the entity is likely to disclose the personal information to overseas recipients (and if so, where).

### Collection and use limitation

The Applicant **MUST** ensure that it:

- only collects personal information that is reasonably necessary for one or more of its functions or activities
- only collects information by lawful and fair means
- only collect information from the individual or their representative, unless it is unreasonable or impractical to do so
- only uses or discloses information about an individual with the consent of the individual or
  - where the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order
  - where the Applicant reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body

---


\(^{11}\) Or particular jurisdictional Privacy Principle
○ the use or disclosure is required to monitor or detect fraud
○ or for purposes related to allowing the Identity Service Provider to verify the individual’s identity (such as investigating fraud, conducting a sole identity check, fraud analytics, hosting and maintaining the Identity Service Provider's digital service) that are within the individual’s reasonable expectations

- only discloses the minimum identity attributes required for the relying party’s transaction (i.e. supply proof of age rather than date of birth if that is all is required)

The Applicant MUST NOT ensure that it use personal information for direct marketing purposes.

### Identity Service Provider additional requirements

The Identity Service Provider MUST NOT:

- collect sensitive information (e.g. a facial image) about an individual unless:
  - the individual explicitly consents to the collection of the information and
  - the information is reasonably necessary for one or more of its functions or activities and
  - the information is destroyed once it is used to verify an individual’s attribute and is not used for any other purpose (in particular the information is not disclosed to an Identity Exchange or other third party).

The Identity Service Provider MUST ensure that it only collects and retains the minimum set of identification details required to verify and maintain an individual's identity as outlined in the Trust Framework: Digital Identity Verification Standard\(^{12}\).

#### NOTE

- The Identity Service Provider only discloses facial images to the Facial Verification Service (FVS) for the purpose of verification
- The Identity Service Provider destroys all facial images it collects immediately following a successful verification by the FVS
- The Identity Service Provider cannot disclose facial images to any other third party.

### Identity Exchange additional requirements

The Identity Exchange MUST ensure that it:

- Publishes in an open and accessible manner an annual ‘Transparency Report’ that discloses the scale, scope and reasons for access to personal information by an enforcement bodies.
- MUST NOT collect sensitive information about an individual
- MUST NOT retain users attributes once they are passed from the Identity Service Provider to the Relying Party

### Consent

For consent to be valid the following conditions MUST be satisfied:

---

\(^{12}\) See Trust Framework: Digital Identity Verification Standard for further information
- the individual is adequately informed before giving consent
- consent is voluntary
- consent is current and specific
- the individual has the capacity to understand and communicate their consent

Consent **MUST** be given explicitly.

An individual **MUST** be made aware of the implications of providing or withholding consent.

The Applicant **MUST** ensure that an individual is properly and clearly informed (without legal or industry jargon) about how their personal information will be handled.

An individual **MUST** have the capacity to consent.

If an entity is uncertain as to whether an individual has capacity to consent at a particular time, it **SHOULD** not rely on any statement of consent given by the individual at that time.

Issues that could affect an individual’s capacity to consent include:

- age
- physical or mental disability
- temporary incapacity, for example during a psychotic episode, a temporary psychiatric illness, or because the individual is unconscious, in severe distress or suffering dementia
- limited understanding of English.

Consent given at a particular time in particular circumstances **MUST NOT** be assumed to endure indefinitely.

An individual **MAY** withdraw their consent at any time, and this **MUST** be an easy to use and straightforward process.

Once an individual has withdrawn consent, reliance **MUST NOT** be placed on past consent for any future use or disclosure of the individual’s personal information.

The Applicant **MUST** inform users of other channels available to verify identity and make clear to the user what the consequences are of declining to provide the required information.

**Identity Service Provider additional requirements**

The Identity Service Provider **MUST**:

- seek and obtain consent:
  - prior to the verification of identity attributes through the Document Verification Service (DVS) and
  - prior to disclosing the verified attributes to an Identity Exchange
- seek and obtain consent to the disclosure of verified attributes with an Identity Exchange at each subsequent verification event
- seek and obtain consent to the capture and verification of facial images through the FVS
- maintain auditable logs that demonstrate that consent has been obtained
- inform individuals of any proposed changes to the way their personal information is handled and obtain consent before the changes are made.

**Cross border and contractor disclosure**

The following requirements apply solely to Identity Service Providers.
Before an Identity Service Provider discloses personal information to an overseas recipient (for example an overseas cloud host) or a contractor service provider, the Identity Service Provider **MUST** take such steps that are reasonable to ensure the recipient only uses the information for purposes related to identity verification.

The Identity Service Provider **MUST** ensure it has an enforceable contractual arrangement with the overseas recipient or contractor that specify:

- the purpose/s for which the overseas recipient are permitted to use or disclose the personal information
- the minimum technical and organisational measures that will apply to ensure the security of the personal information overseas
- that the Identity Service Provider owns and controls the information, including specifying that it can request that the overseas party destroy the information
- mechanisms that enable the Identity Service Provider to monitor compliance with these arrangement.

See the *Trust Framework: Core Security Requirements* for more information on security and contractors.

**Government Identifiers**

The following requirements apply solely to Identity Service Providers.

The Identity Service Provider **MUST NOT** adopt a government related identifier of an individual as its own identifier unless that adoption is authorised by an Australian law.

**Access, correction and dashboard**

The Applicant **MUST**:

- provide the individual with access within 30 days at no charge to the user
- respond to complaints promptly and within 30 days

**Identity Service Provider additional requirements**

The Identity Service Provider **MUST**:

- enable the individual, without restriction, to ascertain whether records contain their personal information, the nature of that information and the steps that the individual should take to access their record and make any changes that may be warranted
- provide access to all the records that it holds about an individual, without restriction
- provide a clear and straightforward process to enable the individual to correct any errors or incorrect information that it holds
  - noting that changes to name and date of birth attributes will require re-verification with an authoritative source in order to prevent identity fraud

**Identity Exchange additional requirements**

The Identity Exchange **MUST**:

- provide the user with access to the metadata on their [yet to be determined timeframe] transactions (a dashboard), in order to assist users to recognise suspicious transaction or identity fraud.
Quality of personal information

The Applicant **MUST**:

- take reasonable steps to ensure that the personal information it collects is, having regard to the purpose of the use or disclosure is accurate, up-to-date, complete, relevant and not misleading.
- take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure is accurate, up-to-date, complete, relevant and not misleading.

*Identity Service Provider additional requirements*

The Identity Service Provider **SHOULD**:

- implement internal practices, procedures and systems to audit, monitor, identify and correct poor quality personal information (including training staff in these practices, procedures and systems)
- ensure updated or new personal information is promptly added to relevant existing records
- provide individuals with a simple means to review and update their personal information on an ongoing basis.

*Handling Privacy Complaints*

The Applicant **MUST** provide a complaints service which:

- is accessible, including prominent contact information about the service
- is fair, including a process that is impartial, confidential and transparent
- has a process which is timely, clear and can provide a remedy
- has skilled and professional people who have knowledge of privacy laws and these Core Privacy Requirements and the complaint service process
- is integrated with other complaint handling bodies, (e.g other participants of the identity federation) so it can assist the user and refer complaints
- analyses complaint information, including complaint processes, and feeds conclusions into privacy risk planning and improving documentation and processes
- Publishes de-identified information and analysis about complaints

The Applicant **MUST** participate in a service that enables agreed de-identified data on complaints to be shared across participants in the identity federation to ensure participants learn from complaints.

*Destruction and de-identification*

The Applicant **MUST** ensure that:

---

• it takes reasonable steps to destroy or de-identify personal information once it is no longer needed for identity verification and related administrative purposes
• it has a written management policy that specifies:
  ○ whether stored personal information needs to be retained under law or a court/tribunal order
  ○ data retention timeframes
  ○ de-identification policies and practices (including mitigate the risk of re-identification)
  ○ data destruction policies and practices.
• all staff are informed of document destruction and de-identification procedures
• where required, personal information contained in hard copy records is destroyed through a process such as pulping, burning, pulverising, disintegrating or shredding
• hardware containing personal information (including back-ups) in electronic form is ‘sanitised’ in accordance with Australian Signals Directorate requirements to completely remove the stored personal information
• where personal information is stored on a third-party’s hardware (e.g. cloud storage) procedures are in place to verify that instructions to irretrievably destroy/de-identify the personal information have been complied with.