Trusted Digital Identity Framework

Core User Experience Requirements (document 8 of 14)

version 0.01
PUBLIC CONSULTATION DRAFT
## 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>Conventions</td>
<td>3</td>
</tr>
<tr>
<td>Scope of this document</td>
<td>3</td>
</tr>
<tr>
<td>Terms and their meaning</td>
<td>3</td>
</tr>
<tr>
<td>Intended audience</td>
<td>4</td>
</tr>
<tr>
<td>Relationship to other documents</td>
<td>5</td>
</tr>
<tr>
<td>Introduction</td>
<td>7</td>
</tr>
<tr>
<td>Usability requirements</td>
<td>8</td>
</tr>
<tr>
<td>Usability of the user journey</td>
<td>8</td>
</tr>
<tr>
<td>Learning about the identity service</td>
<td>8</td>
</tr>
<tr>
<td>Requirements for the verification journey</td>
<td>8</td>
</tr>
<tr>
<td>Requirements for the post-verification journey</td>
<td>10</td>
</tr>
<tr>
<td>Requirements for the authentication journey</td>
<td>10</td>
</tr>
<tr>
<td>Maintaining focus on usability when the service is live</td>
<td>10</td>
</tr>
<tr>
<td>Useful resources</td>
<td>11</td>
</tr>
<tr>
<td>Accessibility</td>
<td>12</td>
</tr>
<tr>
<td>Accessibility requirements</td>
<td>12</td>
</tr>
<tr>
<td>Interface and User Experience testing</td>
<td>14</td>
</tr>
<tr>
<td>Develop test plans</td>
<td>14</td>
</tr>
<tr>
<td>Conduct testing</td>
<td>14</td>
</tr>
<tr>
<td>References</td>
<td>15</td>
</tr>
</tbody>
</table>
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>0.01</td>
<td>20 Sept 2017</td>
</tr>
</tbody>
</table>

Change log

This is version 0.01 of the Trust Framework: Core User Experience 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>Sept 17</td>
<td>JC &amp; DR</td>
<td>Initial 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

Scope of this document

This document defines the usability and accessibility requirements to be met by organisations and government agencies that undergo the Trust Framework Accreditation Process.

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 the Trusted Digital Identity Framework: Glossary of Terms.
Public Consultation Draft

- **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.

- **Authorised Assessor** are 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.

- **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.

- **Trust Framework Accreditation Process** includes a number of activities and involve a combination of documentation requirements, third party evaluations and operational testing that Applicants are required to complete in order to achieve Trust Framework accreditation.

- **User Experience** for the purpose of the Trust Framework covers the accessibility, usability and inclusive design aspects of solution design to ensure identity services are straightforward and easy to use.

- **User Researcher** is a person who focuses on understanding user behaviors, needs, and motivations through observation techniques, task analysis, and other feedback methodologies.

**Intended audience**

The intended audience for this document includes:
Relationship to other documents

Figure 1: Trust Framework document hierarchy and relationships

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.
Public Consultation Draft

- Trust Framework: Core Privacy Requirements, which sets out requirements for maintaining user privacy.
- 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 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.

This document is based on the Digital Service Standard\(^1\), particularly:

- Criteria 1: Understand user needs
- Criteria 6: Consistent and responsive design
- Criteria 9: Make it accessible
- Criteria 10: Test the service

The Web Content Accessibility Guidelines 2.0 (WCAG 2.0)\(^2\) are also central to this document. Under the Disability Discrimination Act 1992 (Cwth), Australian government agencies are required to ensure information and services are provided in a non-discriminatory accessible manner. In 2009, the government endorsed the transition to WCAG 2.0, which requires all Australian government digital services to implement WCAG 2.0 to meet the middle level of conformance (Level AA) by 2013.


\(^2\) WCAG 2.0 AA [Web Content Accessibility Guidelines (WCAG) 2.0](https://www.w3.org/WAI/standards-guidelines/wcag/2.0/)

Digital Transformation Agency – Trust Framework Core User Experience Requirements Public Consultation Draft 6
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.

This document defines the Applicant’s responsibilities for usability and accessibility to ensure their identity service is simple and easy for all to use.
Usability requirements

The Applicant **MUST** implement an identity service that:

- is simple and easy to use so that people can complete their journey unassisted,
- is presented in plain language that is clear and easy for people to understand,
- is built using common design patterns to ensure consistency,
- minimises the number of steps required for people to prove who they are,
- minimises or prevents users from making errors,
- ensures users can recover from errors with minimum loss and frustration,
- ensures that people who use the digital service can also use the other available channels if needed, without repetition or confusion,
- enables people with low digital skills to seek assisted digital support,
- is built with responsive design methods to support common devices and browsers, including desktop and mobile devices,
- allows users to remember how the service works and retain proficiency with it, and
- allows users to provide feedback, seek assistance or otherwise resolve disputes or complaints.

**Usability of the user journey**

*Learning about the identity service*

Ensuring users are aware of and understand the benefits of using the identity service is critical to the overall success of the identity service.

The Applicant **MUST** provide users with:

- Clear public communications promoting the benefits of their identity service using consistent and simple language, and
- Trained staff who can educate users when they have questions about their identity service.

The Applicant **SHOULD** provide users with straightforward ways to learn about its identity service on digital channels using a memorable URL that goes straight to its identity service home page.

*Requirements for the verification journey*

Ensuring users are as prepared to use the identity service is critical to the overall success and usability of identity service.
The Applicant **MUST** provide users with:

- Information about the entire identity management process, including what to expect in each step of the user journey and what they’ll need to do in order to complete each step.
- The expected duration of the journey to allow users to plan their time accordingly.
- Information that describes how the user’s privacy is maintained, written in clear and easy to understand language.
- Information on technical requirements (for example, requirements for internet access, or access to a mobile phone or webcam), written in clear and easy to understand language.
- Information on the required identity evidence and attributes, whether each piece is mandatory, and the consequences for not providing the complete set of identity evidence. Users need to know the specific combinations of identity evidence, including requirements specific to a piece of identity evidence.
- Explanation of which identifying information will be discarded and what, if any, information will be retained for future identity verification activities. In the case of an incomplete journey, what identity evidence users will need to take to an alternative channel (for example, a shopfront) to complete an identity verification activity.
- Clear instructions on digital codes (if a code is issued as part of the identity verification process):
  - Notify users in advance that they will receive a digital code, when to expect it, the length of time for which the code is valid, how it will arrive and what to do with it.
- Ability to use an identity account recovery option in the event a user cannot access their identity account using previously issued authentication credentials.
- Clear information at the end of the identity verification process:
  - If verification is successful, send users confirmation regarding the successful verification and information on next steps.
  - If verification is partially complete (due to users not having the complete set of identity evidence, user's choosing to stop the process, or session timeouts), communicate to users what information will be discarded. Communicate to users what, if any, information will be retained for future identity verification activities (and for how long), and what identity evidence they will need to bring to complete a future identity verification activity.
  - If verification is unsuccessful, provide users with clear instructions for alternative options, for example, offering an over-the-counter identity verification process if they failed the digital identity verification process.
- Online help options for users who need assistance during the identity verification process.
- Trained support staff to assist users if needed - via phone, online chat, or in person.
A well supported offline channel to assist users who do not have the technology or capacity to prove their identity online.

**Requirements for the post-verification journey**

After a user has proved their identity, the Applicant **MUST**:

- Give users information relevant to the use and maintenance of the authentication credential. This may include instructions for use, information on credential expiry, and what to do if the credential is forgotten or stolen.
- Provide clear instructions on how a user can update their personal details collected as part of the identity verification process.

**Requirements for the authentication journey**

When a user is re-using their authentication credential the Applicant **MUST** enable simple account recovery if a user has forgotten their credential or is no longer able to access their credential.

When a user is re-using their authentication credential the Applicant **SHOULD** ensure that simple and consistent design enables users to remember how the identity service works and retain proficiency with it, even after significant time has elapsed.

**Maintaining focus on usability when the service is live**

To ensure there is an ongoing focus on usability, when its service is live the Applicant **MUST**:

- Measure and monitor its operational identity service using the following key performance indicators:
  - user satisfaction,
  - the number of digital users compared to non digital users,
  - completion rate, and
  - cost per transaction.
- Analyse feedback, support requests and analytics to ensure areas of high support need are addressed to continuously improve the service.
- Provide the Trust Framework Accreditation Authority with a report on its key performance indicators.
Useful resources


Accessibility

Accessibility requirements

The Applicant is required to undergo a Web Content Accessibility Guidelines (WCAG) Assessment of their identity service as part of the Trust Framework Accreditation Process. The assessment MUST at a minimum meet Level AA of the WCAG 2.0.

An Authorised Assessor who is also a WCAG specialist MUST assess the Applicant’s identity service for conformance to the AA level of WCAG 2.0.

The aim of the WCAG assessment is to:

- assess whether the Applicant can demonstrate its identity service confirms to the aaaa level of WCAG 2.0, and
- Document the result of the assessment in a report to the Trust Framework Accreditation Authority.

The Trust Framework Accreditation Authority has determined the following WCAG 2.0 rules are excluded and MUST NOT to be evaluated as part of the assessment:

- 1.4.3 Contrast (Minimum) (Level AA) The visual presentation of text and images of text has a contrast ratio of at least 4.5:1:
  - This guideline is excluded due to the need for service providers to adhere to their own branding and style guidelines.
- 2.4.5 Multiple Ways: More than one way is available to locate a Web page within a set of Web pages except where the Web Page is the result of, or a step in, a process. (Level AA)
  - This guideline has been excluded due to the federated nature of the digital identity ecosystem.

For the purpose of Trust Framework accreditation, an Authorised Assessor suitable to evaluate WCAG compliance MUST be either a person or company that is a:

- supplier listed on the Australian Government’s Digital Marketplace as a WCAG specialist, or
- an approved supplier listed on a government panel as an accessibility specialist.

Where an Applicant cannot support a user’s technology preference, the user journey SHOULD indicate how users will use an alternative channel to complete a specific activity.
For example, the identity service might require a user to have an active camera on their device in order to take a photograph of themselves. If the user does not have a camera on their device then the identity service **MUST** provide the user with an alternative way to complete this activity.

The Applicant **MUST** write in a clear and concise manner, using plain language that is easy to understand and accessible across all devices. Eighty percent (80%) of text displayed to the user **MUST** have a Flesch reading-ease score of 90 or more.\(^6\)

---

### Interface and User Experience testing

#### Develop test plans

The Applicant **MUST** document how they will conduct usability testing. At a minimum the test plans **MUST** include the following:

- Describe the test objectives, usability goals, and usability metrics that will be captured,
- Identify a range of representative users of the service including the following cohorts:
  - people of disability,
  - older people,
  - people who use assistive technologies,
  - people with low literacy,
  - people from culturally and linguistically diverse backgrounds, and
  - people using older technology and low bandwidth connections.
- Describe the number of test participants, how they will be recruited, and the cohort to which they belong.
- Document the approach and the methodology used to conduct the tests. This is required to indicate what is working well and where improvements are needed, and
- Document representative scenarios for testing, on both desktop and mobile devices.

#### Conduct testing

The Applicant **MUST**:

- Use experienced researchers to test its service. (An experienced user researcher is highly skilled in identifying user needs, conducting usability tests, and feeding insights back to the product team.)
- Continually test as the identity service is developed or refined.
- Test the identity service from end to end, in an environment that replicates the live environment and include both desktop and mobile devices.
- Test its identity service with a full range of representative users.
## References

The following information sources have been referenced in this document.

<table>
<thead>
<tr>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Caldwell, B. Cooper, M. Reid L. G. and Vanderheiden, G, 2008, ‘Web Content Accessibility Guidelines’ (WCAG) 2.0’, World Wide Web Consortium (W3C) <a href="https://www.w3.org/TR/WCAG20/">https://www.w3.org/TR/WCAG20/</a></td>
</tr>
</tbody>
</table>