Australian Government

Digital Transformation Agency

Usability and Accessibility Requirements

Trusted Digital Identity Framework
February 2018, version 1.0

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties with 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

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

Endorsement

Group	Endorsement date
Director, Trusted Digital Identity Framework	Jan 2018
Commonwealth GovPass Design Authority	Feb 2018

Change log

Version	Date	Author	Description of the changes
0.01	Sept 2017	JS, JC & DR	Initial version
0.02	Jan 2018	JS	Incorporated feedback from stakeholders and public consultation
1.0	Feb 2018		Endorsed by the Commonwealth GovPass Authority

Conventions

The following conventions[1] are used in this document.

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

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

Contents

1 Introduction 1

2 Part one: Usability and accessibility requirements 2

2.1 Usability requirements 2

2.2 Usability of the user journey........ 2

2.2.1 Learning about the identity service 2

2.2.2 Requirements for the verification journey 3

2.2.3 Requirements for the post-verification journey 4

2.2.4 Requirements for the authentication journey 5

2.2.5 Maintaining focus on usability when the service is live 5

2.3 Accessibility requirements 5

3 Part two: Interface and user experience testing 8

3.1 Develop test plans 8

3.2 Conduct testing 8

4 References........10

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 identity ‘eco-system’ (the ‘identity federation’). Implementation and operation of the identity federation is underpinned by the Trusted Digital Identity Framework (TDIF). This document should be read in conjunction with the *Trust Framework: Overview and Glossary*, which provides a high-level overview of the TDIF including its scope and objectives, the relationship between its various documents and the definition of key terms.

This document defines the usability and accessibility requirements to be met by Applicants to gain Trust Framework accreditation. The objective of this document to ensure identity services are simple and easy to use.

This document is based on the Digital Service Standard[2] and the Web Content Accessibility Guidelines 2.0 (WCAG 2.0)[3]. Under the *Disability Discrimination Act 1992* (Cth), 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.

The intended audience for this document includes:

- Accredited Providers.
- Applicants.
- Authorised Assessors.
- Relying Parties.
- Trust Framework Accreditation Authority.

[2] DSS design guides - http://guides.service.gov.au/design-guide/

[3] WCAG 2.0 AA - Web Content Accessibility Guidelines (WCAG) 2.0

2 Part one: Usability and accessibility requirements

2.1 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, in light of other TDIF requirements, 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 have readily available access to 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.
- Allows users to provide feedback, seek assistance or otherwise resolve disputes or complaints.

2.2 Usability of the user journey

2.2.1 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 information promoting the benefits of their identity service using consistent and simple language and multiple accessible formats.

- 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.

2.2.2 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 will 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 or numbers (if a code or number is issued as part of the identity verification process):

    - Notify users in advance that they will receive a digital code or number, 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 were unable to complete 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.

2.2.3 Requirements for the post-verification journey

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

- Give users information that is 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.

2.2.4 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 **MUST** 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.

2.2.5 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.
  - Cost per transaction.
- Analyse feedback, support requests and analytics to ensure areas where users are facing difficulties or need high support are addressed to continuously improve the service.
- Provide the Trust Framework Accreditation Authority with a report on its key performance indicators.

2.3 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 a WCAG specialist **MUST**, as a minimum, assess the Applicant’s identity service for conformance to level AA of WCAG 2.0.

The aim of the WCAG assessment is to:

- Assess whether the Applicant or Accredited Provider can demonstrate that its identity service conforms to level AA of WCAG 2.0.
- 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 not mandatory but **SHOULD** be complied with:

- 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 as mandatory due to the potential 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 and quality 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[4].

[4] GOV.AU Content Guide - http://guides.service.gov.au/content-guide/

3 Part two: Interface and user experience testing

3.1 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.
  - 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.
- Document representative scenarios for testing, on both desktop and mobile devices.

3.2 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.

4 References

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

1. Bradner, S. 1997, ‘Key words for use in RFCs to Indicate Requirements Level’ (RFC 2119), Internet Engineering Task Force, Switzerland. https://tools.ietf.org/html/rfc2119
2. Caldwell, B. Cooper, M. Reid L, G. and Vanderheiden, G, 2008, ‘Web Content Accessibility Guidelines’ (WCAG) 2.0’, World Wide Web Consortium (W3C) https://www.w3.org/TR/WCAG20/
3. Digital Transformation Agency, 2017, ‘Digital Service Standard’, Australian Government, Canberra. https://www.dta.gov.au/standard/
4. Digital Transformation Agency, 2017, ‘GOV.AU content guide’, Australian Government, Canberra. http://guides.service.gov.au/content-guide/
5. Digital Transformation Agency, 2017, ‘GOV.AU design guide’, Australian Government, Canberra. http://guides.service.gov.au/design-guide/
6. Digital Transformation Agency, 2017, ‘GOV.AU design principles’, Australian Government, Canberra. https://www.dta.gov.au/standard/design-principles/
7. Disability Discrimination Act 1992 (Cth)
8. WCAG World Wide Web Consortium (W3C), 2008, ‘Seb Content Accessibility Guidelines (WCAG 2.0)’, W3C. https://www.w3.org/TR/WCAG20/