Australian Government
Digital Transformation Agency

User Experience Requirements

Trusted Digital Identity Framework
March 2019, version 1.3

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (http://www.itsanhonour.gov.au)

Conventions

TDIF documents refenced by this document are denoted in italics. For example, *TDIF: Overview and Glossary* is a reference to the TDIF document titled Overview and Glossary.

The key words **"MUST", "MUST NOT", "SHOULD", "SHOULD NOT",** and **"MAY"** in this document are to be interpreted as described in the current version of the Trusted Digital Identity Framework: Overview and Glossary.

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, Digital Identity Policy at identity@dta.gov.au.

Document Management

The TDIF Accreditation Authority has reviewed and endorsed this document for release.

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
1.1	Oct 2018	GJF	Rename of document, updates based on feedback and inclusion of WCAG 2.1 and User Experience Report
1.2	Jan 2019	GJF	Incorporated feedback from stakeholders.
1.3	Mar 2019	SJP	Incorporated feedback from public consultation.

Contents

Introduction

Agencies and organisations that apply to be accredited under the TDIF undergo a series of rigorous evaluations across all aspects of their identity service operations. The *TDIF: Accreditation Process* requires Applicants to demonstrate their identity service is usable, privacy enhancing and is secure and resilient to cyber threats. The intent of these evaluations is to determine whether the Applicant's identity service meets the TDIF Guiding Principles[1] and whether it is suitable to join the identity federation.

This document is based on the tenets of the Digital Service Standard[2] and the Web Content Accessibility Guidelines (WCAG)[3] and defines the user experience requirements to be met by Applicants. The objective of these requirements is to enable simple and easy to use experiences for users within the identity federation.

The user experience needs be shaped and positioned into content and functionality that clearly communicates and facilitates purpose, intent and relevance. This is especially true in a transactional context where users need to know and understand at all times:

- Where they are in a specific process (and what they should expect from that process).
- Where they have come from.
- What options, actions or steps they have in front of them (if any).
- The (implicit) consequences of taking those actions or next steps.
- An unambiguous signal, feedback and/or response, once that action is taken.

It is essential to move beyond the pure mechanics of the transactional process and into a meaningful, supportive and trusted experience that directly addresses the user's needs, goals and concerns. This can be achieved in the way a transaction is structured and also how it is expressed, designed for and organised around a range of fluctuating human needs.

[1] See *TDIF: Overview and Glossary* for further information on the TDIF guiding principles.
[2] DSS design guides - http://guides.service.gov.au/design-guide/
[3] WCAG - https://www.w3.org/WAI/standards-guidelines/wcag/

User experience can be considered as a sub-set of Service Design, which is human-centred design approach that places equal value on the customer experience and the business process, aiming to create quality customer experiences, and seamless service delivery. From the federations' perspective, as the users journey will cross multiple channels and Accredited Providers to achieve their outcomes, it is vital that Accredited Providers meet, or exceed, these requirements in order to contribute to the overall user satisfaction with the Service Design of the environment.

The intended audience for this document includes:

- Applicants and Accredited Providers.
- Relying Parties.
- TDIF Accreditation Authority.

User Experience requirements

The *TDIF: Overview and Glossary* Guiding Principles and Objectives highlight the importance of ensuring the user experience is easy to use, accessible and voluntary. This is needed to ensure the identity federation provides value to all participants.

Applicants **MUST** design user journeys in order to deliver the best possible experience and outcome.

To meet the transactional context of the service Applicants' products and services **MUST** enable:

- Informed decision making: User journeys **MUST** be intuitive and information **MUST** be easily assimilated in order to ensure informed user decision making while remaining understandable, intuitive and effective.
- Simple and easy navigation: There **MUST** be no unnecessary steps, delay or friction in the customer journey.
- Parity of Experience: The experience available to a user when authenticating a journey via an Accredited Provider **SHOULD** involve no more steps, delay or friction in the user journey than the equivalent experience they have when interacting directly with the Relying Party.
- Familiarity and trust: The user **MUST** only need to use the login credentials provided by the Accredited Provider.

The DTA, in the process of establishing the identity federation, has developed a series of Service Design guidelines. As the functions performed by the participants within the federated digital identity system will contribute to the overall user experience, these guidelines **SHOULD** be used by Applicants as common design patterns to ensure consistency and promote identity services that are easy, convenient and simple.

2.1 Usability and Accessibility

Usability is part of the broader term "user experience" and, as a quality attribute, focuses on how easy user interfaces are to use to achieve the intended outcome. ISO 9241-210 defines usability as "the extent to which a product can be used by specified

users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."

The World Wide Web Consortium defines web accessibility as an attribute through which "people with disabilities can perceive, understand, navigate, and interact with the web, and they can contribute to the web". Web accessibility includes all types of disabilities that impact access to the web and thus includes visual, auditory, physical, speech, cognitive and neurological disabilities and adherence to web accessibility principles also benefits elderly users.

Context and audience frame usability and accessibility. The desktop context for use is most likely to be different from the mobile context and the audience will likely have different situations when they use the mobile version than the desktop version. Likewise, users of the system are more than likely to be diverse, and potentially subsets may only use either a desktop or mobile. It is also important to ensure information and services are provided in a non-discriminatory accessible manner, especially for Australian government agencies to comply with their requirements under the Disability Discrimination Act 1992 (Cth). However, accessibility is a subset of usability and whilst usability implies accessibility, the contrary is not necessarily true.

2.1.1 Usability requirements

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

- Ensures that users of the digital service can also use other available channels if needed, without repetition or confusion.
- Enables users 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 provide feedback, seek assistance or otherwise resolve disputes or complaints.

The Applicant **MUST** create, and maintain, a user (experience) end-to-end journey map[4] for their service.

Where information provided by the Applicant to a user, that information **MUST** be available in multiple accessible formats, including accessible online formats (such as HTML), large print format, Easy English, and braille (on request).

The Applicant **MUST** provide users with straightforward ways to learn about its identity service on digital channels that is available from its identity service home page.

2.1.1.1 Requirements for the verification journey

Ensuring users are as prepared as possible 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.
- Information on technical requirements (for example, requirements for internet access, or access to a mobile phone or webcam).
- 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.
- Explanation of 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. In the case of an incomplete journey, what identity evidence users will need to take to an

[4]A user journey map is a visualization/diagram (or several diagrams) that depict the stages, and interfaces, that a person goes through when interacting with the service in order to accomplish their goal.

alternative channel (for example, a shopfront) to complete an identity verification activity.

- 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.
- 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.
    - If verification is unsuccessful, provide users with 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.
- An offline channel to assist users who do not have the technology or capacity to prove their identity online.

2.1.1.2 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.

2.1.1.3 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.

Where an Applicant cannot support a user's technology preference[5], 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.

2.2 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:
    - Users with disability.
    - Older users.
    - Users who use assistive technologies.
    - Users with low literacy.
    - Users from culturally and linguistically diverse backgrounds.
    - Users who are Aboriginal or Torres Strait Islander.

[5] A *user's technical preference* will be their preference as it is the most accessible device/browser for them to use. They may have limited familiarity using other devices or browsers. This is why it's important that a wide range of devices and browsers are able to be used throughout the user journey.

    - Users from regional and remote areas.
    - Users 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.

Usability testing **SHOULD**, at least, include a heuristic evaluation[6] of the Applicant's identity service, with a minimum of three evaluators. Of the available sets of usability heuristics, Jakob Nielsen's '10 Usability Heuristics for User Interface Design' are probably the most commonly used.

2.3 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 range of representative users.
- Document the outcomes of its testing, including test methodology(s), test results, findings and recommendations.

2.4 Maintaining focus on usability when the service is live

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

[6]Heuristic evaluation involves having a small set of evaluators examine the interface and judge its compliance with recognized usability principles (the "heuristics")

- Monitor and measure its operational identity service using the following key performance indicators, and the applicable measurement methods defined in Annex A:
    - 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 TDIF Accreditation Authority, within the User Experience Assessment, a report on its key performance indicators.

The TDIF Accreditation Authority will publish on its public dashboard key performance indicators for the environment.

There will be other metrics Applicants service **SHOULD** measure and monitor to understand how it is performing, such as:

- Task Success Rate.
- Time to completion (Time on Task).
- User Error Rate.

2.5 Accessibility requirements

The Applicants' identity service **MUST:**

- Meet, at a minimum, the international accessibility standard WCAG 2.0 AA[7] [8].
- Be presented in a clear and concise manner, using plain language that is easy to understand and accessible across all devices.
- Publish an accessibility statement for all applicable systems (mobile and website).

[7] https://www.w3.org/TR/WCAG20/

[8] Note: The TDIF development team recognise the current WCAG 2.0 AA guidelines do not accommodate mobile applications. We'll look to address how mobile applications can be accommodated in the TDIF Accreditation Process in the next release of this document.

The Applicant **MUST:**

- Provide the TDIF Accreditation Authority, as part of the User Experience Assessment, an Assessor's Findings Report of the Applicant's compliance against the accessibility requirements.
- In the development of the Report, utilise an Assessor who has the required WCAG skills, experience and qualifications to assess the Applicant's identity service for conformance against the accessibility requirements.

User Experience Reporting

3.1 User Experience Report

The Applicant **MUST** document the outcomes of their Usability and Accessibility User Experience Assessments activities in a User Experience Report. This report **SHOULD**:

- Summarise the activities performed.
- Report the Applicant's compliance against the TDIF User Experience requirement, including:
    - Test methodology(s), test results, findings and recommendations.
    - Document, as an annex, the Applicant's compliance against the accessibility requirements, including the WCAG Assessment.
    - Report the services performance against the key performance indicators.
- Suggest remediation actions to address areas of non-compliance or unmitigated risk.
- Express an unmodified opinion and recommend whether or not the Applicant has satisfied the TDIF Usability and Accessibility requirements.

Annex A – Measuring Key Performance Indicators

The Accredited Provider **MUST** use the following methods for measuring the applicable Key Performance Indicators.

Measuring user satisfaction

By tracking user satisfaction Accredited Providers, and the TDIF Accreditation Authority, can find out what users think about the service and which parts of it causes them problems. This will help to decide what to improve.

Satisfaction is calculated by asking people to rate the service on a five-point scale (eg. 1 to 5 corresponding from “Strongly disagree” to “Strongly agree”). The annual Satisfaction rate is calculated by averaging the total of the responses.

Refer to https://www.gov.uk/service-manual/measuring-success/measuring-user-satisfaction for further guidance to assist in measuring user satisfaction.

The number of digital users compared to non-digital users

Digital take-up is the percentage of people using the services online in relation to other channels, for example paper or telephone. When calculating digital take-up, include people who get support from someone else to use the digital service (called ‘assisted digital support’).

To calculate digital take-up, follow these steps:

- Find the number of completed digital transactions over the period (include digital transactions where assisted digital support was used).
- Divide that number by the total number of transactions from all channels in the same period.
- Show the result as a percentage.

Refer to https://www.gov.uk/service-manual/measuring-success/measuring-digital-take-up for further guidance to assist in measuring digital take-up.

Completion rate

The Accredited Provider's service's completion rate is the number of digital transactions that users complete as a percentage of all digital transactions that users start. This includes transactions where the user receives assisted digital support.

To calculate completion rate:

- Count the number of completed transactions - the numerator.
- Divide it by the total number of transactions (including partially completed or failed ones) - the denominator.
- Show the result as a percentage.

Ensure to count only genuine users, i.e. set up the analytics tools to exclude internal users, test users and web robots from the data.

Refer to https://www.gov.uk/service-manual/measuring-success/measuring-completion-rate for further guidance to assist in measuring completion rates.

Cost per transaction

The indicator provides the average cost to the Accredited Provider of each transaction.

To calculate the cost per transaction:

- Work out the total cost of providing the service, including assisted digital support costs, through all channels.
- Divide it by the total number of completed transactions.

In total cost, include the following:

- Accommodation and capital charges for freehold properties.
- Fixtures, fittings, maintenance and utilities.
- Office equipment, including IT systems.

- Postage, printing and telecommunications.
- Total employment and training costs for people who provide the service.
- Overheads, e.g. (shares of) payroll, audit, top management costs, legal services.
- Raw materials and stocks.
- Research and development.
- Depreciation of start-up and one-off capital items.
- Taxes (GST, import tax, stamp duty, etc).
- Capital charges (if not paid separately when the service was established).
- Speculative or actual insurance premiums.
- Fees to sub-contractors.
- Distribution costs, including transport.
- All costs associated with promoting the service.
- Bad debts.
- Provisions (i.e. an amount put aside to cover a future liability).

Also include all the costs of providing assisted digital support as part of the total cost for the service.

Refer to https://www.gov.uk/service-manual/measuring-success/measuring-cost-per-transaction for further guidance to assist in measuring cost per transaction.