Australian Government

Digital Identity

05A Role Guidance

Trusted Digital Identity Framework

Release 4 June 2021, version 1.4

PUBLISHED VERSION

Digital Transformation Agency (DTA)

Licence

Use of the Coat of Arms

Conventions

References to *TDIF* documents, abbreviations and key terms (including the words *MUST*, *MUST NOT*, and *MAY)* are denoted in italics are to be interpreted as described in the current published version of the *TDIF: 01 – Glossary of Abbreviations and Terms.*

TDIF requirements and references to *Applicants* are to be read as also meaning *Accredited Providers*, and vice versa. The scope of *TDIF* requirements are to be read as applying to the identity system under *Accreditation* and not to the organisation's broader operating environment.

Contact us

The *DTA* is committed to providing web accessible content wherever possible. This document has undergone an accessibility check however, if you are having difficulties with accessing the document, or have questions or comments regarding the document please email digitalidentity@dta.gov.au

Document management

The *DTA* has reviewed and endorsed this document for release.

Change log

Version	Date	Author	Description of the changes
0.1	Oct 2019	MC	Initial version
0.2	Dec 2019	MC	Updated to incorporate feedback provided by stakeholders during the second round of collaboration on TDIF Release 4
0.3	Mar 2020	MC	Updated to incorporate feedback provided during the third consultation round on TDIF Release 4
1.0	May 2020		Published version
1.1	Sept 2020	MC	Updated Appendix A EOI requirements to ensure consistency with TDIF 05 Role Requirements
1.2	Feb 2021	JK	CRID0004 – Biometrics guidance changes, major grammar, style and format changes
1.3	Mar 2021	JK, SJP	Consultation Version
1.4	Jun 2021	JK, SJP, AV	Published Version CRID0009, CRID0012, CRID0018 – Updates to Proofing Guidance, Name Matching, Attribute Disclosure, Credential Service Provider Guidance, Identity Exchange Guidance. Removal of duplicated content.

Document review

All changes made to the TDIF are published in the TDIF Change Log which is available at https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework.

Contents

Introduction

This document provides guidance to *Applicants* undergoing *Accreditation* on how to meet the *TDIF: 05 - Role Requirements.* This document includes guidance on:

- *Identity Service Provider* obligations and *identity proofing* concepts.
- *Credential Service Provider* obligations.
- *Attribute Service Provider* obligations.

The intended audience for this document includes:

- *Accredited Providers*.
- *Applicants.*
- *Assessors.*
- *Relying Parties*.

Disclaimer ⚠

The guidance information provided in this document is here to support an *Applicant's* accreditation effort. It does not replace an *Applicant's* obligations to meet *TDIF* requirements.

If any conflicts exist between the *TDIF* guidance and requirements, the requirements take precedence.

Identity Service Provider Guidance

Identity proofing concepts

*Relates to section **3.1**Identity Proofing Concepts in the TDIF 05 Role Requirements.*

Identity Proofing Objectives

Identity Proofing refers to the process of collecting, *verifying*, and *validating* sufficient *Attributes* (and supporting evidence) about a specific *Individual* to confirm their *Identity*. *Relying Parties* and digital services require varying levels of confidence in a *Digital Identity* based on the consequence of incorrectly identifying an *Individual* in the provision of their services. To achieve this *Identity Service Providers* (*IdP*) undertake an *Identity Proofing* process that tests the veracity of claims. The veracity of claims about an *Individual's Identity* is established through evidence, i.e. *Evidence of Identity* (*EoI*) *documents* (the full list of accepted *EoI documents* can be found in **Appendix A** of *TDIF 05 – Role Requirements*), provided to meet some or all of the following five *Identity Proofing* objectives.

Uniqueness Objective **- confirm uniqueness of the identity in the IdP context** to ensure that *Digital Identities* can be distinguished from one another in the *IdP* context and that the right service is delivered to the right *person*. This reduces risks such as doubling up on service provision[1]. This would include a check that another *Individual* has not previously claimed ownership of the *Identity* (i.e. there is a sole claimant), for example by checking the *IdP's* database for records with the same *Attributes*.

Legitimacy Objective **- confirm the claimed identity is legitimate** to ensure the *Identity* has been genuinely created (i.e. the *Identity* is that of a real *person*) through evidence of *Commencement of Identity* (*CoI*) creation in Australia. Where greater confidence in the claimed *Identity* is required, this objective may also include a check that the *Identity* has not been recorded as deceased (through either internally or

[1] *Individuals* are legally allowed to operate in the community using different names. An *Individual* can use legitimate verifiable *Identity Documents* in one or more names which relate to them to create one or more legitimate *Digital Identities* at one or more *IdPs*.

external sources, such as law enforcement agencies or comparing *Attributes* against a *Fact of Death File*).

This objective also includes a check that there is continuity in an *Individual's Attributes* where there have been changes. Increased confidence in the legitimacy of an *Individual's Identity* is achieved through verifying *EoI documents* and verifying *Linking Documents* where name or date of birth details differ between different *EoI*. This reduces risks such as the registration of imposters or non-genuine identities.

Operation Objective **- confirm the operation of the identity in the Australian community over time** to provide additional confidence that an *Individual's Identity* is legitimate in that it is being used in the Australian community (including online where appropriate). Even where a *person* can obtain genuine *Identity Documents* in a fictitious name, it will be harder to provide evidence that the identity has been active in the Australian community. Particularly over an extended period and if evidence reflects the breadth of an *Individual's* life, such as:

- Completing schooling, attending university or receiving support or services provided by government.
- Providing evidence that demonstrates the *person's* financial or working life.
- Providing evidence that demonstrates the *person's* family situation, where they live and what they consume.

Binding Objective **- confirm the link between identity and the individual claiming the identity** to provide confidence that the *Individual's Identity* confirmed through the *Legitimacy Objective* and *Operation Objective* is not only legitimate, but that the *Individual* currently claiming the *Identity* is its legitimate holder. This has traditionally been done by comparing a *person's* face against a *Photo ID document*, although there is an increasing range of technologies and approaches that can provide alternative methods, such as comparison of a biometric captured during the *Identity Proofing* process against a biometric previously captured using an *Identity Matching Service*. The *TDIF* supports the use of *Biometric verification* to satisfy the *Binding Objective*.

Fraud Control Objective **- confirm the identity is not known to be used fraudulently** to provide additional confidence that a fraudulent (either fictitious or stolen) identity is not being used. This could be through checks against internal registers of known fraudulent identities or against 'dummy biographical records' recorded in the *IdP's* identity system. This could include checks against information provided by external sources, such as law enforcement agencies.

Evidence of Identity

Evidence of Identity may be a physical or electronic *Identity Document* or non-documentary identity data held in a repository accessible by an *IdP*. *Evidence of Identity* can have widely varying strength in relation to the *Authoritative Source* and *Identity Document* security. In addition, there may be different *Attributes* contained within the evidence, including *Attributes*, document identifiers and contact information.

The TDIF supports four *EoI document* categories:

- **Commencement of Identity** is a government issued *Identity Document*:
    - Which anchors an *Individual's Identity* and provides evidence of its establishment or creation in Australia.
    - Which is the product of high integrity business processes which create and issue the *Identity Document* and manage it throughout its lifecycle.
    - With *Attributes* contained in or printed on the *Identity Document* able to be securely verified through an *Identity Matching Service*.
- **Linking document** is a government, or court issued *Identity Document*:
    - Which provides a link that shows the continuity of the claimed Identity where *Identity Attributes* have changed.
    - With Attributes contained in or printed on the *Identity Document* that can be verified through an *Identity Matching Service*.
- **Use in the Community (UitC)** is a verifiable *Identity Document* issued by a reliable source which:
    - Includes *Attributes* either contained in or printed on the *Identity Document*, or within a repository that provides reasonable confidence that they cannot be modified after the fact.
    - Can be used to confirm the activity or provide historical evidence of an *Identity* operating in the Australian community over time.
    - This check can review either physical *Identity Documents* or non-documentary identity data held in a repository accessible by an *IdP*, that

provides a degree of confidence that the date has not been modified after the fact.

- **Photo ID** is an *Identity Document*:
  - Which allows binding between the presented *Attributes* and the *Individual* claiming the *Identity*.
  - Which allows *Visual Verification* or *Biometric verification* between the *Individual* and the *Photo ID*.
  - Where the biometric image of the *individual* is securely contained in or printed on the *Identity Document*.
  - Where high integrity business processes are followed when creating, issuing and managing the document throughout its lifecycle.
  - In which the *Attributes* contained in or printed on the *Identity Document* are able to be securely verified through an *Identity Matching Service*.
  - Where the image of the holder contained in or printed on the *Identity Document* can undergo *Biometric verification* through an *Identity Matching Service*, undergo *Technical Verification* or undergo *Visual Verification* by a trained operator.

Verification methods

Within the *Identity Proofing* process, the actions associated with checking the veracity of the claims about an *Individual's Identity* are heavily dependent on *EoI document* verification. Whilst verifying an *Identity Document* depends upon their format (physical or electronic), they can be checked using various methods which all have respective strengths and weaknesses. As such the *TDIF* supports three verification methods.

- ***Source Verification*** - the act of verifying physical or electronic *EoI* directly with the issuing body (or their representative, e.g. via an *Identity Matching Service*[2]). *Source Verification* generally provides the most accurate, up to date information, however it may not be able to prove physical possession of a document (e.g. a licence number may be written down) and it may not have all the details of an original document (e.g. birth certificate information is often a summary of the original).

[2] *Applicants* that use *Identity Matching Services* for *Source Verification* will need to meet Document Match Specifications. Further information on *Identity Matching Services* is available at https://www.idmatch.gov.au/

- ***Technical Verification*** – the act of verifying physical or electronic evidence using an *Australian Signals Directorate Approved Cryptographic Algorithm (AACA)* bound to a secure chip or appended to it (e.g. via *Public Key Technology*). *Technical Verification* is generally very accurate but is dependent of the issuer's revocation processes (e.g. a stolen passport yet to be revoked may still pass *Technical Verification*).
- ***Visual Verification*** - the act of a trained operator visually confirming, either electronically or in-*person*, that the *EoI* presented, with any security features, appears to be valid and unaltered, and/or making a facial comparison check. Generally, *Visual Verification* is less secure than *Source Verification* or *Technical Verification* as it introduces the possibility of operator error; however, it also allows for a more detailed human evaluation of the *Individual* and *Identity Document*.

These methods may be combined; for example, the details of a particular *Identity Document* may be able to *Source Verification*, however the photo on the document might require *Visual Verification*.

In all cases, regardless of verification method used, the *IdP* must be satisfied that a particular *Identity Document* can be reasonably and securely verified. This may mean rejecting an *Identity Document*, if for example, it is known that the associated database is compromised (invalidating *Source Verification*), or a cryptography protocol is broken (invalidating *Technical Verification*), or a particular document has few or no physical security features or is damaged (invalidating *Visual Verification*).

See Appendix A of *TDIF: 05 Role Requirements* for a table of all approved *EoI documents* that an *IdP's identity system* may support and the *verification* methods that must be used by the *IdP* for each *EoI document* within the *Identity Proofing* process.

Identity Proofing

*Relates to TDIF requirements **IDP-03-02-01** to **IDP-03-02-02** of section **3.2** in the TDIF: 05 Role Requirements.*

The *TDIF IP levels* define the *identity proofing* process, which are ranked from lowest to highest based on the consequence of incorrectly identifying an individual. The assurance reflected by each level is derived from the veracity of the claims about an individual's *identity*, through the evidence provided, to meet some or all of the *identity proofing* objectives of:

- *Uniqueness.*
- *Legitimacy.*
- *Operation.*
- *Binding.*
- *Fraud Control.*

Table 1 of *TDIF 05 Role Requirements* contains the *Identity* proofing objectives, levels and document combination requirements.

The *TDIF's Identity Proofing Levels* are:

- **Identity Proofing Level 1** is used when no identity verification is needed or when a very low level of confidence in the claimed *Identity* is needed. This level supports self-asserted identity (I am who I say I am) or pseudonymous *Identity*. The intended use of *Identity Proofing Level 1* is for services where the risks of not undertaking identity verification will have a negligible consequence to the *Individual* or the service. For example, to pay a parking infringement or obtain a fishing licence.
- **Identity Proofing Level 1 Plus** is used when a low level of confidence in the claimed *Identity* is needed. This requires one *Identity Document* to verify someone's claim to an existing *Identity*. The intended use of *Identity Proofing Level 1 Plus* is for services where the risks of getting *identity* verification wrong will have minor consequences to the *Individual* or the service. For example, the provision of loyalty cards.
- **Identity Proofing Level 2** is used when a low-medium level of confidence in the claimed *Identity* is needed. This requires two or more *Identity Documents* to verify someone's claim to an existing *Identity*. The intended use of *Identity Proofing Level 2* is for services where the risks of getting identity verification wrong will have moderate consequences to the *Individual* or the service. For example, the

provision of utility services. An *Identity Proofing Level 2* identity check is sometimes referred to as a “100-point check”.

- **Identity Proofing Level 2 Plus** is used when a medium level of confidence in the claimed *Identity* is needed. This requires two or more *Identity Documents* to verify someone’s claim to an existing *Identity* and requires the *Binding Objective* to be met. The intended use of *Identity Proofing Level 2 Plus* is for services where the risks of getting identity verification wrong will have moderate-high consequences to the *Individual* or the service. For example, undertaking large financial transactions.
- **Identity Proofing Level 3** is used when a high level of confidence in the claimed *Identity* is needed. This requires two or more *Identity Documents* to verify someone’s claim to an existing *Identity* and requires the *Binding Objective* to be met. The intended use of *Identity Proofing Level 3* is for services where the risks of getting identity verification wrong will have high consequences to the *Individual* or the service. For example, access to welfare and related government services.
- **Identity Proofing Level 4** is used when a very high level of confidence in the claimed *Identity* is needed. This requires four or more *Identity Documents* to verify someone’s claim to an existing *Identity* and the *Individual* claiming the *Identity* must attend an in-person interview as well as meet the requirements of *Identity Proofing Level 3*. The intended use of *Identity Proofing Level 4* is for services where the risks of getting identity verification wrong will have a very high consequence to the *Individual* or the service. For example, the issuance of government-issued documents such as an Australian passport.

Individuals unable to meet Identity Proofing Requirements

*Relates to TDIF requirements **IDP-03-03-01** to **IDP-03-03-01b** of section **3.3** in the TDIF 05 Role Requirements.*

Although most *Individuals* should be able to meet the requirements set out in **Section 3.2 Table 1** of the *TDIF:05 Role Requirements* document, in some cases *Individuals* may face genuine difficulty in providing the necessary *EoI documents* to meet the required *Identity Proofing Level*.

Requirements and guidance for cases where *Individuals* are unable to meet *Identity Proofing* requirements and alternative *Identity Proofing* processes are outlined in **Section 3.3** of the *TDIF:05 Role Requirements.*

Identity verification of children

The *TDIF* does not include requirements relating to the minimum age of *individuals* who can undergo an *identity proofing* or *authentication Credential* process.

Identity Service Providers should:

- Verify the identity of the child's parents or legal guardian to the required *Identity Proofing Level*, and
- Establish a documentary link between the child and their parent or legal guardians, such as through the provision of the child's birth certificate.

If seeking to verify the identity of children at IP4, *Identity Service Providers* should use exceptions processes and may request a range of additional evidence to indicate the child's use of their *identity* in the Australian community over time. For example, documents produced through the child's engagement with the health and education sectors.

Identity proofing lifecycle management

*Relates to TDIF requirements **IDP-03-04-01** to **IDP-03-04-02b** of section **3.4** in the TDIF 05 Role Requirements.*

As part of *Identity Proofing* lifecycle management, *Personal information* from *Identity documents* listed in **Table 6** (Appendix A) of the *TDIF: 05 Role Requirements* document may be collected with the *Individual's consent.*

The collection and use of information collected by an *IdP* is underpinned by privacy obligations defined in Section 3.6 of the *TDIF: 04 Functional Requirements* document.

Attribute collection, verification, and validation

*Relates to TDIF requirements **IDP-03-06-01** of section **3.6** in the TDIF 05 Role Requirements.*

Table 3 in *TDIF 05 Role Requirements* allows an *IdP* to collect a person's preferred name. An *IdP* can source a *User's* Given Name and Family Name from the Preferred Name *attribute* if there are no *verified* names available. If an *IdP* has *verified* a *User's* name from an *EoI* document, then the Given Name and Family Name *attributes* should be sourced from this (corresponding to an *IP1 Plus proofing level*).

Name matching guidance

There are a number of reasons why someone's name might be different across evidence of identity documents. For example, their surname might have changed when they got married, or their name may be shown as a synonym on different pieces of evidence (e.g. Samantha on their passport and Sam on their Driver Licence). If someone has changed their name, an *IdP* might need to collect additional evidence to make sure the *identity* documents belong to the same *individual*.

Guidance for the recording of names is provided in the Department of Home Affairs *Improving the integrity of identity data: Recording of a name to establish identity; Better Practice Guidelines for Commonwealth Agencies – June 2011*. See: https://www.homeaffairs.gov.au/criminal-justice/files/recording-name-establish-identity.pdf

Guidance for improving the integrity of *identity* data to enable data matching is provided in the Department of Home Affairs *Improving the Integrity of Identity Data; Data Matching: Better Practice Guidelines 2009*. See: https://www.homeaffairs.gov.au/criminal-justice/files/improving-integrity-identity-data.pdf

Attribute disclosure

*Relates to TDIF requirements **IDP-03-07-01** to **IDP-03-07-03a** of section **3.7** in the TDIF 05 Role Requirements.*

An *IdP* is able to disclose certain *Attributes* collected in **Tables 2** and **3** of the *TDIF 05 Role Requirements* to *Relying Parties* in accordance with PRIV-03-09-01 (Express Consent). Additional identity information such as *EoI document attributes* may be requested by *Relying Parties* as they establish their own identity matching processes during an initial transaction with an *individual*. The following guidance expands on *Applicant* obligations relating to disclosure of personal information and language used in sections 3.6 and 3.7 of *TDIF 05 Role Requirements*.

Expanded technical descriptions of the *Attributes* contained in **Tables 2** and **3** of *TDIF 05 Role Requirements* are available in the *TDIF 06D Attribute Profile*. Please note that *IdPs* that are not connected to the *Australian Government's Identity Federation* do not need to use the same mapping of the *Attributes* provided in *TDIF 06D Attribute Profile*.

The five categories of *attributes* that can be disclosed by an *IdP* are:

1. ***Identity attributes,*** including a *User's Identity Attributes* that are *Verified* by completing the *Identity Proofing Objectives* per *Proofing Level*. This means that the more *Identity Documents* and *Identity Proofing Objectives* these *Attributes* are *Verified* against, the more confidence can be placed in the *Digital Identity* of that *User*.

    - For example, a *person's* name and date of birth at *IP 1 Plus* is only *Verified* using one *UitC document* or *Photo ID*. However, at *IP 3*, a *person's* name and date of birth is *verified* using both a *CoI Document* and a *Photo ID,* as well as a *Visual* or *Biometric Verification* check to confirm the link between the *Identity* and the *Individual* claiming the *Identity* (the *Binding Objective*)*.* These additional document *Attribute Verification* and *Binding Objectives* being met can give a *Relying Party* greater confidence that the *Verified* name and date of birth *attributes* belong to the *Individual's Digital Identity* account and may mitigate some fraud risks associated with offering their service to that *User*.

2. **Contact *attributes*,** including a *User's Validated* contact details such as mobile phone number and email address. Other contact attributes that may be collected (**Table 3** of *TDIF 05 Role Requirements*) such as address or phone numbers may not be able to be validated by an IdP and, unless otherwise indicated by the system metadata, should be *assumed self-asserted* by the *User*. Contact details are a statement as to whether a *User* is contactable using that information, not a statement as to the *identity* of the *Individual*.

    - Currently, there is no *Binding Objective* required between the contact *Attributes* and the *Identity* of an *Individual*, therefore a contact *Attribute* cannot be *Verified*. A *Relying Party* may use the assertion of *Validation* as confirmation that a check has been done to *validate* that the *User* has ownership of that contact information.

3. ***EoI Document Attributes (Verified Restricted Attributes),*** including *Attributes* that are collected from an *Individual's EoI Documents* and *Verified* by an *Authoritative Source* (e.g. An Australian passport number as *Verified* through *DVS*).
4. ***Identity System Metadata,*** including data related to the *User's* interactions with the *Applicant's Identity System*. This data can be trusted as it is generated and controlled by the system, not the *User*.
5. ***Assumed Self-asserted Attributes*,** including *Attributes* that are self-asserted by the *User* and are not or cannot *Verified* or *Validated*. *Self-Asserted Attribute* collection for *IdPs* is limited by **Table 3** in *TDIF 05 Role Requirements.* If an *IdP* wishes to collect *Assumed Self-asserted Attributes* beyond those in **Table 3**, they must be accredited as an *Attribute Service Provider*.

The confidence a *Relying Party* can have in an *attribute* is also based on whether the *attribute* is *system metadata*, *assumed self-asserted*, *validated* or *verified*[3].

Table 1 on the next page sets out how *attributes* disclosed by an *Identity Service Provider* should be viewed by a *Relying Party.* It is intended to assist an *Identity Service Provider* in providing guidance to its *Relying Parties* about how to treat the *Attributes* they disclose and assist them in understanding which *Attributes* they should seek to share at a given *Identity Proofing Level*.

[3] These terms are defined in the *TDIF 01 Glossary.*

Relying Parties should not seek *verified attributes* at *IP1*. *Identity Service Providers* should treat all requests for *verified attributes* at IP1 with suspicion and should monitor for potential fraud risks. If a *Relying Party* requires *verified identity attributes* they should, at a minimum, request *IP 1 PLUS*.

In addition to the terms above, **Table 1** utilises the following syntax:

- Blank cells indicate the *attribute* should not be reasonably required nor requested by the *Relying Party* at the *IP level.*
- Cells marked '*Assume Self-asserted*' mean that if those *Attributes* are requested at that *IP level*, the *IdP* should not return a *Verified* or *Validated* result and the *Relying Party* should assume them to be self-asserted by the *User*.
- Cells marked as '*Restricted Attributes*' have additional controls which limit their disclosure. Sharing of these *Attributes* is restricted by **IDP-03-07-03a** and a request by the *IdP* to share this information with the *Relying Party* must be submitted to the *DTA* for approval. These *attributes* are *verified*.
    - **Note:** *Relying Parties* connected to the *Australian Government Identity Federation* must first be approved to receive *Restricted Attributes*. This request is approved by the *Oversight Authority*.
    - **Note:** *IdPs* that are not connected to the *Australian Government Identity Federation* will need permission from the *DTA* to share *Restricted Attributes* with any *Relying Parties* they are connected to.

Table 1: Attribute Disclosure Table

Attribute Disclosure – Verification of Attributes per IP Level						
Identity Attributes	IP 1	IP 1 Plus	IP 2	IP 2 Plus	IP 3	IP 4
Family Name	*Assume Self-Asserted*	*Verified*				
Given Names	*Assume Self-Asserted*	*Verified*				
Date of Birth	*Assume Self-Asserted*	*Verified*				
Place of Birth	*Assume Self-Asserted*					
Preferred Name	*Assume Self-Asserted*					
Titles (e.g. Dr. Mr, Ms)	*Assume Self-Asserted*					
Contact Attributes	IP 1	IP 1 Plus	IP 2	IP 2 Plus	IP 3	IP 4
Email	*Assume Self-Asserted* **OR** *Validated*					
Mobile Phone Number	*Assume Self-Asserted* **OR** *Validated*					
Residential address[4]	*Assume Self-Asserted*					
Postal address	*Assume Self-Asserted*					
Other address (e.g. second residential address)	*Assume Self-Asserted*					
Other phone number (e.g. landline)	*Assume Self-Asserted*					
EoI document attributes (Verified Restricted Attributes)	IP 1	IP 1 Plus	IP 2	IP 2 Plus	IP 3	IP 4
Verified Documents (container): - *Document type code* - *Document Verification Method* - *Document Verification Date*	-	-	**Restricted Attributes (Verified) -** Sharing of these attributes is restricted by **IDP-03-07-03a** and a request by the *IdP* to share this			

[4] At the time of publication, there are currently no publicly available, free and certified *authoritative sources* for an *IdP* to *validate* an *Individual's* residential or postal address

• *Document identifiers (container)* • *Other Document Attributes (container)*			information with the Relying Party must be submitted to the *DTA* for approval.			
Verification method used for each *EoI document* (i.e. S, T, V)	-	-	*System Metadata*			
Date and time the *EoI document* was verified	-	-	*System Metadata*			
Identity System Metadata	IP 1	IP 1 Plus	IP 2	IP 2 Plus	IP 3	IP 4
Date and time *Attributes* last updated (i.e. verified names and date of birth)	-	*System Metadata*				
Date and time email address was last validated	*System Metadata* [if collected]					
Date and time mobile phone number was last validated	*System Metadata* [if collected]					
Identity Proofing Level achieved	*System Metadata*					
Date and time the *Digital Identity* was created	*System Metadata*					
Digital Identity (user identifier)	*System Metadata*					

Biometric Verification Guidance

Relates to TDIF requirements ***IDP-03-08-01*** *to* ***IDP-03-08-34*** *of section* ***3.8*** *in the TDIF 05 Role Requirements.*

Applicants undertaking biometric acquisition should ensure adequate usability, testing, and accessibility during this process. *NIST Usability & Biometrics: Ensuring Successful Biometric Systems* provides guidance on the usability of biometric systems. See: https://www.nist.gov/system/files/usability_and_biometrics_final2.pdf

Guidance for online Biometric Binding

Relates to TDIF requirements ***IDP-03-08-01*** *to* ***IDP-03-08-04*** *of section* ***3.8.1*** *in the TDIF 05 Role Requirements.*

Applicants should ensure that document acquisition, biometric matching, and *Presentation Attack Detection*, are processed in a singular transaction that is robust and resistant to exploitation.

Applicants must perform either/or *Source Verification* and *Technical Verification* as outlined in the *TDIF: 04 Functional Requirements*.

Guidance for Presentation Attack Detection

Relates to TDIF requirements ***IDP-03-08-05*** *to* ***IDP-03-08-10b*** *of section* ***3.8.2*** *in the TDIF 05 Role Requirements.*

Presentation Attack Detection includes all the methods used in the determination of potential *presentation attacks*. While this is primarily concerned with *liveness detection* and the testing of this technology, the *TDIF* requirements include system level *Presentation Attack Detection* monitoring in addition to *liveness detection* achieved through the data capture subsystem (as in requirement **IDP-03-08-07**).

Guidance on *Presentation Attack Detection* techniques is provided by *ISO 30107 Biometric Presentation Attack Detection*. See: https://www.iso.org/standard/53227.html

PAD testing is to be undertaken in accordance with Evaluation Assurance Level (EAL)1 of the Common Criteria framework (as in requirement ***IDP-03-08-09***). *ISO 30107- 3* describes attack potential for biometric systems in relation to an attacker's knowledge, proficiency, resources and motivation as a part of the EAL system.

The *FIDO Biometric Requirements presentation attack* testing approach simplifies the attack potential to four factors relevant to the TDIF use case:

1. Elapsed time: <=one day, <=one week, <=one month, >one month
2. Expertise: layman, proficient, expert, multiple experts
3. Equipment: standard, specialized, bespoke
4. Access to biometric characteristics: immediate, easy, moderate, difficult

The *FIDO Biometric Requirements* proposes three levels of Presentation Attack Instruments (PAI) which should be used when undertaking EAL1 testing to satisfy the *TDIF PAD* testing requirement.

a) Level A: Simple, basic artefacts

b) Level B: Moderate quality artefacts

c) Level C: High quality, complex artefacts

The submitted report should include, in conformance with *ISO 30107*, the following (as required in ***IDP-03-08-10***):

- General description of the product tested
- Number of unique test subjects
- Test subject distribution of age and gender
- Number and general description of artefacts used
- Number of impostor verification transactions per artefact type
- Attack presentation classification error rate
- Attack presentation non-response rate

Additional information and guidance can be found in the *FIDO Biometric Requirements*. See: https://fidoalliance.org/specs/biometric/Biometrics-Requirements-v1.0-wd-20190606.html

The *Biometric Evaluation and Testing Framework*, funded by the European Commission, contains further guidance around biometric testing. See: https://www.beat-eu.org/

Guidance for Document Biometric Matching

*Relates to TDIF requirements **IDP-03-08-11** to **IDP-03-08-16a** of section **3.8.3** in the TDIF 05 Role Requirements.*

Applicants should refer to the *FIDO Biometric Requirements* for guidance on biometric testing for *Technical Verification/Document biometric matching* processes. This includes:

- A minimum of 245 test subjects
- 1:1 verification scenario
- Accuracy with a false match rate no more than 0.01% and a false non-match rate no more than 3%

For the reporting of biometric matching outcomes, applicants should refer to *ISO 19795 Biometric performance testing and reporting*. See: https://www.iso.org/standard/41447.html

Photo ID guidance

*Relates to TDIF requirements **IDP-03-08-17** to **IDP-03-08-18d** of section **3.8.4** in the TDIF 05 Role Requirements.*

Further information on checking ePassports can be found on the International Civil Aviation Organisation’s website. See: https://www.icao.int/Security/FAL/PKD/Pages/ePassport-Validation.aspx

Image quality specific guidance

*Relates to TDIF requirements **IDP-03-08-19** and **IDP-03-08-20** of section **3.8.5** in the TDIF 05 Role Requirements.*

Ensuring good image quality is essential to good biometric matching outcomes for both *Source Verification* and *Technical Verification*

Guidance on biometric quality is provided by ISO 29794 Biometric sample quality. See: https://www.iso.org/standard/62782.html

Guidance for local Biometric Binding

*Relates to TDIF requirements **IDP-03-08-21** to **IDP-03-08-23** of section **3.8.6** in the TDIF 05 Role Requirements.*

Ensuring good practices for *Manual Face Comparison* and fraud control processes for in-person transactions is important to meeting the *TDIF* requirements.

Guidance on *Manual Face Comparison* processes can be found on the *Facial Identification Scientific Working Group* website. See: https://fiswg.org/index.htm

Guidance for logging and data retention

*Relates to TDIF requirements **IDP-03-08-24** to **IDP-03-08-27b** of section **3.8.7** in the TDIF 05 Role Requirements.*

Applicants should refer to Section 3 of the *TDIF 04 Functional Requirements* for privacy requirements in relation to biometric data, logging, and data retention

Manual Face Comparison guidance

*Relates to TDIF requirements **IDP-03-08-28** to **IDP-03-08-34** of section **3.8.8** in the TDIF 05 Role Requirements.*

The TDIF requirements permit *Manual Face Comparison* processes to be performed remotely where there are appropriate controls, privacy measures, and security.

Credential Service Provider Guidance

These guidelines incorporate the National Institute of Standards and Technology (*NIST*) Special Publication (*SP*) *800-63B, Digital Identity Guidelines – Authentication and Lifecycle Management*. This publication will be referred to as *NIST SP* 800-63B.

The *TDIF Credential Service Provider (CSP)* requirements address how an *Individual* can securely authenticate to a CSP to access a digital service or set of digital services. This section also describes the process of binding a *Credential* to a *digital* identity account*.*

For services in which return visits are applicable, a successful *authentication* provides reasonable risk-based assurances that the *Individual* accessing the service today is the same as that which accessed the service previously. The robustness of this confidence is described by a CL categorisation. The *TDIF* addresses how an *Individual* can securely authenticate to a CSP to access a digital service or set of digital services.

This guidance references *Australian Signals Directorate Approved Cryptographic Algorithms (AACA)* and *Australian Signals Directorate Approved Cryptographic Protocols (AACP)* from the Information Security Manual (ISM)***.*** The latest version of the ISM is available from the Australian Signals Directorate website.
See: https://www.cyber.gov.au/ism

For further guidance related to *Credential* risk management see *TDIF 03A Digital Identity Risk Management.*

Credential Concepts

Authentication Management

The classic paradigm for *Credential* systems identifies three factors as the cornerstones of authentication:

- Something you know (e.g. a password).
- Something you have (e.g. an ID badge or a *Cryptographic Key*).
- Something you are (e.g. a fingerprint or other biometric data).

Multi-factor Authentication (MFA) refers to the use of more than one of the above factors. The strength of *Credential* systems is largely determined by the number of different factors incorporated by the system — the more factors employed, the more robust the *Credential authentication* system. For the purposes of *TDIF* guidance, using two *authentication factors* is adequate to meet the highest security requirements. Other types of information, such as location data or device identity, may be used by a *Relying Party* to evaluate the risk in a claimed *identity*, but they are not considered *authentication factors*.

In digital *Credential authentication* the *Individual* claims they possess or control one or more *authentication factors* that have been registered with the *CSP* and are used to prove their *Digital Identity*. The *Credential* contains secrets the *Individual* can use to prove they are a valid *User* of the *identity system*.

The secrets contained in a *Credential* utilise *Public Key Infrastructure* and *Public Key Technology*, using public key pairs (asymmetric keys) or shared secrets (symmetric keys). A public key and a related private key comprise a public key pair. The private key is stored on the *Credential* and is used by the *Individual* to prove possession and control of the *Credential*. The *CSP*, knowing the *Individual's* public key through some *Credential* (typically a public key certificate), can use an *authentication* protocol to verify the *Individual's identity* by proving that they are in possession and control of the associated private key.

Shared secrets stored on a *Credential* may be either symmetric keys or memorized secrets (e.g. passwords and PINs), as opposed to the asymmetric keys described above, which *Individual's* need not share with the *CSP*. While both keys and passwords can be used in similar protocols, one important difference between the two is how they relate to the *Individual*. While symmetric keys are generally stored in hardware or software that the *Individual* controls, passwords are intended to be memorised by the *Individual*. Since most *users* choose short passwords to facilitate memorisation and ease of entry, passwords typically have fewer characters than *Cryptographic Key* s.

Furthermore, whereas systems choose keys at random, *users* attempting to choose memorable passwords will often select from a very small subset of the possible passwords of a given length, and many will choose very similar values. As such, whereas *Cryptographic Key* s are typically long enough to make network-based guessing attacks untenable, *user*-chosen passwords may be vulnerable, especially if no defences are in place.

Some of the classic authentication factors do not apply directly to digital *authentication*. For example, a physical driver's licence is something you have, and may be useful when authenticating to a human (e.g. a security guard), but is not in itself a *Credential* for digital *authentication*. *Authentication factors* classified as something you know are not necessarily secrets, either. Knowledge-based *authentication*, where the *Individual* is prompted to answer questions that are presumably known only by the *Individual*, also does not constitute an acceptable secret for digital *authentication*. A *biometric* also does not constitute a secret. Accordingly, the *TDIF* only allows the use of *biometrics* for *authentication* when strongly bound to a physical *Credential*.

A digital *Credential* system may incorporate multiple factors in one of two ways:

1. The system may be implemented so that multiple factors are presented to the *CSP.*
   - For example, this can be satisfied by pairing a memorised secret (what you know) with an out-of-band device (what you have). Both outputs are presented to the *CSP* to authenticate the *Individual*.
2. Some factors may be used to protect a secret that will be presented to the *CSP*.
   - For example, consider a piece of hardware that contains a *Cryptographic Key* where access is protected with a fingerprint. When used with the *biometric*, the *Cryptographic Key* produces an output that is used to authenticate the *Individual*.

Credential Levels

This section relates to TDIF requirements ***CSP-04-01-01*** *to* ***CSP-04-01-05b*** *of section* ***4.1*** *in the TDIF 05 Role Requirements.*

The *TDIF* has three *Credential Levels* (CL) of assurance (confidence) for the *Credentials* used, ranked from lowest to highest. These levels are derived from the associated technology, processes, and policy and practice statements controlling the operational environment in which they are used. As the 'consumers' of *digital identities*, *Relying Parties* will determine their required level of *Credential* (and *identity*) assurance based on a risk *assessment*. Further information on undertaking risk assessments is set out in *TDIF 03A Digital Identity Risk Assessment*.

The three *CLs* define the subsets of options *Applicants* and organisations can select based on their risk profile and the potential harm caused by an attacker taking control of a *Credential* and accessing an organisation's *identity system.*

A detailed description of the *CLs* are as follows:

- ***Credential* Level 1 (CL 1)**: provides a low level of confidence that the *Individual* controls a *Credential* bound to their *digital identity*. The intended use of this level is for services where the risks of getting *Credential* binding wrong will have negligible to minor consequences to the *Individual* or the service. At a minimum, *single-factor authentication* is used at this level.

- ***Credential* Level 2 (CL 2)**: provides a medium level of confidence that the *Individual* controls a *Credential* bound to their *digital identity*. The intended use of this level is for services where the risks of getting *Credential* binding wrong will have moderate to high consequences to the *individual* or the service. Proof of possession and control of two different *authentication factors* (*multi-factor authentication*) is required through a secure authentication protocol.

- ***Credential* Level 3 (CL 3)**: provides a very high level of confidence that the *Individual controls* a *Credential* bound to their *digital identity*. The intended use of this level is for services where the risks of getting *Credential* binding wrong will have very high consequences to the *Individual* or the service. *Authentication* at *CL 3* is based on proof of possession of a key through a cryptographic protocol (*AACP*). *CL 3* is similar to *CL 2* but also requires a 'hard' cryptographic token that provides *CSP-impersonation resistance.*

Within the *TDIF* it is the *CSP,* via their symbiotic relationship with the *IdP*, who is responsible for all processes relevant to the management of a *Credential*, or means to produce *Credentials*, and the data that can be used to authenticate *Credentials*. Depending on the *Credential* form factor, this management may include:

- Creation of *Credentials*
- Issuance of *Credentials* or of the means to produce *Credentials*
- Activation of *Credentials* or the means to produce *Credentials*

- Storage of *Credentials*
- Revocation and/or destruction of *Credentials* or of the means to produce *Credentials*
- Renewal and/or replacement of *Credentials* or the means to produce *Credentials*.
- Record-keeping
- Expiration of *Credentials.*

The *authentication* process begins with the *Individual* demonstrating to the *CSP* that they possess and control a *Credential* that is bound to the asserted *identity* through an *authentication* protocol. Once possession and control have been demonstrated, the *CSP* verifies that the *Credential* remains valid.

The exact nature of the interaction between the *CSP* and the *Individual* during the *authentication* protocol is extremely important in determining the overall security of the *identity system*. Well-designed protocols can protect the integrity and confidentiality of communication between the *Individual* and the *CSP* both during and after the *authentication* and can help limit the damage that can be done by an attacker masquerading as a legitimate *User*.

Additionally, mechanisms located at the *CSP* can mitigate online guessing attacks against lower entropy secrets — like passwords and PINs — by limiting the rate at which an attacker can make *authentication* attempts, or otherwise delaying incorrect attempts. Generally, this is done by keeping track of and limiting the number of unsuccessful attempts, since the premise of an online guessing attack is that most attempts will fail.

Further guidance for TDIF *Credential* management is in the *Credential Lifecycle Management Guidance* section of this document (*TDIF 05A Role Guidance*).

Credential types and guidance

*This section relates to TDIF requirements **CSP-04-02-01** to **CSP-04-02-09g** of section **4.2** in the TDIF 05 Role Requirements.*

Memorised secrets

A *Memorised Secret* — commonly referred to as a password or, if numeric, a PIN — is a secret value intended to be chosen and memorised by the *user*. *Memorised secrets* need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value. A *memorised secret* is something you know.

Look-up secrets

A *look-up secret* is a physical or electronic record that stores a set of secrets shared between the *Individual* and the *CSP*. The *Individual* looks up the appropriate secret(s) needed to respond to a prompt from the *CSP*. For example, the *CSP* may ask an *Individual* to provide a specific subset of the numeric or character strings printed on a card in table format. A common application of *look-up secrets* is the use of "recovery keys" stored by the *Individual* for use in the event another *Credential* is lost or malfunctions. A *look-up secret* is something you have.

Out-of-Band devices

An *out-of-band Credential* is a physical device that is uniquely addressable and can communicate securely with the *CSP* over a distinct communications channel, referred to as the secondary channel. The *out-of-band device* is possessed and controlled by the *Individual* and supports private communication over this secondary channel, separate from the primary channel for e-authentication. An *out-of-band device Credential* is something you have.

The *out-of-band device Credential* can operate in one of the following ways:

- The *Individual* transfers a secret received by the *out-of-band device* via the secondary channel to the *CSP* using the primary channel. For example, the *Individual* may receive the secret on their mobile device and type it (typically a 6-digit code) into their *authentication session*.

- The *Individual* transfers a secret received via the primary channel to the *out-of-band device* for transmission to the *CSP* via the secondary channel. For example, the *Individual* may view the secret on their *authentication session* and either type it into an application on their mobile device or use a technology such as a barcode or QR code to enable the transfer.

- The *Individual* compares secrets received from the primary channel and the secondary channel and confirms the *authentication* via the secondary channel.

The secret's purpose is to securely bind the *authentication* operation on the primary and secondary channel. When the response is via the primary communication channel, the secret also establishes the *Individual's* control of the *out-of-band device*.

Examples of out-of-band devices may be a mobile phone or landline.

Single-Factor One Time Password (SF OTP) devices

A *single-factor OTP device* generates *OTPs*. This category includes hardware devices and software-based *OTP* generators installed on devices such as mobile phones. These devices have an embedded secret that is used as the seed for generation of *OTPs* and does not require activation through a second factor. The *OTP* is displayed on the device and manually input for transmission to the *CSP*, thereby proving possession and control of the device. An *OTP* device may, for example, display 6 characters at a time. A *single-factor OTP device* is something you have.

Single-factor OTP devices are similar to *look-up secret* with the exception that the secrets are cryptographically and independently generated and compared by the *CSP*. The secret is computed based on a nonce that may be time-based or from a counter on the *Credential* and *CSP*.

Examples of SF OTP devices may include mobile phones.

Multi-Factor OTP (MF OTP) devices

A *multi-factor OTP device* generates *OTPs* for use in *authentication* after activation through an additional *authentication factor*. This includes hardware devices and software-based *OTP* generators installed on devices such as mobile phones. The second factor of *authentication* may be achieved through some kind of integral entry pad, an integral *biometric* (e.g. fingerprint) reader, or a direct computer interface (e.g. USB port). The *OTP* is displayed on the device and manually input for transmission to the *CSP*. For example, an *OTP device* may display 6 characters at a time, thereby proving possession and control of the device. The *multi-factor OTP device* is something you have and it is activated by either something you know or something you are.

Single-Factor Cryptographic (SF Crypto) software

A *single-factor cryptographic software Credential* is a *Cryptographic Key* stored on disk or some other "soft" media. *Authentication* is accomplished by proving possession and control of the key. The *Credential* output is highly dependent on the specific cryptographic protocol (*AACP*), but it is generally some type of signed message. The *single-factor cryptographic software Credential* is something you have.

Single-Factor Cryptographic (SF Crypto) devices

A *single-factor cryptographic device* is a hardware device that performs cryptographic operations using protected *Cryptographic Key* (s) and provides the *Credential* output via direct connection to the user endpoint. The device uses embedded symmetric or asymmetric *Cryptographic Key* s and does not require activation through a second factor of *authentication*. *Authentication* is accomplished by proving possession of the device via the *authentication protocol*. The *Credential* output is provided by direct connection to the *Individual's* endpoint and is highly dependent on the specific cryptographic device and protocol, but it is typically some type of signed message. A *single-factor cryptographic device* is something you have.

Examples of SF Crypto devices may include a USB key fob or a mobile phone.

Multi-Factor Cryptographic (MF Crypto) software

A *multi-factor cryptographic software Credential* is a *Cryptographic Key* stored on disk or some other "soft" media that requires activation through a second factor of *authentication*. *Authentication* is accomplished by proving possession and control of the key. The *Credential* output is highly dependent on the specific *cryptographic protocol* (*AACP*), but it is generally some type of signed message. The *multi-factor cryptographic software Credential* is something you have and is activated by either something you know or something you are.

Examples may include digital certificates issued by a *Certification Authority* (CA)

Multi-Factor Cryptographic (MF Crypto) devices

A *multi-factor cryptographic device* is a hardware device that performs cryptographic operations using one or more protected *Cryptographic Keys* and requires activation through a second *authentication factor*. *Authentication* is accomplished by proving possession of the device and control of the key. The *Credential* output is provided by direct connection to the *Individual's* endpoint and is highly dependent on the specific cryptographic device and protocol, but it is typically some type of signed message. The *multi-factor cryptographic device* is something you have and it is activated by either something you know or something you are.

Examples of MF Crypto devices may include a smart card with an embedded digital certificate.

General Credential Guidance

Biometrics (for authentication use)

*This section relates to TDIF requirements **CSP-04-03-03** to **CSP-04-03-03n** of section **4.3.3** in the TDIF 05 Role Requirements.*

The use of biometrics (something you are) in authentication includes both measurement of physical characteristics (e.g. fingerprint, iris, facial characteristics) and behavioural characteristics (e.g. typing cadence). Both classes are considered biometric modalities, although different modalities may differ in the extent to which they establish authentication intent.

For a variety of reasons, the TDIF supports only limited use of biometrics for authentication. These reasons include:

- The biometric False Match Rate (FMR) does not provide confidence in the authentication of the Individual by itself. In addition, FMR does not account for spoofing attacks.
- Biometric comparison is probabilistic, whereas the other authentication factors are deterministic.
- Biometric template protection schemes provide a method for revoking biometric *Credential*s that is comparable to other authentication factors (e.g. PKI certificates

and passwords). However, the availability of such solutions is limited, and standards for testing these methods are under development.

- Biometric characteristics do not constitute secrets. They can be obtained online or by taking a picture of someone with a camera phone (e.g. facial images) with or without their knowledge, lifted from objects someone touches (e.g. latent fingerprints), or captured with high resolution images (e.g. iris patterns). While presentation attack detection (*PAD*) technologies (e.g. liveness detection) can mitigate the risk of these types of attacks, additional trust in the sensor or biometric processing is required to ensure that *PAD* is operating in accordance with the needs of the *CSP* and the *Individual*.

CSP-impersonation resistance

*This section relates to TDIF requirements **CSP-04-03-05** to **CSP-04-03-05f** of section **4.3.5** in the TDIF 05 Role Requirements.*

CSP-impersonation attacks, sometimes referred to as “phishing attacks,” are attempts by attackers to fool an unwary *Individual* into authenticating to an impostor website.

A *CSP-impersonation resistant authentication* protocol must establish an authenticated protected channel with a *CSP*. It must then strongly and irreversibly bind a channel identifier that was negotiated in establishing the authenticated protected channel (e.g. by signing the two values together using a private key controlled by the *Individual* for which the public key is known to the *CSP*). The *CSP* should validate the signature or other information used to prove *CSP-impersonation resistance*. This prevents an impostor posing as a *CSP*, even one that has obtained a certificate representing the actual *CSP*, from replaying that authentication on a different authenticated protected channel.

AACAs must be used to establish *CSP-impersonation resistance* where it is required. Keys used for this purpose must provide at least the minimum-security strength specified in the latest version of the *ISM*.

One example of a *CSP-impersonation resistant* authentication protocol is client-authenticated *TLS*, because the client signs the *Credential* output along with earlier messages from the protocol that are unique to the particular *TLS* connection being negotiated.

Credentials that involve the manual entry of a *Credential* output, such as *out-of-band* and *OTP Credentials*, are not considered *CSP-impersonation resistant* because the manual entry does not bind the *Credential* output to the specific session being authenticated. In a *Man-in-the-Middle (MitM)* attack, an impostor could replay the *OTP Credential* output to the *CSP* and successfully authenticate.

IDP-CSP Communications

*This section relates to TDIF requirements **CSP-04-03-06** of section **4.3.6** in the TDIF 05 Role Requirements.*

In situations where the *IDP* and *CSP* are separate entities (*IdP* and *CSP*) communications must occur through a mutually authenticated secure channel (such as a client-authenticated *TLS* connection) using approved *AACAs* and *AACPs*.

CSP-Compromise Resistance

*This section relates to TDIF requirements **CSP-04-03-07** to **CSP-04-03-07b** of section **4.3.7** in the TDIF 05 Role Requirements.*

Use of some types of *Credentials* requires that the *CSP* store a copy of the *authentication* secret. For example, an *OTP Credential* requires that the *CSP* independently generate the *Credential* output for comparison against the value sent by the *Individual*. Because of the potential for the *CSP* to be compromised and stored secrets stolen, *authentication* protocols that do not require the *CSP* to persistently store secrets that could be used for *authentication* are considered stronger and are described herein as being *CSP-compromise resistant*.

CSP-compromise resistance can be achieved in different ways, for example:

- Use a cryptographic *Credential* that requires the *CSP* store a public key corresponding to a private key held by the *individual*.
- Store the expected *Credential* output in hashed form. This method can be used with some *look-up secret Credentials* for example.

To be considered CSP-compromise resistant, public keys stored by the *CSP* must be associated with the use of *AACAs* and must provide at least the minimum-security strength specified in the latest published edition of the *ISM*.

Other *CSP-compromise resistant* secrets must use approved hash algorithms and the underlying secrets must have at least the minimum-security strength specified in the latest published edition of the *ISM*. Secrets (e.g. *memorised secrets*) having lower complexity must not be considered CSP-compromise resistant when hashed because of the potential to defeat the hashing process through dictionary lookup or exhaustive search.

Replay Resistance

*This section relates to TDIF requirements **CSP-04-03-10** of section **4.3.8** in the TDIF 05 Role Requirements.*

An *authentication* process resists replay attacks if it is impractical to achieve a successful *authentication* by recording and replaying a previous *authentication* message. *Replay resistance* is in addition to the replay resistant nature of *authenticated* protected channel protocols since the output could be stolen prior to entry into the protected channel. Protocols that use nonces or challenges to prove the "freshness" of the transaction are resistant to replay attacks since the *CSP* will easily detect when old protocol messages are replayed since they will not contain the appropriate nonces or timeliness data.

Examples of replay-resistant *Credentials* are *OTP* devices, cryptographic protocol (*AACP*) *Credentials*, and *look-up secrets*. In contrast, *memorised secrets* are not considered replay resistant because the *Credential* output — the secret itself — is provided for each *authentication*.

Authentication Intent

*This section relates to TDIF requirements **CSP-04-03-09** to **CSP-04-03-09b** of section **4.3.9** in the TDIF 05 Role Requirements.*

An *authentication* process demonstrates intent if it requires the *Individual* to explicitly respond to each *authentication* or reauthentication request. The goal of *authentication* intent is to make it more difficult for directly connected physical *Credentials* (e.g. *multi-factor cryptographic devices*) to be used without the *Individual's* knowledge, such as by malware on the endpoint. *Authentication* intent must be established by the *Credential* itself, although *multi-factor cryptographic devices* may establish intent by re-entry of the other *authentication factor* on the endpoint with which the *Credential* is used.

Authentication intent may be established in several ways. *Authentication* processes that require the *Individual's* intervention (e.g. an *Individual* entering an *Credential* output from an *OTP* device) establish intent. Cryptographic devices that require user action (e.g. pushing a button or reinsertion) for each *authentication* or reauthentication operation also establish intent.

Depending on the modality, presentation of a biometric may or may not establish *authentication* intent. Presentation of a fingerprint would normally establish intent, while observation of the *Individual's* face using a camera normally would not by itself. Behavioural biometrics similarly are less likely to establish *authentication* intent because they do not always require a specific action on the *Individual's* part.

Restricted *Credentials*

*This section relates to TDIF requirements **CSP-04-03-10** to **CSP-04-0311** of section **4.3.10** in the TDIF 05 Role Requirements.*

As threats evolve, a *Credential's* capability to resist attacks typically degrades. Conversely, some *Credentials'* performance may improve — for example, when changes to their underlying standards increases their ability to resist particular attacks.

To account for these changes in *Credential* performance, the *TDIF* places additional restrictions on *Credential* types or specific classes or instantiations of a *Credential* type.

The use of a *Restricted Credential* requires that the implementing organisation assess, understand, and accept the risks associated with that *Restricted Credential* and acknowledge that risk will likely increase over time. It is the responsibility of the organisation to determine the level of acceptable risk for their system(s) and associated data and to define any methods for mitigating excessive risks. If at any time the organisation determines that the risk to any party is unacceptable, then that *Restricted Credential* must not be used.

Furthermore, the risk of an *authentication* error is typically borne by multiple parties, including the implementing organisation, organisations that rely on the *authentication* decision, and the *Individual*.

Because the *Individual* may be exposed to additional risk when an organisation accepts a *Restricted Credential* and that the *Individual* may have a limited understanding of and ability to control that risk, the *CSP* must:

1. Offer *Individual's* at least one alternate *Credential* that is not Restricted and can be used to authenticate at the required CL.
2. Provide meaningful notice to *Individuals* regarding the security risks of the *Restricted Credentials* and availability of alternative(s) that are not Restricted.
3. Address any additional risk to *Individuals* in its risk assessment.
4. Develop a migration plan for the possibility that the *Restricted Credential* is no longer acceptable at some point in the future and include this migration plan in its *System Security Plan.*

Credential Lifecycle Management Guidance

*This section relates to TDIF requirements **CSP-04-04-01** to **CSP-04-04-09** of section **4.4** in the TDIF 05 Role Requirements.*

Credential Binding

*This section relates to TDIF requirements **CSP-04-04-01** to **CSP-04-04-01g** of section **4.4.1** in the TDIF 05 Role Requirements.*

Credential binding refers to the establishment of an association between a specific *Credential* and an *Individual's* account, enabling the *Credential* to be used — possibly in conjunction with other *Credentials* — to authenticate for that account.

Credentials must be bound to an *Individual's* account by either:

- Issuance by the *CSP* as part of enrolment; or
- Associating an *Individual*-provided *Credential* that is acceptable to the *CSP*.

The *TDIF* refers to the binding rather than the issuance of a *Credential* as to accommodate both options.

Throughout the *digital identity* lifecycle, *CSPs* must maintain a record of all *Credentials* that are or have been associated with each *digital identity*. The *CSP* must maintain the information for throttling authentication attempts when required. The *CSP* must also verify the type of *user*-provided *Credentials* (e.g. *single-factor cryptographic device* vs. *multi-factor cryptographic device*) so they can determine compliance with requirements at each *CL.*

The record created by the *CSP* must contain the date and time the *Credential* was bound to the account. The record should include information about the source of the binding and (e.g. IP address, device identifier) of any device associated with the enrolment. If available, the record should also contain information about the source of unsuccessful *authentications* attempted with the *Credential*.

When any new *Credential* is bound to an *Individual's* account, the *CSP* must ensure that the binding protocol and the protocol for provisioning the associated key(s) are done at a level of security commensurate with the *CL* at which the *Credential* will be used. For example, protocols for key provisioning must use authenticated protected channels or be performed in person to protect against *MitM*. Binding of multi-factors must require *multi-factor authentication* or equivalent (e.g. association with the *session* in which *identity proofing* has been just completed) be used to bind the *Credential*. The same conditions apply when a key pair is generated by the *Credential* and the public key is sent to the *CSP*.

Binding at enrolment

This section relates to TDIF requirements ***CSP-04-04-02*** *to* ***CSP-04-04-02a*** *of section* ***4.4.2*** *in the TDIF 05 Role Requirements.*

It is important that *Credentials* are bound to an *Individual's* account at enrolment to enable an *individual* access to their personal data established by the *identity proofing* process.

The *CSP* must bind at least one, and should bind at least two, physical (something you have) *Credentials* to the *Individual's digital identity*, in addition to a *memorised secret* or one or more biometrics. Binding of multiple *Credentials* is preferred in order to allow account recovery from the loss or theft of the *Individual's* primary *Credential*.

While all identifying information is self-asserted at *IP 1*, preservation of online material or an online reputation makes it undesirable to lose control of a *digital identity* account due to the loss of a *Credential*. The second *Credential* makes it possible to securely recover from loss of one of the primary *Credentials*. For this reason, a *CSP* should bind at least two *Credentials* to the *Individual's digital identity,* this includes at *IP 1* as well.

If enrolment and binding cannot be completed in a single physical encounter or electronic transaction (i.e., within a single protected *session*), the following methods must be used to ensure that the same *individual* acts as the *User* throughout the processes:

For remote online transactions:

1. The *User* must identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction or sent to the *User's* mobile phone number or email address.
2. Long-term *authentication* secrets must only be issued to the *User* within a protected *session*.

For in-person transactions:

1. The *User* must identify themselves in-person by either using a secret as described in the remote online transactions section (point 1) above, or through use of a biometric that was recorded during a prior encounter.
2. Temporary secrets must not be reused.
3. If the *CSP* issues long-term *authentication* secrets during a physical transaction, then they must be loaded locally onto a physical device that is issued in-person to the *User* or delivered in a manner that confirms the address of record.

Binding additional *Credentials*

*This section relates to TDIF requirements **CSP-04-04-03** to **CSP-04-04-05a** of section **4.4.3** in the TDIF 05 Role Requirements.*

Binding an additional authentication *Credential* to an existing CL

CSPs should permit the binding of additional *Credentials* to an *Individual's digital identity* account. Before adding the new *Credential*, the *CSP* must first require the *Individual* to authenticate at the *CL* (or a higher *CL*) at which the new *Credential* will be used. When a *Credential* is added, the *CSP* should send a notification to the *Individual* via a mechanism that is independent of the transaction binding the new *Credential* (e.g. an email to an address previously associated with the *Individual*). The *CSP* may limit the number of *Credentials* that may be bound in this manner.

Adding an additional factor to a Single-Factor account

If the *Individual's digital identity* account has only one *authentication factor* bound to it (i.e., at *IP1 / CL1*) and an additional *Credential* of a different *authentication factor* is to be added, the *Individual* may request that the account be upgraded to *CL 2*. The *IP Level* would remain at *IP 1.*

Before binding the new *Credential*, the *CSP* must require the *Individual* to authenticate at *CL 1*. The *CSP* should send a notification of the event to the *Individual* via a mechanism independent of the transaction binding the new *Credential* (e.g. an email to an address previously associated with the *Individual*).

Binding a User-provided *Credential*

*This section relates to TDIF requirement **CSP-04-04-06** of section **4.4.4** in the TDIF 05 Role Requirements.*

An *Individual* may already possess *Credentials* suitable for *authentication* at a particular *CL*. For example, they may have a *multi-factor Credential* from a social network provider, considered *CL 2* and *IP 1*, and would like to use that *Credential* at a *Relying Party* that requires *IP 2.*

CSPs should, where practical, accommodate the use of *Individual*-provided *Credentials* to relieve the burden to the *Individual* of managing many *Credentials*. In situations where the *Credential's* strength is not self-evident (e.g. between *single-factor* and *multi-factor Credentials* of a given type), the *CSP* should assume the use of the weaker *Credential* unless it is able to establish that the stronger *Credential* is in fact being used (e.g. by *verification* with the issuer or manufacturer of the *Credential*).

Renewal

*This section relates to TDIF requirements **CSP-04-04-07** to **CSP-04-04-08** of section **4.4.5** in the TDIF 05 Role Requirements.*

The *CSP* should bind an updated *Credential* an appropriate amount of time before an existing *Credential's* expiration. The process for this should conform closely to the initial *Credential's* binding process (e.g. confirming address of record). Following successful use of the new *Credential*, the *CSP* should revoke the *Credential* that it is replacing.

Loss, theft, damage and unauthorised duplication

*This section relates to TDIF requirements **CSP-04-05-01** to **CSP-04-05-06** of section **4.5** in the TDIF 05 Role Requirements.*

Compromised *Credentials* include those that have been lost, stolen or subject to unauthorised duplication. Generally, one must assume that a lost *Credential* has been stolen or compromised by someone that is not the legitimate *Individual* to whom the *Credential* is bound to*.* Damaged or malfunctioning *Credentials* are also considered compromised to guard against any possibility of extraction of the *Credential* or secret. One notable exception is a *memorised secret* that has been forgotten without other indications of having been compromised, such as having been obtained by an attacker.

Suspension, revocation or destruction of compromised *Credentials* should occur as promptly as practical following detection. *CSPs* should establish time limits for this process.

To facilitate secure reporting of the loss, theft or damage to a *Credential*, the *CSP* should provide the *Individual* with a method of *authenticating* to the *CSP* using a backup or alternate *Credential*. This backup *Credential* may be either a *memorised secret* or a physical *Credential*. Either may be used, but only one *authentication factor* is required to make this report. Alternatively, the *Individual* may establish an authenticated protected channel to the *CSP* and verify information collected during the *identity proofing* process. The *CSP* may choose to verify an address of record (e.g. email, mobile phone number) and suspend *Credential*(s) reported to have been compromised. The suspension must be reversible if the *Individual* successfully *authenticates* to the *CSP* using a valid (i.e., not suspended) *Credential* and requests reactivation of an *Credential* suspended in this manner. The *CSP* may set a time limit after which a suspended *Credential* can no longer be reactivated.

Credential expiration

This section relates to TDIF requirements ***CSP-04-06-01*** *to* ***CSP-04-06-01b*** *of section* ***4.6*** *in the TDIF 05 Role Requirements.*

CSPs may issue *Credentials* that expire. If and when a *Credential* expires, it must not be usable for *authentication*. When an *authentication* is attempted using an expired *Credential*, the *CSP* should give an indication to the *Individual* that the *authentication* failure is due to expiration rather than some other cause.

The *CSP* must require *Individuals* to surrender or prove destruction of any physical *Credential* containing *attribute* certificates signed by the *CSP* as soon as practical after expiration or receipt of a renewed *Credential*.

Credential revocation and termination

This section relates to TDIF requirements ***CSP-04-07-01*** *to* ***CSP-04-07-02*** *of section* ***4.7*** *in the TDIF 05 Role Requirements.*

CSPs must revoke the binding of *Credentials* promptly when a *digital identity* ceases to exist (e.g. an *individual's* death, discovery of a fraudulent *individual*), when requested by the *individual* or when the *CSP* determines that the *individual* no longer meets its eligibility requirements.

The *CSP* must require *individuals* to surrender or certify destruction of any physical *Credentials* containing attributes digitally signed by the *CSP* as soon as practical after revocation or termination takes place. This may be necessary to block the use of the

Credential's digitally signed attributes in offline situations between revocation or termination and expiration of the key.

Session management

This section relates to TDIF requirements ***CSP-04-08-01*** *to* ***CSP-04-08-01b*** *of section* ***4.8*** *in the TDIF 05 Role Requirements.*

Once an *Individual* has authenticated, it is often desirable to allow them to continue using the application across multiple subsequent interactions without the need to repeat the authentication process. This requirement is particularly true for federation scenarios where authentication necessarily involves several components and parties coordinating across a network.

To facilitate this behaviour, a session may be started in response to an authentication event and continue the session until such time that it is terminated. The session may be terminated for any number of reasons, including but not limited to an inactivity timeout, an explicit logout event, or other means. The session may be continued through a reauthentication event wherein the *Individual* repeats some or all of the initial authentication process, thereby re-establishing the session. Session management is preferable over continual presentation of *Credential*s as the poor usability of continual presentation often creates incentives for workarounds such as cached unlocking *Credential*s, negating the freshness of the authentication process.

The ISM contains further security controls related to session management See: https://www.cyber.gov.au/acsc/view-all-content/ism

Attribute Service Provider Guidance

Attribute Service Providers are *TDIF* accredited organisations or government agencies that manage *attributes* relating to people and *non-person entities*. The role of an *Attribute Provider* is to represent an authoritative source for a selected set of authorisation, qualification, or entitlement *Attributes* under the *TDIF*.

Attributes are provided to *Relying Parties* on behalf of a *person* or *non-person entity* to support their decision-making processes.

Attribute Service Providers differ from *IdPs* in that they assert one or more *attributes* about a *person* or *non-person entity* relating to authorisations, qualifications, or entitlements, rather than about a *person's identity* information. Whereas an *IdP* verifies the *identity attributes* of a person (e.g. I am Sue Jones), an *Attribute Provider* verifies specific *attributes* relating to entitlements, qualifications or characteristics of that *person* (e.g. this Sue Jones is authorised to act on behalf of business xyz in a particular capacity).

The Australian Taxation Office *(ATO)* Relationship Authorisation Manager *(RAM)* is an example of a service that can be used by individuals and businesses to set up and manage relationships and authorisations across government online services to manage who can act on behalf of their business online. See: https://info.authorisationmanager.gov.au/

Attribute Classes

*Relates to TDIF requirements **ASP-05-01-01** to **ASP-05-01-03** of section **5.1** in the TDIF 05 Role Requirements.*

Attribute Service Providers can provide several different classes of *attributes*:

- Authorisation.
- Qualification.
- Entitlement.
- Self-Asserted.
- Platform.

A description of the *Attribute classes* is outlined in **Table 5** of section **5.1** of the *TDIF: 05 - Role Requirements*.

Authorisation

Broadly speaking, in the *TDIF,* authorisation refers to the ability for an authenticated *person* to act on behalf of another *entity*.

Types of authorisations include:

- The authorisation for a *person* to act on behalf of a non-person or organisational *entity*.
- The authorisation for a non-person or organisational entity to act on behalf of a *person.*
- The authorisation for a *person* to act on behalf of another *person.*

In general:

- Authorisation *attributes* are managed by an accredited *Attribute Service Provider (ASP)*.
- An *ASP* connected to an IdP enables a *person* to *authenticate* using their *digital identity* to:
    a) Establish authorisation *attributes* and associate them to their *digital identity*.
    b) Manage authorisation *attributes*.
- Authorisation *attributes* can be shared with *Relying Parties* so that the authorisation can be used by the *person* to access services at the *Relying Party*.

Identity Exchange Guidance

Identity Exchanges are *TDIF* accredited organisations or government agencies that convey, manage and coordinate the flow of *Identity Attributes* and *Assertions* between members of an *Identity Federation*.

Identity Exchanges operate a key role in an *Identity Federation*, however exactly how they do this will vary depending on the architecture of the *Identity Federation* that they are a part of. As a result, beyond the core audit logging and consent management requirements required to support its operation, the requirements in section 6 are mostly optional for an *Identity Exchange*.

Guidance on Audit Logging

Relates to TDIF requirements ***IDX-06-01-01*** *to* ***IDX-06-01-02*** *of section 6.1 in the TDIF 05 Role Requirements.*

An *Identity Exchange* generates a unique Audit Id for each *Authentication Request* and logs this *Authentication Request* from the *Relying Party*, including logging the audit ID. The audit ID is stored alongside the names of the *Attributes* that were shared in that request, but not the values of the *Attributes* themselves. How it does this is up to an *Identity Exchange's* discretion—if, in doing so, they are complying with the other requirements of an *Identity Exchange,* including those set out in the *TDIF 04 – Functional Requirements.*

Information logged by an *Identity Exchange* is limited to that required to meet forensic and non-repudiation requirements defined by the *TDIF*. The name of identity *Attributes* that were shared via the *Identity Exchange* will be retained as part of the audit history, but the values of these attributes will not be retained, as described in the *TDIF: 04 - Functional Requirements*.

Guidance on Consent Management

Relates to TDIF requirements ***IDX-06-02-01*** *of section 6.2 in the TDIF 05 Role Requirements.*

These requirements operate in addition to the consent storage requirements of an *Identity Exchange* set out in section 3.9 of the TDIF 04 Functional Requirements. They set out additional information that an Identity Exchange is required to store in their *audit logs* as part of recording the *Express Consent* given by a *User,* as required by PRIV-03-09-03.

Guidance for Single Sign-on/Single Logout

Relates to TDIF requirements ***IDX-06-03-01*** *to* ***IDX-06-03-04*** *of section 6.3 in the TDIF 05 Role Requirements.*

Single sign-on is an optional feature that an *Applicant* may implement in their system.

Single Sign-On

Single Sign-on (SSO) refers to the ability for a *User* to make use of their *Digital Identity* at multiple services in a short period of time, with only a single *User Authentication*. For example, where two or more services or transactions would normally each require a *User Authentication* event, and if these transactions are completed within a reasonable timeframe and the same web browser session, then their *Digital Identity* information can be cached in an authentication *Session* and reused by the *Identity Exchange*.

A possible implementation of this is for an *Identity Exchange* to create an *Authentication Session* for the *User*, storing their core *Attributes* for the duration of the *Session* in an encrypted cookie in the *User's* browser. This cookie can then be used to satisfy an *Authentication Request* sent by a *Relying Party*. If the cookie is unable to satisfy the *Authentication Request*, or the *Relying Party* has requested that the *User* authenticate regardless of an existing *Session*, then the *Identity Exchange* will send the *User* to an *Identity Service Provider* to *Authenticate*.

There are times when a *Relying Party* has determined that it wants the *User* to *Authenticate* at the *Identity Service Provider* regardless of a pre-existing *Authenticated Session* at the *Relying Party* or an *Identity Exchange*. This could occur when the *User* accesses a higher risk transaction. In this instance, a *Relying Party* may inform the *Identity Exchange* that it requires the user to authenticate.

If the *Relying Party* is utilising the *SAML Federation protocol*, this can be done using the ForceAuthn attribute. If the *Relying Party* is utilising the *OIDC Federation Protocol* this can be done using the `login` value for the prompt parameter.

Single Logout

Single Logout (SLO) refers to the ability for a user to initiate a logout process for all *Relying Parties* that relied on a single logon *Session* for the *User* at an *Identity Exchange*.

Standard *Federation Protocols* generally provide two mechanisms for enabling single logout that can be characterised as follows:

- Front-channel *Single Logout*. The front-channel single logout model uses front-channel communication via the user agent (web browser).

- Back-channel *Single Logout*. The back-channel single logout model relies on direct server to server communication between the *Session* participants.

The TDIF does not include requirements specifying a particular mechanism for an *Identity Exchange* to achieve *single Logout* in their *Identity Federation*.

Guidance for User Dashboards

*Relates to TDIF requirements **IDX-06-04-01** to **IDX-06-04-03** of section 6.4 in the TDIF 05 Role Requirements*

A *User Dashboard is* an optional feature that an *Applicant* may implement in their system.

The *User Dashboard* is a collective term for the features that an *Identity Exchange* provides to a *User* that has been *Authenticated* by a *Credential Service Provider*. This includes:

- Access to the *Consumer History*, which is the history of all the *User's* interactions performed via an *Identity Exchange* using the *Identity Service Provider* they are using to access the *User Dashboard*.
- Ability to revoke ongoing *Consent* to shared *Attributes* with a *Relying Party*.

The *Consumer History* is a historical record of all federated identity interactions that relate to a *Digital Identity*. This includes any requests and responses between:

- A *Relying Party* and an *Identity Exchange*.
- An *Identity Service Provider* and an *Identity Exchange*.
- An *Attribute Service Provider* and an *Identity Exchange*.

No identity *Attribute* values are stored in the *Consumer History*.

The information available to be viewed about a transaction at the *User Dashboard* includes:

- The date and time of the transaction
- The attributes requested by a *Relying Party*.
- *Consent* provided.
- *Attributes* returned to a *Relying Party* (but not the actual values returned).

The *User* will need to be *Authenticated* by an *Identity Service Provider* to access the *User Dashboard*.

Guidance for IdP Selection

Relates to TDIF requirements ***IDX-06-05-01*** *to* ***IDX-06-05-03b*** *of section 6****.5*** *in the TDIF 05 Role Requirements.*

An *Identity Exchange* may provide a method for an *Individual* to select an *Identity Service Provider* from a list of *Identity Service Providers* that are integrated with the *Identity Exchange* when accessing a *Relying Party*. This is known as *IdP Selection.*

IdP Selection is comprised of the following:

- Filtering of the available *Identity Service Providers* to the subset of *Identity Service Providers* integrated with an *Identity Exchange* that are accredited to meet the *Identity Proofing Level* required by the *Relying Party* and are connected to *Credential Service Providers* able to provide the *Credential Level* requested.
- Interacting with the *User* so they can choose their preferred *Identity Service Provider*.

- Providing the *User* with the option to remember their *Identity Service Provider* selection. The end-to-end service design must provide a mechanism for the User to change this preference and will inform whether there is a need for an *Identity Exchange* to persist this preference server-side.

Appendix A – Biometric Verification Use Case

Biometric binding

The following use case covers the *Applicant* creation of an *identity* at *IP 2 Plus*. This includes the generic use cases for Online *Biometric Binding* and *Local Biometric Binding.* At a high level, this includes a check of the document either via *DVS*, security certificate check, and visual inspection, and a check of the face against either the document *RFID* chip, via *FVS*, or by visual inspection.

Roles

The roles associated with this use case are:

- *Applicant*
- *User*
- *Photo ID Issuing Authority*

This use case covers the *Users* provision of the *Acquired Image*, the *Applicant* processing of the *Acquired Image*, the matching of the *Acquired Image* to the image held by the *Photo ID Issuing Authority* and the return of a matching result.

Basic Flow

- The *User* accesses the *Applicant Capability*

- The *User* submits required information fulfilment to the *Applicant* including the provision of two or more documents using the *Applicant Capability*.

- The documents are verified either via *DVS* check, security certificate check (ePassport only), or visual inspection (*Local Biometric Binding* only).

- The *User* submits the *Acquired Image* through the *Applicant's* face image acquisition process.

- The *Applicant* completes biometric quality assessment (*Online Biometric Binding*).
- The *Applicant* completes *Presentation Attack Detection* (*Online Biometric Binding*).
- Matching is undertaken either against the document *RFID* chip, via *FVS*, or by *visual verification* (*Local Biometric Binding* only).
- The *Applicant* collects required data for audit (matching, *presentation attack* data, *personnel* details). Note that this does not include retention of face images.
- *IP2 Plus* is granted to the *User's digital identity*.

At this point the *User* can now complete the action that requires the *IP2 Plus* privilege (e.g. large financial transaction).

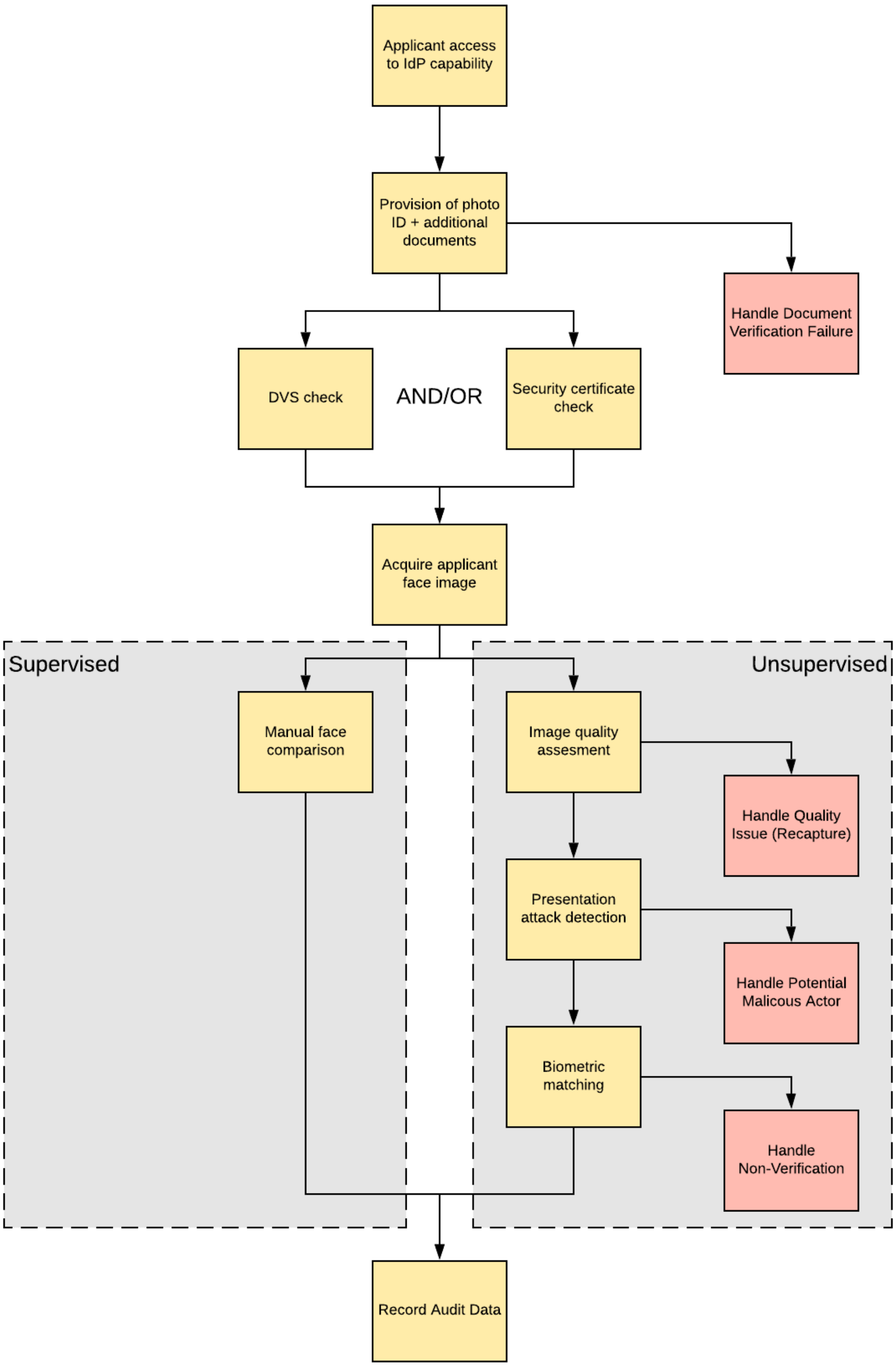
Alternative flows are executed if there is a failure at any stage in the specified flow (e.g. handling detection of *presentation attacks*).

Success Criteria

If the *User's Acquired Image* matches the image stored in the *Authoritative Source*, *verification* is successful and *IP2 Plus* is provided.

Else *IP2 Plus* is not provided.

Flow Diagram


Applicant access to IdP capability
Provision of photo ID + additional documents
Handle Document Verification Failure
DVS check
AND/OR
Security certificate check
Acquire applicant face image
Supervised
Unsupervised
Manual face comparison
Image quality assesment
Handle Quality Issue (Recapture)
Presentation attack detection
Handle Potential Malicous Actor
Biometric matching
Handle Non-Verification
Record Audit Data