Australian Government
Digital Transformation Agency

05A - Role Guidance

Trusted Digital Identity Framework Release 4
February 2021, version 1.2

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 Participants*, 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 the Director, Digital Identity Policy at identity@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

Document review

The next scheduled review of this document will occur by July 2022. Any changes made to the document prior to this date will be recorded in a *TDIF* change management document and published to the *DTA* website.

Contents

Introduction

This document provides guidance to *Applicants* undergoing *Accreditation* on how to meet the *TDIF: 05 - Role Requirements.* Over time this document will be updated with specific guidance for meeting *TDIF* requirements and how the DTA will assess compliance. 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 Participants*.
- *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 the *TDIF* requirements.

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

Identity Service Provider Guidance

Identity proofing concepts

Identity Proofing Objectives

Establishing confidence in an individual's *identity* is a critical starting point for delivering a range of *digital services* and benefits, as it is for many transactions conducted by the private sector and other non-government organisations. The objective of *identity proofing* is to verify an individual's *identity* information to obtain a reusable *digital identity*.

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.

The *TDIF Evidence of Identity (EoI)* document categories.

- *Commencement of Identity (CoI)*
- *Linking document*
- *Use in the Community* (UitC) and
- *Photo ID*.

UitC documents provide historical evidence of the *identity* operating in the community over time and, as per all *UitC verification* activities, can only be undertaken after the individual's name has been verified. A *UitC* document is used as an alternative option when the *person* does not provide evidence that can be verified via an approved *UitC* document.

Further information regarding *EoI* documents is outlined at 3.1.2 of the *TDIF: 05 – Role Requirements* document.

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
- ***Technical Verification*** - the act of verifying physical or electronic evidence using an *Australian Signals Directorate Approved Cryptographic Algorithm* bound to a secure chip or appended to
- **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.

A full description of *Verification* methods is outlined in section 3.1.3 of the *TDIF: 05 - Role Requirements* document.

Identity Proofing Levels

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 between the individual and the evidence of identity.*
- *Confirmation that an identity is not known to be used fraudulently.*

As a result of these objectives being met at different levels of assurance across the IPs the *Relying Party* can have a degree of confidence, depending on the IP achieved, that:

- The *claimed identity* has been resolved to a unique individual.
- The supplied *identity* evidence has been confirmed as legitimately existing, correct and genuine.
- The *claimed identity* exists and accepted as operating in the real world.
- The *claimed identity* has been verified as being associated with and bound to the individual supplying the *identity* evidence.
- The *claimed identity* is not known to be fraudulent.

The *TDIF*'s *Identity Proofing* (*IP*) *Levels* are:

- ***Identity Proofing Level 1*** is used when no i*dentity 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 IP1 is for services where the risks of not undertaking identity verification will have negligible consequences to the individual. 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 three 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.*

Appendix A outlines the *Identity* proofing objectives, levels and document combinations.

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* themselves in order to meet the required *Identity Proofing Level*.

Guidance for cases where *Individuals* are unable to meet *Identity Proofing* requirements and alternative *Identity Proofing* processes that may be implemented to support exception cases are outlined in Section 3.3 of the *TDIF:05 Role Requirements.*

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 7 (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.

Attributes to be verified, validated and recorded

*Relates to TDIF requirements **IDP-03-06-01** to **IDP-03-06-04** of section **3.6** in the TDIF 05 Role Requirements.*

Attributes to be verified, validated and recorded are outlined in Section 3.6 Table 2 and Table 3 of the *TDIF: 05 Role Requirements*.

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.*

Biometric Verification Guidance

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

In order to conduct business in an online world, people need to be able to identify themselves remotely and reliably. In most cases however, it is not sufficient for them to simply make the *assertion* that "I am who I say I am - believe me." A *Relying Party* needs to be able to know to some degree of certainty that a presented electronic *identity credential* truly represents the *person* presenting the *credential*. Therefore, from a *Relying Party*'s perspective, the requirement to establish both confidence in a *person's identity* and the *credential* used to *authenticate* their *identity* is central to delivering online trusted services and benefits.

Within the *identity federation*, the provision of *identity* and *credential* services are provided by *IdPs* and *CSPs* respectively. While an agency or organisation can provide either or both services, for the purposes of *accreditation* the requirements related to *credentials* have been separately defined.

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.*

*Applicant*s that undergo the *TDIF Accreditation Process* should note the following:

- 'SHALL' and '*MAY*' statements in *NIST* should be read to mean '*MUST'* and '*MAY'* statements in the *TDIF*, respectively. 'SHOULD' statements in *NIST* should also be read as '*MAY'* statements in the *TDIF*.
- *NIST* Authenticator Assurance Levels (AAL) should be read as *TDIF Credential Level* (*CL*).
- *NIST* 'authenticator' requirements should be read as *TDIF credential* requirements.
- And time records management requirements in *NIST* 800-63B are subject to applicable Australian laws, regulations and policies including those set out in the *Archives Act 1983* (Cth).
- All requirements in *NIST* 800-63B are subject to the requirements set out in *TDIF: 04 - Functional Requirements*.

Source:
NIST SP 800-63B is available online. See:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

Credential Levels

Relates to TDIF requirements ***CSP-04-01-01*** *to* ***CSP-04-01-02*** *of section* ***4.1*** *in the TDIF 05 Role Requirements.*

The *TDIF* has three C*redential 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 an *identity* risk *assessment*.

Credential Level 1 provides some assurance that the *person controls* a *credential* bound to their *IdP* account. At a minimum, a single factor authentication is used for *Credential Level 1*.

A wide range of single factor credentials can be employed as well as any of the higher assurance authentication methods used at CL2-3. Refer to *NIST SP* 800-63B section 4.1 for *credential* guidance and examples of options.

Credential Level 2 provides a moderate confidence that the *person controls credential*(s) bound to their *IdP* account. MFA is used for *Credential Level 2*. Refer to *NIST SP* 800-63B section 4.2 for *credential* guidance and examples of options.

Credential Level 3 provides a high confidence that the *person controls credential*(s) bound to their *IdP* account. MFA that includes a *credential* that is hard-ware based and a protocol that provides verifier impersonation-resistance is used for *Credential Level 3*.

There are strong processes and protocols for verifying *credentials* with this strength, and more rigorous system and security requirements for verifier and re-authentication services.

Refer to *NIST SP* 800-63B section 4.3 for *credential* guidance and examples of options. See: https://pages.nist.gov/800-63-3/sp800-63b.html#sec4

Credential Lifecycle Management

Relates to TDIF requirements ***CSP-04-01-03*** *to* ***CSP-04-01-05b*** *of section* ***4.1.1*** *in the TDIF 05 Role Requirements.*

Within the *TDIF* it is the *CSP,* via their symbiotic relationship with the *IdP*, who is responsible for all processes relevant to the lifecycle 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 lifecycle 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.

Further guidance in relation to *credential* lifecycle and *session* management events is outlined in section 6 *Authenticator Lifecycle Management* and section 7 *Session Management* of *NIST SP* 800-63B. See: https://pages.nist.gov/800-63-3/sp800-63b.html#sec6

Credential and verifier guidance

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

Credentials come in many different forms and there are a wide variety of authentication technologies that may be used with them. The following examples of *credentials* that may be issued and managed by the *CSP* and includes:

- *Memorised Secret*
- *Look-Up Secret*
- *Out-of-Band Device*
- *Single-Factor One-Time-Password (OTP) Device*
- *Multi-Factor OTP Device*

- *Single-Factor Cryptographic Software*
- *Single-Factor Cryptographic Device*
- *Multi-Factor Cryptographic Software*
- *Multi-Factor Cryptographic Device*

For guidance on the specific requirements for each *CL* applicable to the different types of *credentials* refer to section 5 – *Authenticator and Verifier Requirements* of *NIST SP* 800-63B. This document describes types of authentication processes, authenticators, and other recommendations in relation to digital identity systems. This includes a focus on authentication of subjects interacting with government systems over open networks.

NIST SP 800-63B is available online. See: https://pages.nist.gov/800-63-3/sp800-63b.html.

General credential guidance

*Relates to TDIF requirements **CSP-04-03-01** to **CSP-04-03-10** of section **4.3** in the TDIF 05 Role Requirements.*

Physical Credentials

Refer to section 5.2.1 *Physical Authenticators* of *NIST SP 800-63B.*

Rate Limiting (throttling)

Refer to section 5.2.2 *Rate Limiting (Throttling)* of *NIST SP 800-63B.*

Biometrics (for authentication use)

Refer to section 5.2.3 *Use of Biometrics* of *NIST SP 800-63B.*

Attestation

Refer to section 5.2.4 *Attestation* of *NIST SP 800-63B.*

Verifier-impersonation resistance

Refer to section 5.2.5 *Verifier Impersonation Resistance* of *NIST SP 800-63B.*

Verifier-CSP communications

Refer to section 5.2.6 *Verifier-CSP Communications* of *NIST SP 800-63B.*

Verifier-compromise resistance

Refer to section 5.2.7 *Verifier-Compromise Resistance* of *NIST* SP *800-63B.*

Replay resistance

Refer to section 5.2.8 *Replay Resistance* of *NIST SP 800-63B.*

Authentication intent

Refer to section 5.2.9 *Authentication Intent* of *NIST SP 800-63B*.

Restricted Credentials

Refer to section 5.2.10 *Restricted Authenticators* of *NIST SP 800-63B.*

Credential lifecycle management

*Relates to TDIF requirements **CSP-04-04-01** to **CSP-04-04-07** of section **4.4** in the TDIF 05 Role Requirements.*

Credential Binding

Refer to section 6.1 *Authenticator Binding* of *NIST SP 800-63B*.

Binding at enrolment

Refer to section 6.1.1 *Binding at Enrolment* of *NIST SP 800-63B.*

Post-enrolment binding

Refer to section 6.1.2.1 *Binding of an Additional Authenticator at Existing AAL* of *NIST SP 800-63B.*

Binding to a User-provided credential

Refer to section 6.1.3 *Binding to a Subscriber-provided Authenticator* of *NIST SP 800-63B.*

Renewal

Refer to section 6.1.4 *Renewal* of *NIST SP 800-63B.*

Loss, theft, damage, and unauthorised duplication

*Relates to TDIF requirement **CSP-04-05-01** of section **4.5** in the TDIF 05 Role Requirements.*

Refer to section 6.2 *Loss, Theft, Damage, and Unauthorized Duplication* of *NIST SP 800-63B.*

Expiration

*Relates to TDIF requirement **CSP-04-06-01** of section **4.6** in the TDIF 05 Role Requirements.*

Refer to section 6.3 *Expiration* of *NIST SP* 800-63B.

Revocation and termination

*Relates to TDIF requirement **CSP-04-07-01** of section **4.7** in the TDIF 05 Role Requirements.*

Refer to section 6.4 *Revocation and Termination* of *NIST SP 800-63B.*

Session Management

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

Session bindings

Refer to section 7.1 *Session Bindings* of *NIST SP 800-63B.*

Browser cookies

Refer to section 7.1.1 *Browser Cookies* of *NIST SP 800-63B.*

Access tokens

Refer to section 7.1.2 *Access Tokens* of *NIST SP 800-63B.*

Device identification

Refer to section 7.1.3 *Device Identification* of *NIST SP 800-63B.*

Reauthentication

*Relates to TDIF requirement **CSP-04-09-01** of section **4.9** in the TDIF 05 Role Requirements.*

Refer to section 7.2 *Reauthentication* of *NIST SP 800-63B.*

Attribute Service Provider Requirements

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 6 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*.

Appendix A – Identity Proofing objectives, levels and document combinations

	IP 1	IP 1 Plus	IP 2	IP 2 Plus	IP 3	IP 4
***Identity proofing* objectives**	Claimed *identity* meets: • Uniqueness	Claimed *identity* meets: • Uniqueness • Legitimacy • Fraud Control	Claimed identity meets: • Uniqueness • Legitimacy • Operation • Fraud Control	Claimed identity meets: • Uniqueness • Legitimacy • Operation • Binding • Fraud Control	Claimed *identity* meets: • Uniqueness • Legitimacy • Operation • Binding • Fraud Control	Claimed *identity* meets: • Uniqueness • Legitimacy • Operation • Binding • Fraud Control
EOI requirements	NIL	1 *Photo ID* OR 1 UITC that can verify both name and date of birth	1 CoI OR 1 *Photo ID* AND 1 UiTC AND *Linking documents* (where necessary)	1 *Photo ID OR CoI* AND 1 UiTC AND *Linking documents* (where necessary)	1 CoI AND 1 *Photo ID* AND 1 UiTC, AND *Linking documents* (where necessary)	1 CoI AND 1 *Photo ID* AND 1 UiTC, AND Interview AND *Linking documents* (where necessary)

	IP 1	IP 1 Plus	IP 2	IP 2 Plus	IP 3	IP 4
Intended use	For transactions where no *verification* is required, but the parties desire a continuing conversation (e.g. post in a discussion forum) 'trusted'/ privileged positions)	For very low risk or services where *fraud* will have minor consequences (e.g. provision of loyalty cards)	For low risk or services where *fraud* will have minor consequences (e.g. provision of utility services)	For moderate risk or services where *fraud* will have moderate consequences and *legitimacy objective* is less important (e.g. access to common government services or undertaking financial transactions).	For moderate risk or services where *fraud* will have moderate consequences (e.g. access to common government services or undertaking financial transactions).	For high risk or services where major consequences arise from fraudulent verifications. (e.g. for secure access or 'trusted'/ privileged positions)
Whether Face matching is required	Pseudonymity is supported, but not anonymity	Face matching is not required	Face matching is not required	Face matching is required	Face matching is required	Face matching and In-person interview required

Appendix B – 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).

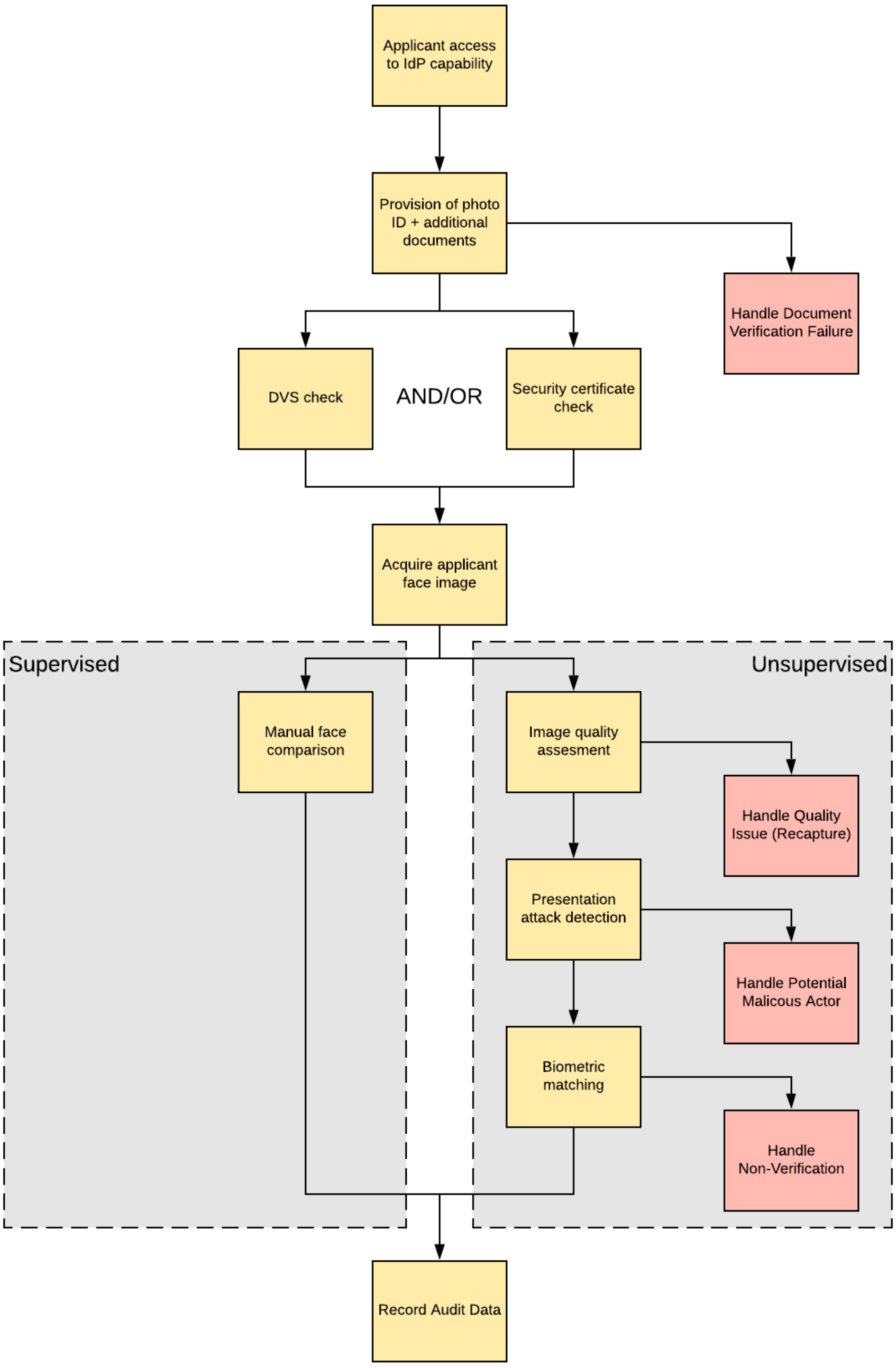
Alternative flows are executed if there is a failure at any stage in the specified flow (e.g. handling detection of *presentation attacks*).

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