Australian Government

Digital Identity

05 Role Requirements

Trusted Digital Identity Framework

Release 4.8 – Feb 2023

PUBLISHED VERSION

Department of Finance (Finance)

Licence

Use of the Coat of Arms

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

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

Finance 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 digitalid@finance.gov.au

Document management

Finance has reviewed and endorsed this document for release.

Change log

Document Version	Release Version	Date	Author	Description of the changes
0.1		July 2019	SJP	Initial version
0.2		Oct 2019	SJP	Updated to incorporate feedback provided by stakeholders during the first round of collaboration on TDIF Release 4
0.3		Dec 2019	SJP	Updated to incorporate feedback provided by stakeholders during the second round of collaboration on TDIF Release 4
0.4		Mar 2020	SJP	Updated to incorporate feedback provided during the third consultation round on TDIF Release 4
1.0	4.0	May 2020		Published version
1.1	4.0	Aug 2020	MC	Minor updates to Tables 1 and 5
1.2	4.0	Sep 2020	MC	Minor update to IP3 wording and Table 1 Operation Objective and update to Appendix A UiTC Document Concession Card.
1.3	4.1	Jan 2021	JK	CRID0005 – Emergency Change to CSP-04-01-05a – referenced requirement that did not exist. Corrected.
1.4	4.2	Feb 2021	JK, SJP	CRID0008 – Emergency Change to IDP-03-07-03 – referenced incorrect requirement.
1.5	4.3	Mar 2021	JK	CRID0017 – Emergency Change to IDP-03-08-21 – Temporary error while waiting for legislation to pass to implement
1.6	4.3	Mar 2021	AV, JK, SJP	Consultation Version – March 2021 version
1.7	4.4	Jun 2021	AV, JK, SJP	Published version CRID0006, CRID0009, CRID0012, CRID0016, CRID0018 – Changes to requirements, new requirements added, archived requirements: see Change Log for full list of requirements changes. Tables 1, 2, 3, 4 rewritten and reformatted.
1.8	4.5	Oct 2021	AV	CRID0027 – Emergency Change to Table 4
1.9	4.6	Mar 2022	AV, JK, DN, SJP, MS	Applicability of requirements added. Improvements to structure and clarity. Section 3.8 Biometric Binding Requirements updated See TDIF Change Log for full list and description of changes
1.10	4.7	June 2022	JK, AV	Appendix A clarifications. Addition of Convention Travel Document (Titre de Voyage) as CoI.
NA	4.8	Feb 2023		No changes to document

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

List of tables

1 Introduction

This document sets out the *TDIF* role requirements to be met by *Applicants* to achieve *TDIF* accreditation.

These *TDIF* role requirements do not replace, remove or diminish existing obligations imposed on organisations or government agencies through other policies, legislation or regulations, or by any other means. These *TDIF* role requirements supplement existing obligations and apply specifically to *Identity* services that undergo the *TDIF Accreditation Process*.

The intended audience for this document includes:

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

2 Common Role Requirements

2.1 User terms

TDIF Req: ROLE-02-01-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* have user terms in place between the *Applicant* and each *User* that include:

a) A general acknowledgment by the *User* that their use of the *Identity System* provided by the *Applicant* is governed by the User terms.
b) The scope of the *User's* right to access and use the *Identity System* must be consistent with the *TDIF*.
c) That the *User* is responsible for providing accurate *Identity Documents* and *Attributes* to the *Applicant*.
d) That the *User* is responsible for reporting unauthorised use of their *Digital Identity* or *Credential* to the *Applicant* as soon as they become aware of it.
e) That the *Applicant* may suspend, cancel or terminate the *User*'s access to the *Identity System* at any time.
f) That the *Applicant* may make changes to the User terms at any time without prior notice and if the User terms are changed, the *User*'s continued use of the *Identity System* will be subject to their acceptance of the updated User terms.
g) If applicable, that the *User's* access to the *Identity System* may be facilitated by third party services or software and the provider may require, enable or facilitate access to third party services or software.
h) That the *User* must comply with security requirements or instructions provided to them by the *Applicant*.
i) The governing law of the User terms
j) Provisions setting out a process for dispute resolution

TDIF Req: ROLE-02-01-01a; **Updated**: Mar-20; **Applicability**: A, C, I, X
The user terms *MUST NOT* be inconsistent with the requirements of the *TDIF*.

3 Identity Service Provider Requirements

3.1 Identity proofing concepts

Identity proofing concepts, descriptions and guidance is available in *TDIF 05A Role Guidance*.

The list of approved *Evidence of Identity (EoI) documents* that an *Identity Service Provider'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 are set out in Appendix A.

Descriptions of the *Identity Proofing Levels* are available in *TDIF: 05A Role Guidance*.

All Identity Proofing lifecycle management operations must be informed by the *Applicant's Fraud Control Plan* (FRAUD-02-02-01), *Privacy Policy* (PRIV-03-02-03) and *System Security Plan* (PROT-04-01-11a). These requirements can be found in *TDIF 04 Functional Requirements*.

3.2 Identity Proofing

TDIF Req: IDP-03-02-01; **Updated**: Mar-22; **Applicability**: I

The *Applicant* *MUST* support *Identity proofing* at the level of *Identity Proofing level 1 Plus* or above as described in *Table 1 Identity Proofing Levels*[1].

TDIF Req: IDP-03-02-02; **Updated**: Mar-22; **Applicability**: I

For each supported *Identity Proofing Level*, the *Applicant* *MUST* implement it in accordance with the requirements for that *Identity Proofing Level* set out in *Table 1 Identity Proofing Levels.*

TDIF Req: IDP-03-02-02a; **Updated**: Mar-22; **Applicability**: I

The *Applicant* MUST NOT make a representation, digitally or otherwise, that a *Digital Identity* has achieved a particular *Identity Proofing Level* unless the *Applicant* is accredited to support that *Identity Proofing Level*, and the *User* has achieved the requirements for that *Identity Proofing Level* as set out in Table 1 below

[1] This does not prevent an IdP from supporting IP1. Rather, TDIF accreditation will not be supported for Applicants that can only meet IP1 requirements.

Table 1: Identity Proofing Levels

Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
Intended use:	For very low-risk transactions where no verification of identity is required, but the parties desire a continuing conversation	For low-risk transactions or services where fraud will have minor consequences for the service or *User*	For moderate-risk transactions or services where fraud will have moderate consequences for the service or *User*	For moderate to high-risk transactions or services where fraud will have moderate to high consequences for the service or *User*	For high-risk transactions or services where fraud will have high consequences for the service or *User*	For very high-risk transactions or services where major consequences arise from fraudulent verifications.
***Identity Proofing* objectives**[2]	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
Uniqueness Objective						
***Identifier* chosen by the *Individual* is unique**	*MUST*	*MUST*	*MUST*	*MUST*	*MUST*	*MUST*
A check undertaken by the *IdP* to establish that the *Individual* is the sole claimant of the *Identity*[3]	-	*MUST*	*MUST*	*MUST*	*MUST*	*MUST*
Legitimacy Objective						

[2] See *TDIF 05A Role Guidance* for full descriptions of each proofing objective.

[3] This *MAY* be done through checking internal organisation records for an *Identity* with the same *Attributes*.

Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
A check undertaken by the *IdP* that the *identity* is not that of a deceased person	-	*MAY*	*MAY*	*MAY*	*MUST*	*MUST*
Binding Objective						
Confirmation of the link between the *individual* and the claimed *identity* by completing Biometric Binding in accordance with Section 3.8 Requirements for Biometric Binding	-	-	-	*MUST*	*MUST*	*MUST*
If completing Manual Face Comparison (as per section 3.8.6), then the original, physical *Photo ID* is to be provided in-person				*MUST*	*MUST*	*MUST*
ALL original, physical *EoI documents* to be provided and the individual witnessed in-person at IP4	-	-	-	-	-	*MUST*
Fraud Control Objective						
Checks to be undertaken against information or records held within the *IdP*[4] to confirm the *identity* is not known to be used fraudulently.	-	*MUST*	*MUST*	*MUST*	*MUST*	*MUST*
Checks to be undertaken against information on known fraudulent identities from other *Authoritative Sources*[5]	-	*MAY*	*MAY*	*MAY*	*MAY*	*MAY*
Other Requirements						
Personnel* performing *Identity Proofing* processes required to be provided with tools and training to detect fraudulent *Attributes* and *Identity	-	*MAY*	*MAY*	*MUST*	*MUST*	*MUST*

[4] Such as checks against internal registers of known fraudulent identities or vulnerable identities

[5] Such as law enforcement or other government agencies.

Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
Documents **before such** ***personnel*** **start work on those duties and annually thereafter.**[6]						
NAATI **accredited translation of identity documents in languages other than English required?**[7]	-	-	*MAY*	*MAY*	*MUST*	*MUST*
Attributes that MUST be verified with Source Verification or Technical Verification[8]	-	All names Date of Birth	All names Date of Birth	All names Date of Birth	All names Date of Birth	All names Date of Birth
Documents required for Verification	**IP1**	**IP1 Plus**	**IP2**	**IP2 Plus**	**IP3**	**IP4**
Verification of a ***CoI document MUST*** **be undertaken?**	-	-	Yes or *Photo ID* (see below)	Yes or *Photo ID* (see below)	Yes[9]	Yes[9]
Verification of a ***Photo ID MUST*** **be undertaken?**	-	Yes or UiTC (see below)[10]	Yes or CoI (see above)	Yes or CoI (see above)	Yes	Yes
Verification of a ***UiTC document MUST*** **be undertaken*?***	-	-	Yes x1	Yes x1	Yes x1	Yes x2
Verification of a ***Linking document MUST*** **be undertaken if** ***Attribute*****s vary across** ***EoI*** **documents?**	-	-	Yes	Yes	Yes	Yes
Verification of a ***UiTC document MUST*** **be undertaken that can confirm name and date of birth required?**	-	Yes or *Photo ID* (see above)[10]	-	-	-	-
Approved technical ***Credential*** **bindings**	CL1/CL2/CL3	CL1/CL2/CL3	CL2/CL3	CL2/CL3	CL2/CL3	CL3

[6] This may include training on recognition of document security features, particularly for foreign documents. Evidence of the training provided *MUST* be submitted to *Finance*.

[7] National Accreditation Authority for Translators and Interpreters. Further information is available at https:///www.naati.com.au/

[8] This requires all names and the date of birth of the *Individual* to be verified as part of the *Identity Proofing* process. It does not require every identity document to include these *attributes*.

[9] Australian Passports *MAY* be used for *CoI* and *Photo ID* for up to *IP3* proofing but *MUST NOT* be accepted as *CoI* for IP4 proofing.

[10] To satisfy the Operation Objective at *Identity Proofing Level 1 Plus*, the Individual's name and date of birth *MUST* be verified.

3.3 Individuals unable to meet Identity Proofing Requirements

Although most *Individuals* should be able to meet the requirements set out in Table 1, in some cases *Individuals* may face genuine difficulty in providing the necessary *EoI documents* themselves to the required *Identity Proofing Level*. The *IdP* may develop alternative *Identity Proofing* processes for these exception cases.
Exceptional Use Cases are those where an *Individual* does not possess, and is unable to obtain, the necessary information or *EoI documents* to the required *Identity Proofing Level*. This may include:

- *Individuals* whose birth was not registered.
- *Individuals* who are homeless or displaced.
- Undocumented arrivals to Australia.
- *Individuals* living in remote areas.
- *Individuals* who do not have enough *Identity Documents*, for example, foreign nationals living in Australia or Australians living in other countries.
- *Individuals* who do not have any *Identity Documents* but need a *Digital Identity*, for example, foreign nationals living outside Australia who need to access government systems or services.
- *Individuals* of diverse gender identity.
- *Individuals* of diverse sex.
- *Individuals* effected by natural disasters.
- *Individuals* with limited access to *Identity Documents*, for example, *Individuals* who were raised in institutional or foster care.
- *Individuals* with limited participation in society.
- Young people and those over 18 years who are yet to obtain *EoI documents*.

TDIF Req: IDP-03-03-01; **Updated**: Mar-22; **Applicability**: I
The *Applicant* MAY implement alternative *Identity Proofing* processes to the requirements set out in *Table 1 Identity Proofing Levels* to support *Exceptional Use Cases*.

TDIF Req: IDP-03-03-01a; **Updated**: Jun-21; **Applicability**: I

The alternative *Identity Proofing* processes *MAY* include:

- Acceptance of alternative types of *EoI* (for example, evidence of the operation of an *Identity* in a non-Australian community over time.
- Verification of an *Individual's* claimed *Identity* with a trusted referee whose *Identity* has been verified to an equal or greater *Identity Proofing Level*.
- Verification of an *Individual's* claimed *Identity* with reputable organisations or bodies known to them (for example, Aboriginal and Torres Strait Islander organisations may hold, or be able to verify, the *Identity* of *Individuals* where no prior government record exists).
- Reliance on the *Identity Proofing* processes of other organisations that have verified the *Identity* of the *Individual* (i.e. *Known Customer*)
- A detailed interview with the *Individual* about their life story to assess the consistency and legitimacy of their claims.
- Alternative methods of providing *Attributes* or *Identity Documents* (such as the provision of certified copies by trusted third parties instead of attending an in-person interview where an *Individual* can demonstrate they live in a very remote area).
- Providing support for *Individuals* to obtain evidence (such as assisting the *Individual* to register their birth with a *RBDM*)
- Any other processes or approaches supported by the IdP and consistent with requirement IDP-03-03-01b

TDIF Req: IDP-03-03-01b; **Updated**: Mar-22; **Applicability**: I

Before implementing an alternative identity proofing process under IDP-03-03-01, the *Applicant MUST*:

a) perform an assessment of the risk associated with implementing the alternative process and provide the risk assessment to *Finance*
b) Have in place mitigation methods and a plan to manage the risks of an alternative identity proofing process and provide the plan to *Finance*; and
c) Receive permission from *Finance* to perform an alternative *Identity Proofing* process and assert that it is equivalent to a particular *Identity Proofing Level*.

3.4 Identity proofing lifecycle management

***TDIF* Req:** IDP-03-04-01; **Updated:** Mar-22; **Applicability**: I
If the *Applicant* supports *Identity Proofing* Lifecycle Management[11], then the *Applicant* ***MUST*** implement the following requirements for the operation of Identity Proofing Lifecycle Management.

TDIF Req: IDP-03-04-01a; **Updated**: Mar-20; **Applicability**: I
The *Applicant* ***MUST*** allow *Individuals* to update their *Attributes* held by the *Applicant*.

TDIF Req: IDP-03-04-01b; **Updated**: Mar-20; **Applicability**: I
The *Applicant* ***MUST*** verify updates to the *Individual's Identity* prior to making changes to the *Individual's Digital Identity*. This includes any status changes made to the *Individual's Digital Identity* (e.g. temporary suspension or reactivation).

TDIF Req: IDP-03-04-01c; **Updated**: Mar-20; **Applicability**: I
Where unusual transactions are detected, the *Applicant* ***MUST*** verify the *Digital Identity* is still under the control of its legitimate account holder.

TDIF Req: IDP-03-04-02; **Updated**: Mar-22; **Applicability**: I
When requested to do so by an *Authorised Representative* or a *User*, the *Applicant* ***MUST*** either:

a) suspend the use of a *Digital Identity* for the period requested; or
b) deactivate the *Digital Identity*.

TDIF Req: IDP-03-04-02a; **Updated**: Mar-20; **Applicability**: I
The *Applicant* ***MUST*** confirm the legitimacy of any request by a *User* to prevent the continued use of their *Digital Identity* in accordance with IDP-03-04-02, prior to preventing the continued use of that *Digital Identity*.

TDIF Req: IDP-03-04-02b; **Updated**: Mar-20; **Applicability**: I
The *Applicant* ***MUST*** notify the *User* that a *Digital Identity* can no longer be used in accordance with IDP-03-04-02 and the reason why it can no longer be used (e.g. deactivated, suspended, etc).

[11] reusable digital identities

TDIF Req: IDP-03-04-02c; **Updated**: Mar-22; **Applicability**: I

If a *Digital Identity* is suspended in accordance with IDP-03-04-02, the *Applicant* *MUST* provide a process for a *User* to recover that *Digital Identity* which *MUST* include a requirement for the user to be reproofed to the highest *Identity Proofing Level* as applied to the *Digital Identity* before the suspension.

3.4.1 Expiry of a Digital Identity

TDIF Req: IDP-03-04-03; **Updated**: Mar-22; **Applicability**: I

If the Applicant has implemented *Identity Proofing* Lifecycle Management and subject to IDP-03-04-03a, the *Applicant* *MUST:*

- require that the maximum time elapsed between verifications of the link between the *User* and their *Digital Identity* is 5 years; and
- suspend a digital identity where the period between verifications of the link between the *User* and the *User's Digital identity* is longer than 5 years

TDIF Req: IDP-03-04-03a; **Updated**: Mar-22; **Applicability**: I

To verify the link between the *User* and their *Digital Identity*, the *Applicant* *MUST* either:

- Require the *User* to complete the *Identity Proofing* process for the *Identity Proofing level* of the *Digital Identity* and ensure that the *Attributes* presented can be linked to the *Attributes* which comprise the *Digital Identity*.
- Require the *User* to complete *Biometric Verification* in accordance with the requirements in section 3.8 of the *TDIF 05 Role Requirements* using a document whose *Attributes* can be linked to the *Attributes* which comprise the *Digital Identity*.

TDIF Req: IDP-03-04-03b; **Updated**: Mar-22; **Applicability**: I

If a *Digital Identity* is suspended in accordance with IDP-03-04-03, the *Applicant* *MUST* provide a process for a *User* to recover that *Digital Identity* by completing one of the two processes outlined in IDP-03-04-03a for an appropriate period of time after the *Digital Identity* has been suspended.

3.5 Identity proofing Step-Up

TDIF Req: IDP-03-05-01; **Updated**: Mar-22; **Applicability**: I
If the *Applicant* supports *Identity Proofing* Step-up for a *User* then the *Applicant* *MUST* implement the following requirements for the operation of *Identity Proofing* Step-up.

TDIF Req: IDP-03-05-01a; **Updated**: Mar-22; **Applicability**: I
The *Applicant* *MUST* ensure that the *User* achieves all the requirements of the higher *Identity Proofing Level*.

TDIF Req: IDP-03-05-01b; **Updated**: Mar-22; **Applicability**: I
The *Applicant* *MUST* be accredited to conduct an *Identity Proofing Process* at the higher *Identity Proofing Level.*

TDIF Req: IDP-03-05-02; **Updated**: Mar-22; **Applicability**: I
The *Applicant* *MUST* ensure that the *User* can prove ownership of their existing *Digital Identity* by authenticating with their *Credential* prior to commencing the *Identity Proofing Step-Up* process.

TDIF Req: IDP-03-05-02a; **Updated**: Mar-20; **Applicability**: I
When a *User* completes the *Identity Proofing Step-up* process, the *Applicant* *MAY* send a notification to the *User*.

3.6 Attribute collection, verification and validation

TDIF Req: IDP-03-06-01; **Updated**: Jun-21; **Applicability**: I
The *Applicant* *MUST NOT* collect, verify or validate *Attributes* beyond those listed in Table 2 and Table 3[12][13].

[12] An *Applicant* must demonstrate to *Finance* a need for its accredited *identity system* to collect, verify and validate *Attributes* beyond those listed in tables 2 and 3. An *Applicant's* accredited *identity system* must be separate from the Applicant's other business operations.

[13] Collection of Biometric attributes and verification are covered separately under section 3.8 of the *TDIF 04 Functional* Requirements.

Table 2: *Attribute* collection, *verification* and *validation*

Attribute collection, verification and validation
Identity Attributes (verified)
All verified names – family name(s), given name(s), surname(s), full name(s), previous name(s) as recorded on the *EoI document*
Verified date of birth as recorded on the *EoI document* [if collected]
Contact Attributes (validated)
Mobile phone number
Email address
EoI* document *Attributes (verified restricted Attributes)
EoI document type name
EoI document type code
EoI document issuer
EoI document identifier(s) (e.g. registration, document, licence, or card numbers)
EoI document issuer state
Other *EoI document Attributes* (i.e. other *Attributes* on the document verified by an *Authoritative Source*)
Verification method used for each *EoI document* (i.e. S, T, V)
Date and time the *EoI document* was verified
Identity System metadata
Date and time *Attributes* last updated (i.e. verified names and date of birth)
Date and time email address was last validated (if collected)
Date and time mobile phone number was last validated (if collected)
Date and time the *User* authenticated at the *Identity Service Provider*
Identity Proofing Level achieved
Date and time the *Digital Identity* was created
Digital Identity (*User Identifier*)

Table 3: *Assumed Self-asserted Attributes*

***Attributes* that may be collected and recorded**[14]
Preferred name(s)
Residential address
Postal address
Other address (e.g. second residential address)
Other phone number (e.g. landline)
Place of Birth
Titles (e.g. Dr. Mr, Ms)

[14] Assumed Self-asserted attributes in this table are limited and are considered separate from Assumed Self-asserted attributes that an Attribute Service Provider (ASP) may offer. See Section 5 of this document for a list of ASP requirements.

3.7 Attribute disclosure

These requirements do not overwrite the privacy obligations defined in section 3.6 of the *TDIF: 04 Functional Requirements* that an *Applicant* must meet regarding disclosure of *Attributes*.

TDIF Req: IDP-03-07-01; **Updated**: Mar-22; **Applicability**: I
The *Applicant* ***MUST*** limit disclosure of *Attributes* to an *Authoritative Source* to *Attributes* listed in Table 2.

TDIF Req: IDP-03-07-02; **Updated**: Mar-22; **Applicability**: I
Unless permission has been obtained under IDP-03-07-03, or *Attributes* are being disclosed to an *Authoritative Source* in accordance with IDP-03-07-01*,* the *Applicant* ***MUST*** limit disclosure of *Attributes* to the following *Attributes*:

- Identity *Attribute*s (verified) listed in Table 2.
- Contact *Attribute*s (validated) listed in Table 2.
- *Identity System* metadata listed in Table 2.
- *Assumed Self-asserted Attributes* listed in Table 3.

TDIF Req: IDP-03-07-03; **Updated**: Jun-21; **Applicability**: I
The *Applicant* ***MUST*** seek permission from *Finance* to disclose *Attributes* beyond those listed in IDP-03-07-02.

3.8 Biometric Binding requirements

This section sets out requirements to confirm the link between the *Individual* and the *Identity* being claimed using *Biometric verification*. To satisfy the requirements in this section, the *Applicant* will need to be familiar with the following ISO standards:

- ISO 17025
- ISO 30107-1
- ISO/IEC 30107-3
- ISO/IEC 19795-2ISO/IEC 19795-9
- ISO 29794-5

Finance will not be able to provide the *Applicant* with a copy of these standards.

NOTE: *TDIF 07 Maintain Accreditation* contains requirements and ongoing monitoring obligations for *Applicants* that meet the requirements in this section. They will be assessed at the *Applicant's Annual Assessments*.

3.8.1 General Biometric Binding Requirements.

The General Biometric Binding Requirements are applicable to ALL *IdP*s completing *Biometric Binding* as per Table 1 (required at IP2 Plus, IP3, IP4).

TDIF Req: IDP-03-08-01 **Updated**: Mar-22; **Applicability**: I
If *Biometric Binding* is supported, then the *Applicant* MUST implement the following requirements for the operation of *Biometric Binding*.

TDIF Req: IDP-03-08-02; **Updated**: Mar-22; **Applicability**: I
The *Applicant* MUST complete *Biometric Binding* by performing either:

- *Online Biometric Binding* as per Section 3.8.2, or
- *Local Biometric Binding* as per Section 3.8.3.

TDIF Req: IDP-03-08-03; **Updated**: Mar-22; **Applicability**: I
The *Applicant MUST* consider fraud and security risks, and the associated mitigation strategies and treatments, related to performing *Biometric Binding* when developing their *Fraud Control Plan* and *System Security Plan*, including the following risks (where applicable):

- Risks related to using *Biometric Matching* algorithms and *Presentation Attack Detection (PAD)* systems to complete Biometric Verification and *PAD*
- Risks related to using Assessing Officers to complete Local Biometric Binding.
- Risks related to the capture, temporary storage, and deletion of *Biometric Samples*.
- Risks related to the *Biometric Matching* process the *Applicant* implements (i.e. *Source*, *Technical,* or *Manual Face Comparison*).
- Risks related to potential and known threats and attacks to the *Biometric Capability.*

TDIF Req: IDP-03-08-03a; **Updated**: Mar-22; **Applicability**: I
Evidence of the *Applicant's* consideration of applicable risks outlined in IDP-03-08-03, associated mitigation strategies and treatments, the *Applicant's* risk framework, and any supporting evidence *MUST* be provided to *Finance*.

TDIF Req: IDP-03-08-04; **Updated**: Mar-22; **Applicability**: I
The *Photo ID* used in the *Biometric Matching Process* *MUST* undergo *Source Verification.*

TDIF Req: IDP-03-08-05; **Updated**: Mar-22; **Applicability**: I
Where the *Photo ID* is a foreign passport, the *Applicant* *MUST* perform a *DVS* check to ensure that the document and identity *Attributes* of the foreign passport correspond to the document and identity attributes of a current Australian visa.

TDIF Req: IDP-03-08-06; **Updated**: Mar-22; **Applicability**: I
The *Applicant* *MUST* log information associated with each *Biometric Binding* transaction, as per PROT-04-02-22a, including the specific *Biometric Matching* method utilised.

TDIF Req: IDP-03-08-07; **Updated**: Mar-22; **Applicability**: I
If the Applicant is required to have a *Biometric Testing Entity* test their *Biometric Capability* by either IDP-03-08-12 or IDP-03-08-18, then the Applicant *MUST* provide evidence that:

a) it has engaged a *Biometric Testing Entity* to conduct the biometric testing
b) the *Biometric Testing Entity* has employed appropriately experienced personnel with a background in biometric testing to conduct the biometric testing
c) the *Biometric Testing Entity* is a certified ISO 17025 laboratory
d) the *Biometric Testing Entity* has a policy for working with human test subjects approved by a relevant national body
e) The *Biometric Testing Entity* has established test methods for:
    i. PAD testing informed by ISO/IEC 30107-3, if performing testing relating to IDP-03-08-12 and all its parts, and
    ii. (if applicable) Biometric matching algorithm accuracy testing informed by ISO/IEC 19795-2, if performing testing relating to IDP-03-08-18 and all its parts.
f) The *Biometric Testing Entity* is an independent entity with no conflict of interest, perceived or otherwise.

NOTE: an entity accredited to perform PAD testing according to ISO/IEC 30107-3 and/or biometric performance testing according to ISO/IEC 19795-2 under the National Voluntary Laboratory Accreditation Program (NVLAP) coordinated by National Institute of Standards and Technology (NIST)

would meet the above requirements for each kind of testing respectively. Further information about Biometric Testing Entities is also available in TDIF 05A Role Guidance.

3.8.2 Online Biometric Binding

The *Online Biometric Binding* requirements are applicable for *IdPs* that support *Online Biometric Binding* via *Technical Biometric Matching* and/or *Source Biometric Matching*.

TDIF Req: IDP-03-08-08; **Updated**: Mar-22; **Applicability**: I
If *Online Biometric Binding* is supported, then the *Applicant* ***MUST*** implement the following requirements for the operation of *Online Biometric Binding.*

TDIF Req: IDP-03-08-09; **Updated**: Mar-22; **Applicability**: I
To complete *Online Biometric Binding* the *Applicant* ***MUST*** capture an *Acquired Image* and perform at least one of the following:

- *Technical Biometric Matching* as per Section 3.8.4
- *Source Biometric Matching* as per Section 3.8.5

TDIF Req: IDP-03-08-10; **Updated**: Mar-22; **Applicability**: I
The *Applicant* ***MUST*** create an *Image Quality Profile* of the *Acquired Image* and apply a quality threshold that this image ***MUST*** pass prior to being used for *Biometric Matching*.

TDIF Req: IDP-03-08-10a; **Updated**: Mar-22; **Applicability**: I
The method for generating the *Acquired Image's Image Quality Profile* ***MUST*** be informed by characteristics of biometric image quality described by ISO 29794-5.

TDIF Req: IDP-03-08-10b; **Updated**: Mar-22; **Applicability**: I
The *Applicant* ***MUST*** provide to *Finance* the characteristics used in generating the *Image Quality Profile* as a part of the initial accreditation.

TDIF Req: IDP-03-08-10c; **Updated**: Mar-22; **Applicability**: I
The *Applicant* ***MUST*** include automated quality controls and appropriate user-interface instructions that direct a *User* to provide an image that meets the *Acquired Image's Image Quality Profile*.

TDIF Req: IDP-03-08-11; **Updated**: Mar-22; **Applicability**: I
When performing *Online Biometric Binding*, the *Applicant MUST* incorporate *PAD* technology at the point of capture of the *Acquired Image*.

TDIF Req: IDP-03-08-11a; **Updated**: Mar-22; **Applicability**: I
The *Applicant MUST* complete the capture of the *Acquired Image* and *PAD* processes as part of the same process before submission of the *Acquired Image* to *Biometric Matching*.

TDIF Req: IDP-03-08-11b; **Updated**: Mar-22; **Applicability**: I
The *Applicant MUST* employ *PAD* technology based on data captured by both the data capture subsystem and through system level monitoring, as described by ISO 30107-1.

TDIF Req: IDP-03-08-11c; **Updated**: Mar-22; **Applicability**: I
The *Applicant MUST* include *Liveness Detection* as part of *PAD*.

TDIF Req: IDP-03-08-12; **Updated**: Mar-22; **Applicability**: I
The *Applicant MUST* ensure their *PAD* technology is tested according to ISO 30107-3 by a *Biometric Testing Entity*[15].

TDIF Req: IDP-03-08-12a; **Updated**: Mar-22; **Applicability**: I
The *Applicant MUST* provide the *Biometric Testing Entity's* report with the results of the testing conducted under IDP-03-08-12 to *Finance*.

TDIF Req: IDP-03-08-12b; **Updated**: Mar-22; **Applicability**: I
The *PAD* testing carried out by the *Biometrics Testing Entity MUST* include *Presentation Attack Instrument Species* to address potential *Presentation Attack* threats as informed by the risk assessment completed as part of IDP-03-08-03 and, if applicable, ANNUAL-02-10-03.

[15] NOTE: Applicants who must meet this requirement should be familiar with obligations for retesting PAD technology as described in TDIF 07 Maintain Accreditation.

TDIF Req: IDP-03-08-12c; **Updated**: Mar-22; **Applicability**: I
The *PAD* testing *MUST* be performed on a system that incorporates all hardware and software involved in the *Biometric Binding* process, including the *PAD* technology and *Biometric Matching* (where applicable).

TDIF Req: IDP-03-08-12d; **Updated**: Mar-22; **Applicability**: I
The PAD technology *MUST* be tested by a *Biometric Testing Entity* with configurations and settings that align to the *Applicant's* operational environment.

TDIF Req: IDP-03-08-12e; **Updated**: Mar-22; **Applicability**: I
The *PAD* testing *MUST* calculate and record the completed *PAD* evaluation and corresponding results for each *Presentation Attack Species* as described in ISO 30107-3.

TDIF Req: IDP-03-08-12f; **Updated**: Mar-22; **Applicability**: I
The *PAD* testing *MUST* include at least 6 *Level A Presentation Attack Instrument Species* and at least *6 Level B Presentation Attack Instrument Species*.

TDIF Req: IDP-03-08-12g; **Updated**: Mar-22; **Applicability**: I
The *PAD* testing *MUST* include a minimum of 10 *Individuals*.

TDIF Req: IDP-03-08-12h; **Updated**: Mar-22; **Applicability**: I
For each *Presentation Attack Instrument Species*, at least one *Presentation Attack Instrument MUST* be created for a minimum of 3 *Individuals*.

TDIF Req: IDP-03-08-12i; **Updated**: Mar-22; **Applicability**: I
All utilised *Presentation Attack Instrument Species (PAI Species) MUST* have an attack presentation classification error rate (APCER) of 0%. If the *Applicant's* reported APCER for any *PAI Species* does not meet these requirements, then a risk-based justification for failures *MUST* be provided to *Finance*, who will make a qualitative assessment of whether the *PAD* technology is fit for purpose.

3.8.3 Local Biometric Binding

Local Biometric Binding is performed when an *Individual* is in the physical presence of an *Assessing Officer.* The *Assessing Officer* can facilitate *Technical* or *Source Biometric Matching*, or complete *Manual Face Comparison*.

TDIF Req: IDP-03-08-13; **Updated**: Mar-22; **Applicability**: I
If *Local Biometric Binding* is supported, then the *Applicant MUST* implement the following requirements for the operation of *Local Biometric Binding.*

TDIF Req: IDP-03-08-14; **Updated**: Mar-22; **Applicability**: I
Local Biometric Binding is performed when an *Individual* is in the physical presence of an *Assessing Officer*, and *MUST* be achieved by the *Assessing Officer* performing one or more of the following *Biometric Matching* processes:

- Capturing an *Acquired Image* and performing either:
    - *Technical Biometric Matching* as per Section 3.8.4
    - *Source Biometric Matching* as per section 3.8.5
- A *Manual Face Comparison* as per section 3.8.6.

TDIF Req: IDP-03-08-14a; **Updated**: Mar-22; **Applicability**: I
While performing *Local Biometric Binding*, the *Applicant MUST* restrict access to *Biometric Information* and any aspects of the *Biometric Capability* to *Assessing Officers.*

TDIF Req: IDP-03-08-14b; **Updated**: Mar-22; **Applicability**: I
If an *Acquired Image* is being captured as part of *Local Biometric Binding*, then the *Applicant* MUST develop and apply an *Image Quality Profile* in accordance with IDP-03-08-10 to IDP-03-08-10c.

TDIF Req: IDP-03-08-14c; **Updated**: Mar-22; **Applicability**: I
The *Applicant MUST* only undertake *Local Biometric Binding* at a suitable locations identified in the *Applicant's Fraud Control Plan* and *System Security Plan.*

3.8.4 Technical Biometric Matching

Technical Biometric Matching occurs when a *Biometric Match* is made between an *Acquired Image* (i.e. an *individual's* captured photo) and the image securely extracted from a cryptographically verifiable *Photo ID* (e.g. an ePassport). This method of *Biometric Matching* can occur in the context of both *Online Biometric Binding* and *Local Biometric Binding.*

TDIF Req: IDP-03-08-15; **Updated**: Mar-22; **Applicability**: I
If *Technical Biometric Matching* is supported, then the *Applicant MUST* implement the following requirements for the operation of *Technical Biometric Matching.*

TDIF Req: IDP-03-08-16; **Updated**: Mar-22; **Applicability**: I
When performing *Technical Biometric Matching*, the *Applicant MUST* verify the authenticity of the image read from the *Photo ID* using *Technical Verification*.

TDIF Req: IDP-03-08-16a; **Updated**: Mar-22; **Applicability**: I
The *Applicant MUST* only process *Photo IDs* through *Technical Biometric Matching* that are government issued, and only if the digital signature for the image read from the *Photo ID* can be validated by *Technical Verification.*

TDIF Req: IDP-03-08-17; **Updated**: Mar-22; **Applicability**: I
The *Applicant MUST* use a *Biometric Matching* algorithm to perform one-to-one verification matching between the *Acquired Image* and the image read from the *Photo ID*.

TDIF Req: IDP-03-08-18; **Updated**: Mar-22; **Applicability**: I
The *Applicant MUST* ensure their *Biometric Matching* algorithm is tested by a *Biometric Testing Entity* to determine the *Failure to Enrol rate* (if applicable), *Failure to Acquire Rate, False Match Rate* and *False Non-match Rate* of the *Biometric Capability* as per the testing and reporting specifications described in ISO/IEC 19795-2.[16]

[16] NOTE: Applicants should be familiar with obligations for retesting the Biometric Matching algorithm as described in TDIF 07 Maintain Accreditation.

TDIF Req: IDP-03-08-18a; **Updated**: Mar-22; **Applicability**: I
The *Biometric Matching* algorithm *MUST* be tested by a *Biometric Testing Entity* with operational configurations and settings that align to the Applicant's operating environment.

TDIF Req: IDP-03-08-18b; **Updated**: Mar-22; **Applicability**: I
The *Biometric Matching* algorithm *MUST* be tested by a *Biometric Testing Entity* using representation from a diverse age, gender, and ethnicity demographics that considers possible *Users* of the *Applicant's* system.

TDIF Req: IDP-03-08-18c; **Updated**: Mar-22; **Applicability**: I
The *Biometric Matching* algorithm testing *MUST* establish, with a minimum 90% confidence interval, that the *Biometric Matching* algorithm achieves a false match rate (FMR) of not more than 0.01% and a false non-match rate (FNMR) of not more than 3%, as described in ISO/IEC 19795-9.

TDIF Req: IDP-03-08-18d; **Updated**: Mar-22; **Applicability**: I
As a part of the initial *TDIF Accreditation Process* the *Applicant MUST* provide the report to *Finance* from the *Biometric Testing Entity* outlining that the *Applicant's Biometric Matching* algorithm has been suitably tested as per the testing and reporting specifications described in ISO/IEC 19795-2.

3.8.5 Source Biometric Matching

Source Biometric Matching occurs when an *Acquired Image* is Biometrically Matched against a corresponding image stored in a *Photo ID Authoritative Source*.
NOTE: The list of *Photo ID Authoritative Sources* approved for *Source Biometric Matching* can be found in *TDIF 05A Role Guidance.*

TDIF Req: IDP-03-08-19; **Updated**: Mar-22; **Applicability**: I
If *Online Biometric Binding* with *Source Biometric Matching* is supported, then the *Applicant MUST* implement the following requirements for the operation of *Source Biometric Matching.*

TDIF Req: IDP-03-08-20; **Updated**: Mar-22; **Applicability**: I
To perform *Source Biometric Matching,* the *Applicant MUST* provide the *Acquired Image* and other information about the *Photo ID* in accordance with the instructions

specific to the *Photo ID Authoritative Source* capable of performing *Biometric Matching* to verify the *User's Acquired Image* biometrically matches the corresponding image stored in the *Photo ID Authoritative Source*[17].

TDIF Req: IDP-03-08-21; **Updated**: Mar-22; **Applicability**: I
The Applicant *MUST* provide evidence that end-to-end testing has taken place with the *Photo ID Authoritative Source* and that their *Biometric Capability* can meet any operating standards set by the *Photo ID Authoritative Source*.

3.8.6 Manual Face Comparison

TDIF Req: IDP-03-08-22; **Updated**: Mar-22; **Applicability**: I
If *Manual Face Comparison* is used for any *Biometric Binding* processes, then the *Applicant* MUST implement the following requirements for the operation of *Manual Face Comparison.*

TDIF Req: IDP-03-08-23; **Updated**: Mar-22; **Applicability**: I
If *Manual Face Comparison* is attempted using a *Photo ID* that can undergo *Technical Verification* for authenticity, then *Technical Verification MUST* be attempted.

TDIF Req: IDP-03-08-24; **Updated**: Mar-22; **Applicability**: I
The *Applicant MUST ensure that Assessing Officers* performing *Manual Face Comparison* receive awareness training, as part of Initial accreditation and annually thereafter, in accordance with the guidance provided by the latest version of the Facial Identification Scientific Working Group (FISWG), *Guide for Facial Comparison Awareness Training of Assessors.*

TDIF Req: IDP-03-08-24a; **Updated**: Mar-22; **Applicability**: I
The *Applicant MUST* provide *Assessing Officers* with an up-to-date reference card outlining practical steps and guidance when performing *Manual Face Comparison.*

TDIF Req: IDP-03-08-24b; **Updated**: Mar-22; **Applicability**: I
The *Applicant MUST* provide evidence of the *Manual Face Comparison* training materials and reference cards received by each *Assessing Officer*.[18]

[17] A list of Photo ID Authoritative Sources capable of performing Source Biometric Matching is available in TDIF 05A Role Guidance.

[18] A copy of the training materials will be requested by *Finance* as part of initial accreditation and annually thereafter as part of the *Annual Assessment* under *TDIF: 07-Annual Assessment*.

TDIF Req: IDP-03-08-25; **Updated**: Mar-22; **Applicability**: I
The *Applicant* *MUST* design and implement procedures to detect fraudulent activities by *Assessing Officers* performing *Manual Face Comparison.* These procedures *MUST* be included in the *Fraud Control Plan.*

TDIF Req: IDP-03-08-26; **Updated**: Mar-22; **Applicability**: I
The *Applicant* *MUST* design and implement quality control and quality assurance procedures for *Manual Face Comparison* decisions made by *Assessing Officers* as part of initial accreditation and annually thereafter. The *Applicant* *MUST* include these procedures in their risk assessment for *Biometric Binding* processes.

TDIF Req: IDP-03-08-27; **Updated**: Mar-22; **Applicability**: I
The *Assessing Officer* *MUST* only perform *Manual Face Comparison* using an original, physical *Photo ID* presented in-person by the *Individual.*

4 Credential Service Provider Requirements

These *Credential Service Provider* requirements:

- have been developed from the National Institute of Standards and Technology (NIST), Special Publication (SP) *800-63B, Digital Identity Guidelines – Authentication and Lifecycle Management* (NIST SP 800-63B).
  See: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
- refer to controls in the latest edition of the Information Security Manual (ISM).
  See: https://www.cyber.gov.au/acsc/view-all-content/ism
- assume a high-level of technical knowledge. Italicised words are defined in *TDIF 01 Glossary*.

All *Credential* lifecycle management operations must be informed by the *Applicant's Fraud Control Plan* (FRAUD-02-02-01), *Privacy Policy* (PRIV-03-02-03) and *System Security Plan* (PROT-04-01-11a). These requirements can be found in *TDIF 04 Functional Requirements*.

4.1 Credential Levels

TDIF Req: CSP-04-01-01; **Updated**: Jun-21; **Applicability**: C
The *Applicant* MUST support at least one of the *Credential Levels* described in Table 4.

TDIF Req: CSP-04-01-02; **Updated:** Mar-22; **Applicability:** C
For each supported *Credential Level*, the *Applicant* MUST ensure that when a *Credential Level* is asserted as a result of an *authentication event*, that the *authentication event* met all the requirements of that *Credential Level* as described in Table 4.

Table 4: *Credential* Levels

Requirement	CL1	CL2	CL3
Permitted *Credential* type combinations[19]	ONE OF: • *Memorised Secret* • *Look-up Secret* • *Out-of-Band Device* • *SF OTP Device* • *SF Crypto Software* • *SF Crypto Device* • *MF OTP Device* • *MF Crypto Software* • *MF Crypto Device*	ONE OF: • *MF OTP Device* • *MF Crypto Software* • *MF Crypto Device*; OR *Memorised Secret* AND ONE OF: • *Look-up Secret* • *Out-of-Band Device* • *SF OTP Device* • *SF Crypto Software* • *SF Crypto Device*	• *MF Crypto Device* **OR** • *SF Crypto Devices* **AND** *Memorised Secret* **OR** • *SF OTP Device* **AND** *MF Crypto Software* **OR** • *SF OTP Device* **AND** *MF Crypto Device* **OR** a) *SF OTP Device* **AND** *SF Crypto Software* **AND** *Memorised Secret*
Re-authentication requirements	30 days	12 hours or 30 minutes of inactivity. *MAY* use one *Authentication factor*	12 hours or 15 minutes of inactivity. *MUST* use both *Authentication factors*
Security requirements			
Man-in-the-Middle resistance	*MUST*	*MUST*	*MUST*
CSP-impersonation Resistance	-	-	*MUST*
CSP-compromise Resistance	-	-	*MUST*
Replay Resistance	-	*MUST*	*MUST*
Authentication Intent	-	*MAY*	*MUST*
Approved *Identity Proofing* combinations	IP1 and IP1 PLUS	IP1 through IP3 (inclusive)	All *Identity Proofing Levels*

[19] Expanded terms include: Single-Factor One Time Password (SF OTP), Single-Factor Cryptographic (SF Crypto), Multi-Factor One Time Password (MF OTP), Multi-Factor Cryptographic (MF Crypto)

TDIF Req: CSP-04-01-03; **Updated:** Mar-20; **Applicability:** C
The *Applicant MUST* ensure that *Credentials* presented are valid or active and that they are not expired or revoked prior to authenticating the *Individual*.

TDIF Req: CSP-04-01-04; **Updated**: Mar-20; **Applicability**: C
Where unusual transactions are detected the *Applicant MUST* verify the *Credential* is still under the control of its legitimate owner.

TDIF Req: CSP-04-01-05; **Updated**: Jun-21; **Applicability**: C
When requested by the *Individual,* the *Applicant MUST* prevent the continued use of a *Credential* (e.g. temporary suspension while traveling abroad).

TDIF Req: CSP-04-01-05a; **Updated**: Mar-20; **Applicability**: C
The *Applicant MUST* confirm the legitimacy of the request in accordance with CSP-04-01-05, prior to preventing the continued use of a *Credential*.

TDIF Req: CSP-04-01-05b; **Updated**: Mar-20; **Applicability**: C
The *Applicant MUST* notify the *Individual* that a *Credential* can no longer be used in accordance with CSP-04-01-05 and the reason why it can no longer be used (e.g. deactivated, expired, revoked, etc).

4.2 Credential types and requirements

4.2.1 Memorised Secrets

TDIF Req: CSP-04-02-01; **Updated**: Jun-21; **Applicability**: C
If *Memorised Secrets* are supported, then the *Applicant MUST* implement the following requirements for the operation of *Memorised Secrets*.

TDIF Req: CSP-04-02-01a; **Updated**: Jun-21; **Applicability**: C
Memorised Secrets MUST be at least 8 characters in length if chosen by the *Individual*.

TDIF Req: CSP-04-02-01b; **Updated**: Jun-21; **Applicability**: C
Memorised Secrets chosen randomly by the *Applicant MUST* be at least 6 characters in length and *MAY* be entirely numeric.

TDIF Req: CSP-04-02-01c; **Updated**: Mar-22; **Applicability**: C
When processing requests from an *Individual* to establish or change a *Memorised Secret*, the *Applicant* *MUST* compare the prospective secret against a list that contains secrets known to be commonly used, expected or compromised.

TDIF Req: CSP-04-02-01d; **Updated**: Jun-21; **Applicability**: C
If the *Applicant* disallows a chosen *Memorised Secret* based on its appearance on the list described in CSP-04-02-01c the *Applicant* *MUST*:

a) advise the *Individual* that they need to select a different secret
b) Provide the reason for rejection; and
c) Require the *Individual* choose a different *Memorised Secret*.

TDIF Req: CSP-04-02-01e; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MAY* offer guidance to the *Individual*, such as a password-strength meter, to assist the *Individual* in choosing a strong *Memorised Secret*. This is particularly important following the rejection of a *Memorised Secret* on the above list as it discourages trivial modification of listed (and likely very weak) *Memorised Secrets*.

TDIF Req: CSP-04-02-01f; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MAY* permit *Individuals* to use the “paste” functionality when entering a *Memorised Secret*. This facilitates the use of password managers, which are widely used and, in many cases, increase the likelihood that *Individuals* will choose stronger *Memorised Secrets*.

TDIF Req: CSP-04-02-01g; **Updated**: Jun-21; **Applicability**: C
To assist the *Individual* in successfully entering a *Memorised Secret*, the *Applicant* *MAY* offer an option to display the secret—rather than a series of dots or asterisks—until it is entered. This allows the *Individual* to verify their entry if they are in a location where their screen is unlikely to be observed.

TDIF Req: CSP-04-02-01h; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MAY* permit the *Individual’s* device to display individual entered characters for a short time after each character is typed to verify correct entry. This is particularly applicable on mobile devices.

TDIF Req: CSP-04-02-01i; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* use *Australian Signals Approved Cryptographic Algorithms* (*AACAs*) and an *Authenticated Protected Channel* when requesting *Memorised Secrets* to provide resistance to eavesdropping and *Man-in-the-Middle (MitM)* attacks.

TDIF Req: CSP-04-02-01j; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* store *Memorised Secrets* in a form that is resistant to offline attacks.

TDIF Req: CSP-04-02-01k; **Updated**: Jun-21; **Applicability**: C
Memorised Secrets *MUST* be salted and hashed using a suitable one-way *Key* derivation function.

TDIF Req: CSP-04-02-01l; **Updated**: Jun-21; **Applicability**: C
The salt *MUST* be at least 32 bits in length and be chosen arbitrarily so as to minimise salt value collisions among stored hashes.

TDIF Req: CSP-04-02-01m; **Updated**: Jun-21; **Applicability**: C
Both the salt value and the resulting hash *MUST* be stored for each *Individual* who uses *Memorised Secrets.*

4.2.2 *Look-up Secrets*

TDIF Req: CSP-04-02-02; **Updated**: Jun-21; **Applicability**: C
If *Look-up Secrets* are supported, then the *Applicant* *MUST* implement the following requirements for the operation of *Look-up Secrets*.

TDIF Req: CSP-04-02-02a; **Updated**: Jun-21; **Applicability**: C
An *Applicant* creating *Look-up Secrets* *MUST* deliver them securely to the *Individual*.

TDIF Req: CSP-04-02-02b; **Updated**: Jun-21; **Applicability**: C
When an *Individual* is authenticating, the *Applicant* *MUST* prompt the *Individual* for the next secret from their *Credential* (e.g. the next numbered secret) or a specific secret.

TDIF Req: CSP-04-02-02c; **Updated**: Jun-21; **Applicability**: C

A given *look-up secret* *MUST* be used successfully only once. If the *look-up secret* is derived from a grid card, each cell of the grid *MUST* be used only once.

TDIF Req: CSP-04-02-02d; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* store *Look-up Secrets* in a form that is resistant to offline attacks by ensuring that:

a) *Look-Up Secrets* are hashed using an AACA; and
b) *Look-Up Secrets* that have less than 112 bits of entropy are salted and hashed using an AACA with a salt value of at least 32 bits in length which is arbitrarily chosen.

TDIF Req: CSP-04-02-02e; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* store both the salt value and the resulting hash for each *look-up secret*.

TDIF Req: CSP-04-02-02f; **Updated**: Jun-21; **Applicability**: C
For *Look-up Secrets* that have less than 64 bits of entropy, the *Applicant* *MUST* implement a *Rate-limiting* mechanism that effectively limits the number of failed *Authentication* attempts that can be made on the *Individual's Digital Identity* account.

TDIF Req: CSP-04-02-02g; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* use *AACAs* and an *Authenticated Protected Channel* when requesting *Look-up Secrets* in order to provide resistance to eavesdropping and *MitM* attacks.

4.2.3 Out-of-band devices

TDIF Req: CSP-04-02-03; **Updated**: Jun-21; **Applicability**: C
If *Out-of-band Devices* are supported, then the *Applicant* *MUST* implement the following requirements for the operation of *out-of-band devices*.

TDIF Req: CSP-04-02-03a; **Updated**: Jun-21; **Applicability**: C
The *out-of-band device* *MUST* establish a separate channel with the *Applicant* to retrieve the *out-of-band secre*t or *Authentication Request*.

TDIF Req: CSP-04-02-03b; **Updated**: Jun-21; **Applicability**: C

The *out-of-band device* *MUST* uniquely authenticate itself in one of the following ways when communicating with the *Applicant*:

- Establish an *Authenticated Protected Channel* to the *Applicant* that:
  a) Uses an *AACA*;[20]
  b) stores the cryptographic key in suitably secure storage available to the *Credential* application (e.g. Keychain storage, secure element etc.).
- Only where a secret is being sent from the *Applicant* to the *out-of-band device* via the public switched telephone network, authenticate to a public mobile telephone network using a SIM card or equivalent that uniquely identifies the device.

TDIF Req: CSP-04-02-03c; **Updated**: Jun-21; **Applicability**: C
If the *out-of-band device* sends an approval message over the secondary communication channel — rather than by the *Individual* transferring a received secret to the primary communication channel — it *MUST* do one of the following:

- The device *MUST* accept transfer of the secret from the primary channel, which it *MUST* send to the *Applicant* over the secondary channel to associate the approval with the *Authentication* transaction. The *Individual* *MAY* perform the transfer manually or use a technology such as a barcode or QR code to effect the transfer.
- The device *MUST* present a secret received via the secondary channel from the *Applicant* and prompt the *Individual* to verify the consistency of that secret with the primary channel, prior to accepting a yes/no response from the *Individual*. It *MUST* then send that response to the *Applicant*.

TDIF Req: CSP-04-02-03d; **Updated**: Jun-21; **Applicability**: C
If out-of-band *verification* is to be made using a secure application, such as on a smart phone, the *Applicant* *MAY* send a push notification to that device. The *Applicant* will then wait for the establishment of an *Authenticated Protected Channel* and verify the device's identifying *Key*.

TDIF Req: CSP-04-02-03e; **Updated**: Jun-21; **Applicability**: C

The *Applicant* *MUST NOT* store the identifying *Key* itself.

TDIF Req: CSP-04-02-03f; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* use a *verification* method (e.g. an approved hash function using an *AACA*) to uniquely identify the device. Once authenticated, the *Applicant* will transmit the *Authentication* secret to the device.

TDIF Req: CSP-04-02-03g; **Updated**: Jun-21; **Applicability**: C
Depending on the type of *out-of-band device*, one of the following options (1, 2, OR 3) *MUST* take place:

1. Transfer of secret to primary channel:
    - The *Applicant* *MUST* signal the device containing the *Individual's Credential* to indicate readiness to authenticate
    - It *MUST* then transmit a random secret to the *out-of-band device*
    - The *Applicant* *MUST* then wait for the secret to be returned on the primary communication channel.
2. Transfer of secret to secondary channel:
    - The *Applicant* *MUST* display a random *Authentication* secret to the *Individual* via the primary channel
    - It *MUST* then wait for the secret to be returned on the secondary channel from the *Individual's out-of-band device*.
3. *Verification* of secrets by the *Individual*:
    - The *Applicant* *MUST* display a random *Authentication* secret to the *Individual* via the primary channel and *MUST* send the same secret to the *out-of-band device* via the secondary channel for presentation to the *Individual*.
    - It *MUST* then wait for an approval (or disapproval) message via the secondary channel.

TDIF Req: CSP-04-02-03h; **Updated**: Jun-21; **Applicability**: C
In all cases, the *Authentication* *MUST* be considered invalid if not completed within 10 minutes.

TDIF Req: CSP-04-02-03i; **Updated**: Jun-21; **Applicability**: C

To provide *replay resistance*, the *Applicant* *MUST* accept a given *Authentication* secret only once during the validity period.

TDIF Req: CSP-04-02-03j; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* generate random *Authentication* secrets with at least 20 bits of entropy.

TDIF Req: CSP-04-02-03k; **Updated**: Jun-21; **Applicability**: C
If the *Authentication* secret has less than 64 bits of entropy, the *Applicant* *MUST* implement a *Rate-limiting* mechanism that effectively limits the number of failed *Authentication* attempts that can be made on the *Individual's Digital Identity* account.

TDIF Req: CSP-04-02-03l; **Updated**: Jun-21; **Applicability**: C
If *out-of-band verification* is to be made using the *PSTN*, the *Applicant* *MUST* validate that the pre-registered telephone number being used is associated with a specific physical device.

TDIF Req: CSP-04-02-03m; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* consider risks when developing their *Fraud Control Plan* and *System Security Plan,* associated with device swap, SIM change, number porting or other abnormal behaviour before using the *PSTN* to deliver an out-of-band *Authentication* secret.

4.2.4 Single-factor one-time password (SF OTP) devices

TDIF Req: CSP-04-02-04; **Updated**: Jun-21; **Applicability**: C
If *single-factor OTP devices* are supported, the *Applicant* *MUST* implement the following requirements to operate *single-factor OTP devices*.

TDIF Req: CSP-04-02-04a; **Updated**: Jun-21; **Applicability**: C
The secret *Key* and its algorithm *MUST* provide at least the minimum-security strength specified in the latest edition of the *ISM*.

TDIF Req: CSP-04-02-04b; **Updated**: Jun-21; **Applicability**: C

The nonce *MUST* be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.

TDIF Req: CSP-04-02-04c; **Updated**: Jun-21; **Applicability**: C
OTP Credentials MUST NOT facilitate the cloning of the secret *Key* onto multiple devices.

TDIF Req: CSP-04-02-04d; **Updated**: Jun-21; **Applicability**: C
If the nonce used to generate the *Authentication* output is based on a real-time clock, the nonce *MUST* be changed at least once every 2 minutes.

TDIF Req: CSP-04-02-04e; **Updated**: Jun-21; **Applicability**: C
The *OTP* value associated with a given nonce *MUST* be accepted only once.

TDIF Req: CSP-04-02-04f; **Updated**: Jun-21; **Applicability**: C
When a *single-factor OTP Credential* is being associated with an *Individual's Digital Identity* account, the *Applicant MUST* use *AACAs* to either generate and exchange or to obtain the secrets required to duplicate the *Authentication* output.

TDIF Req: CSP-04-02-04g; **Updated**: Jun-21; **Applicability**: C
The *Applicant MUST* use *AACAs* and an *Authenticated Protected Channel* when collecting the *OTP* to provide resistance to eavesdropping and *MitM* attacks.

TDIF Req: CSP-04-02-04h; **Updated**: Jun-21; **Applicability**: C
To provide *replay resistance,* the *Applicant MUST* accept a given time-based *OTP* only once during the validity period.

TDIF Req: CSP-04-02-04i; **Updated**: Jun-21; **Applicability**: C
Time-based *OTPs MUST* have a defined lifetime that is determined by the expected clock drift — in either direction — of the *Credential* over its lifetime, plus allowance for network delay and *User* entry of the *OTP*.

TDIF Req: CSP-04-02-04j; **Updated**: Jun-21; **Applicability**: C

If the *Authentication* output has less than 64 bits of entropy, the *Applicant* *MUST* implement a *Rate-limiting* mechanism that effectively limits the number of failed *Authentication* attempts that can be made on the *Individual's Digital Identity* account.

4.2.5 Multi-factor one-time password (MF OTP) devices

TDIF Req: CSP-04-02-05; **Updated**: Jun-21; **Applicability**: C
If *multi-factor one-time password (MF OTP)* devices are supported, then the *Applicant* *MUST* implement the following requirements for the operation of *MF OTP* devices.

TDIF Req: CSP-04-02-05a; **Updated**: Jun-21; **Applicability**: C
The secret *Key* and its algorithm *MUST* provide at least the minimum-security strength specified in the latest edition of the *ISM*.

TDIF Req: CSP-04-02-05b; **Updated**: Jun-21; **Applicability**: C
The nonce *MUST* be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.

TDIF Req: CSP-04-02-05c; **Updated**: Jun-21; **Applicability**: C
OTP Authentication *MUST NOT* facilitate the cloning of the secret *Key* onto multiple devices.

TDIF Req: CSP-04-02-05d; **Updated**: Jun-21; **Applicability**: C
If the nonce used to generate the *Authentication* output is based on a real-time clock, the nonce *MUST* be changed at least once every 2 minutes.

TDIF Req: CSP-04-02-05e; **Updated**: Jun-21; **Applicability**: C
Any *Memorised Secret* used for activation *MUST* be a randomly chosen numeric secret at least 6 decimal digits in length.

TDIF Req: CSP-04-02-05f; **Updated**: Jun-21; **Applicability**: C
The unencrypted *Key* and activation secret or *Biometric Sample* — and any biometric data derived from the *Biometric Sample*, such as a probe produced

through signal processing — *MUST* be zeroised immediately after an *OTP* has been generated.

TDIF Req: CSP-04-02-05g; **Updated**: Jun-21; **Applicability**: C
When a *MF OTP Credential* is being associated with an *Individual's Digital Identity* account, the *Applicant MUST* use *AACAs* to either generate and exchange, or to obtain the secrets required to duplicate the *Authentication* output.

TDIF Req: CSP-04-02-05h; **Updated**: Jun-21; **Applicability**: C
The *Applicant MUST* use *AACAs* and an *Authenticated Protected Channel* when collecting the *OTP* to provide resistance to eavesdropping and *MitM* attacks.

TDIF Req: CSP-04-02-05i; **Updated**: Jun-21; **Applicability**: C
The *Applicant MUST* also establish that the *Credential* is a *MF OTP* device.

TDIF Req: CSP-04-02-05j; **Updated**: Jun-21; **Applicability**: C
Time-based *OTPs MUST* have a defined lifetime that is determined by the expected clock drift — in either direction — of the *Credential* over its lifetime, plus allowance for network delay and *User* entry of the *OTP*.

TDIF Req: CSP-04-02-05k; **Updated**: Jun-21; **Applicability**: C
To provide *replay resistance,* the *Applicant MUST* accept a given time-based *OTP* only once during the validity period.

TDIF Req: CSP-04-02-05l; **Updated**: Jun-21; **Applicability**: C
In the event an *Individual's Authentication* is denied due to duplicate use of an *OTP*, the *Applicant MAY* warn the *Individual* in case an *Attacker* has been able to authenticate in advance.

TDIF Req: CSP-04-02-05m; **Updated**: Jun-21; **Applicability**: C
The *Applicant MAY* also warn the *Individual* in an existing *Session* of the attempted duplicate use of an *OTP*.

TDIF Req: CSP-04-02-05n; **Updated**: Jun-21; **Applicability**: C

If the *Authentication* output has less than 64 bits of entropy, the *Applicant* *MUST* implement a *Rate-limiting* mechanism that effectively limits the number of failed *Authentication* attempts that can be made on the *Individual's Digital Identity account.*

4.2.6 Single-factor Cryptographic (SF Crypto) Software

TDIF Req: CSP-04-02-06; **Updated**: Jun-21; **Applicability**: C
If *Single-factor Cryptographic Software* is supported, then the *Applicant* *MUST* implement the following requirements for the operation of *Single-factor Cryptographic Software*.

TDIF Req: CSP-04-02-06a; **Updated**: Jun-21; **Applicability**: C
The *Key* *MUST* be strongly protected against unauthorised disclosure by using access controls that limit access to the *Key* to only those software components on the device requiring access.

TDIF Req: CSP-04-02-06b; **Updated**: Jun-21; **Applicability**: C
Single-factor Cryptographic Software Credentials *MUST NOT* facilitate the cloning of the secret *Key* onto multiple devices.

TDIF Req: CSP-04-02-06c; **Updated**: Jun-21; **Applicability**: C
*Key*s *MUST* be protected against modification.

TDIF Req: CSP-04-02-06d; **Updated**: Jun-21; **Applicability**: C
*Key*s *MUST* be protected against unauthorised disclosure.

TDIF Req: CSP-04-02-06e; **Updated**: Jun-21; **Applicability**: C
The challenge nonce *MUST* be at least 64 bits in length.

TDIF Req: CSP-04-02-06f; **Updated**: Jun-21; **Applicability**: C
The challenge nonce *MUST* either be unique over the *Credential's* lifetime or be statistically unique.

TDIF Req: CSP-04-02-06g; **Updated**: Jun-21; **Applicability**: C

The *Authentication* event *MUST* use approved cryptography (i.e. *AACAs* and *AACPs*).

4.2.7 Single-factor cryptographic (SF Crypto) devices

TDIF Req: CSP-04-02-07; **Updated**: Jun-21; **Applicability**: C
If *Single-factor Cryptographic Devices* are supported, then the *Applicant MUST* implement the following requirements for the operation of *Single-factor Cryptographic Devices.*

TDIF Req: CSP-04-02-07a; **Updated**: Jun-21; **Applicability**: C
Single-factor Cryptographic Devices MUST encapsulate one or more secret *Key*s unique to the device that *MUST NOT* be exportable (i.e. cannot be removed from the device).

TDIF Req: CSP-04-02-07b; **Updated**: Jun-21; **Applicability**: C
The secret *Key* and its algorithm *MUST* provide at least the minimum-security length specified in the latest edition of the *ISM*.

TDIF Req: CSP-04-02-07c; **Updated**: Jun-21; **Applicability**: C
The challenge nonce *MUST* be at least 64 bits in length.

TDIF Req: CSP-04-02-07d; **Updated**: Jun-21; **Applicability**: C
The challenge nonce *MUST* either be unique over the *Credential's* lifetime or be statistically unique.

TDIF Req: CSP-04-02-07e; **Updated**: Jun-21; **Applicability**: C
Approved cryptography (i.e. *AACAs* and *AACPs*) *MUST* be used.

TDIF Req: CSP-04-02-07f; **Updated**: Jun-21; **Applicability**: C
*Key*s *MUST* be protected against modification.

TDIF Req: CSP-04-02-07g; **Updated**: Jun-21; **Applicability**: C
*Key*s *MUST* be protected against unauthorised disclosure.

4.2.8 Multi-factor cryptographic (MF Crypto) software

TDIF Req: CSP-04-02-08; **Updated**: Jun-21; **Applicability**: C
If *Multi-factor Cryptographic Software* is supported, then the *Applicant* *MUST* implement the following requirements for the operation of *Multi-factor Cryptographic Software*.

TDIF Req: CSP-04-02-08a; **Updated**: Jun-21; **Applicability**: C
The *Key* *MUST* be strongly protected against unauthorised disclosure by the use of access controls that limit access to the *Key* to only those software components on the device requiring access.

TDIF Req: CSP-04-02-08b; **Updated**: Jun-21; **Applicability**: C
Authentication events *MUST* require the input of both factors.

TDIF Req: CSP-04-02-08c; **Updated**: Jun-21; **Applicability**: C
Any *Memorised Secret* used for activation *MUST* be a randomly chosen numeric value at least 6 decimal digits in length.

TDIF Req: CSP-04-02-08d; **Updated**: Jun-21; **Applicability**: C
The unencrypted *Key*, and activation secret or *Biometric Sample* — and any biometric data derived from the *Biometric Sample* such as a probe produced through signal processing — *MUST* be zeroised immediately after an *Authentication* has taken place.

TDIF Req: CSP-04-02-08e; **Updated**: Jun-21; **Applicability**: C
*Key*s *MUST* be protected against modification.

TDIF Req: CSP-04-02-08f; **Updated**: Jun-21; **Applicability**: C
*Key*s *MUST* be protected against unauthorised disclosure.

TDIF Req: CSP-04-02-08g; **Updated**: Jun-21; **Applicability**: C
The challenge nonce *MUST* be at least 64 bits in length.

TDIF Req: CSP-04-02-08h; **Updated**: Jun-21; **Applicability**: C
The challenge nonce *MUST* either be unique over the *Credential's* lifetime or, be statistically unique.

TDIF Req: CSP-04-02-08i; **Updated**: Jun-21; **Applicability**: C
The *Authentication* event *MUST* use approved cryptography (i.e. *AACAs* and *AACPs*).

TDIF Req: CSP-04-02-08j; **Updated**: Jun-21; **Applicability**: C
Truncation *MUST NOT* be performed on the *Memorised Secret* used for activation.

4.2.9 Multi-factor Cryptographic (MF Crypto) Devices

TDIF Req: CSP-04-02-09; **Updated**: Jun-21; **Applicability**: C
If *Multi-factor Cryptographic Devices* are supported, the *Applicant MUST* implement the following requirements for the operation of *Multi-factor Cryptographic Devices.*

TDIF Req: CSP-04-02-09a; **Updated**: Jun-21; **Applicability**: C
The secret *Key* and its algorithm *MUST* provide at least the minimum-security length specified in the latest edition of the *ISM*.

TDIF Req: CSP-04-02-09b; **Updated**: Jun-21; **Applicability**: C
The challenge nonce *MUST* be at least 64 bits in length.

TDIF Req: CSP-04-02-09c; **Updated**: Jun-21; **Applicability**: C
The challenge nonce *MUST* either be unique over the *Credential's* lifetime or, be statistically unique.

TDIF Req: CSP-04-02-09d; **Updated**: Jun-21; **Applicability**: C
Approved cryptography (i.e., *AACAs* and *AACPs*) *MUST* be used.

TDIF Req: CSP-04-02-09e; **Updated**: Jun-21; **Applicability**: C
*Key*s *MUST* be protected against modification.

TDIF Req: CSP-04-02-09f; **Updated**: Jun-21; **Applicability**: C

*Key*s *MUST* be protected against unauthorised disclosure.

4.3 General *Credential* requirements

4.3.1 Physical *Credential*s

TDIF Req: CSP-04-03-01; **Updated**: Jun-21; **Applicability**: C
If physical *Credentials* are supported, then the *Applicant MUST* implement the following requirements to operate physical *Credentials*.

TDIF Req: CSP-04-03-01a; **Updated**: Jun-21; **Applicability**: C
The *Applicant MUST* provide the *Individual* with instructions on how to appropriately protect the *Credential* against theft or loss.

TDIF Req: CSP-04-03-01b; **Updated**: Jun-21; **Applicability**: C
The *Applicant MUST* provide a mechanism to revoke or suspend the *Credential* immediately upon notification from the *individual* that loss or theft of the *Credential* is suspected.

4.3.2 Rate limiting (*Throttling*)

TDIF Req: CSP-04-03-02; **Updated**: Jun-21; **Applicability**: C
The *Applicant MUST* implement *Rate Limiting* (or *Throttling*) for all *Credentials.*

TDIF Req: CSP-04-03-02a; **Updated**: Jun-21; **Applicability**: C
The *Applicant MUST* implement controls to protect against online guessing attacks.

TDIF Req: CSP-04-03-02b; **Updated**: Jun-21; **Applicability**: C
The *Applicant MUST* limit consecutive failed *Authentication* attempts on a single account to no more than 100.

TDIF Req: CSP-04-03-02c; **Updated**: Jun-21; **Applicability**: C
Additional techniques *MAY* be used to reduce the likelihood that an *Attacker* will lock the *Individual* out of their *Digital Identity* account as a result of *Rate Limiting*.
Following a failed *Authentication* event, the *Applicant MAY* require:

- The *individual* to complete a Completely Automated Public Turing test to tell Computers and Humans Apart (*CAPTCHA*) before attempting *Authentication*.
- The *Individual* to wait for a period of time that increases as the account approaches its maximum allowance for consecutive failed attempts (e.g. 30 seconds up to an hour).
- Accepting only *Authentication Request*s that come from a whitelist of IP addresses from which the *Individual* has been successfully authenticated before.
- Leveraging other risk-based or adaptive *Authentication* techniques to identify *User* behaviour that falls within or out of typical norms. Examples include: use of IP address, geolocation, timing of request patterns, or browser metadata.

TDIF Req: CSP-04-03-02d; **Updated**: Jun-21; **Applicability**: C
When the *Individual* successfully authenticates, the *Applicant* MAY disregard any previous failed attempts for that *User* from the same IP address.

4.3.3 Biometrics (for Authentication use)

TDIF Req: CSP-04-03-03; **Updated**: Jun-21; **Applicability**: C
If the use of biometrics for *Authentication* is supported, then the *Applicant* ***MUST*** implement the following requirements for the operation of biometrics for *Authentication*.

TDIF Req: CSP-04-03-03a; **Updated**: Jun-21; **Applicability**: C
Biometrics ***MUST*** be used only as part of *multi-factor Authentication* with a physical *Credential*.

TDIF Req: CSP-04-03-03b; **Updated**: Jun-21; **Applicability**: C
An *Authenticated Protected Channel* between sensor and *Applicant* ***MUST*** be authenticated prior to capturing the *Biometric Sample* from the *Individual*.

TDIF Req: CSP-04-03-03c; **Updated**: Jun-21; **Applicability**: C
The biometric system ***MUST*** operate with a *False-Match-Rate* (*FMR*) of 1 in 1000 or better.

TDIF Req: CSP-04-03-03d; **Updated**: Jun-21; **Applicability**: C
This *FMR* ***MUST*** be achieved under conditions of a conformant attack (i.e. zero-effort impostor attempt) as defined in *ISO/IEC 30107-1.*

TDIF Req: CSP-04-03-03e; **Updated**: Jun-21; **Applicability**: C
The biometric system ***MUST*** implement *Presentation Attack Detection* (*PAD*).

TDIF Req: CSP-04-03-03f; **Updated**: Jun-21; **Applicability**: C
Testing of the biometric system to be deployed ***MUST*** demonstrate at least 90% resistance to *Presentation Attacks* for each relevant attack type (i.e. species), where resistance is defined as the number of thwarted *Presentation Attacks* divided by the number of trial *Presentation Attacks*.

TDIF Req: CSP-04-03-03g; **Updated**: Jun-21; **Applicability**: C
Testing of *presentation attack* resistance ***MUST*** be in accordance with Clause 12 of *ISO/IEC 30107-3:2017*.

TDIF Req: CSP-04-03-03h; **Updated**: Jun-21; **Applicability**: C
The *PAD* decision *MAY* be made either locally on the *Individual's* device or by the *Applicant*.

TDIF Req: CSP-04-03-03i; **Updated**: Jun-21; **Applicability**: C
The biometric system *MUST* allow no more than 5 consecutive failed *Authentication* attempts or 10 consecutive failed attempts.

TDIF Req: CSP-04-03-03j; **Updated**: Jun-21; **Applicability**: C
Once the limit of consecutive failed attempts has been reached, the biometric system *MUST* either:

- Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt (e.g. 1 minute before the following failed attempt, 2 minutes before the second following attempt), or
- Disable the biometric *User Authentication* and offer another factor (e.g. a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available.

TDIF Req: CSP-04-03-03k; **Updated**: Jun-21; **Applicability**: C
The *Applicant MUST* make a determination of sensor and endpoint performance, integrity, and authenticity. Acceptable methods for making this determination include, but are not limited to:

- *Authentication* of the sensor or endpoint
- Certification by an approved accreditation authority
- Runtime interrogation of signed metadata (e.g. *Attestation*).

TDIF Req: CSP-04-03-03l; **Updated**: Mar-22; **Applicability**: C
If supported, biometric comparison that is performed centrally *MUST* implement the following requirements:

- Use of the biometric as an *Authentication factor MUST* be limited to one or more specific devices that are identified using *Approved Cryptography*
- a separate *Key MUST* be used for identifying the device
- Biometric revocation, referred to as 'biometric template protection' in *ISO/IEC 24745*, *MUST* be implemented
- All transmission of biometrics *MUST* be over the *Authenticated Protected Channel*.

4.3.4 *Credential Attestation*

TDIF Req: CSP-04-03-04; **Updated**: Jun-21; **Applicability**: C
If *Credential Attestation* is supported, the *Applicant* *MUST* implement the following requirements for the operation of *Credential Attestation*.

TDIF Req: CSP-04-03-04a; **Updated**: Jun-21; **Applicability**: C
Information conveyed by *Credential Attestation* *MAY* include, but is not limited to:

- The provenance (e.g. manufacturer or supplier certification), health, and integrity of the *Credential* and endpoint
- Security features of the *Credential*
- Security and performance characteristics of biometric sensor(s)
- Sensor modality.

TDIF Req: CSP-04-03-04b; **Updated**: Jun-21; **Applicability**: C
If this *Attestation* is signed, it *MUST* be signed using a digital signature that provides at least the minimum-security strength specified in the latest version of the *ISM*.

4.3.5 *CSP-impersonation Resistance*

As per Table 4, *CSP-impersonation Resistance* is required at CL3.

TDIF Req: CSP-04-03-05; **Updated**: Jun-21; **Applicability**: C
Where the *Applicant* supports *CL3,* it *MUST* implement the following *CSP-impersonation Resistance* requirements. These requirements do not need to be implemented for *CL1* or *CL2*.

TDIF Req: CSP-04-03-05a; **Updated**: Jun-21; **Applicability**: C
A *CSP-impersonation* resistant *Authentication Protocol* *MUST* establish an *Authenticated Protected Channel* with the *Applicant*.

TDIF Req: CSP-04-03-05b; **Updated**: Jun-21; **Applicability**: C
A *CSP-impersonation resistant Authentication Protocol* *MUST* strongly and irreversibly bind a channel identifier that was negotiated in establishing the

Authenticated Protected Channel to the *Authentication* output (e.g. by signing the two values together using a *Private Key* controlled by the claimant for which the *Public Key* is known to the *Applicant)*.

TDIF Req: CSP-04-03-05c; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* validate the signature or other information used to prove *CSP-impersonation Resistance*.

TDIF Req: CSP-04-03-05d; **Updated**: Jun-21; **Applicability**: C
AACAs *MUST* be used to establish *CSP-impersonation Resistance*.

TDIF Req: CSP-04-03-05e; **Updated**: Jun-21; **Applicability**: C
*Key*s used for this purpose *MUST* provide at least the minimum-security strength specified in the latest edition of the *ISM*.

TDIF Req: CSP-04-03-05f; **Updated**: Jun-21; **Applicability**: C
Credentials that involve the manual entry of an *Authentication* output, such as *out-of-band* and *OTP Credentials*, *MUST NOT* be considered *CSP-impersonation resistant* because the manual entry does not bind the *Authentication* output to the specific *Session* being authenticated.

4.3.6 IdP-CSP communications

TDIF Req: CSP-04-03-06; **Updated**: Jun-21; **Applicability**: C, I
In situations where the *IdP* and *CSP* are separate entities, communication *MUST* occur through a mutually authenticated secure channel (such as a client-authenticated *TLS* connection) using *Approved Cryptography*.

4.3.7 *CSP-compromise Resistance*

As per Table 4, *CSP-compromise Resistance* is required at *CL3*.

TDIF Req: CSP-04-03-07; **Updated**: Jun-21; **Applicability**: C
Where the *Applicant* supports *CL3,* it *MUST* implement the following *CSP-compromise Resistance* requirements. These requirements do not need to be implemented for *CL1* or *CL2.*

TDIF Req: CSP-04-03-07a; **Updated**: Jun-21; **Applicability**: C
To be considered *CSP-compromise* resistant, *Public Key*s stored by the *Applicant* *MUST* be associated with the use of *approved cryptographic algorithms* (i.e. *AACAs*).

TDIF Req: CSP-04-03-07b; **Updated**: Jun-21; **Applicability**: C
*Key*s *MUST* provide at least the minimum-security strength specified in the latest version of the *ISM*.

4.3.8 *Authentication* intent

As per Table 4, *Authentication* intent is required at *CL 3*.

TDIF Req: CSP-04-03-08; **Updated**: Mar-22; **Applicability**: C
Where the *Applicant* supports *CL 3* it *MUST* implement the following *Authentication* intent requirements. These requirements do not need to be implemented for *CL 1* or *CL 2.*

TDIF Req: CSP-04-03-08a; **Updated**: Mar-22; **Applicability**: C
Authentication intent *MUST* be established by the *Credential* itself.

TDIF Req: CSP-04-03-08b; **Updated**: Mar-22; **Applicability**: C
Authentication intent *MAY* be established in several ways, including:

- *Authentication* processes that require the *Individual's* intervention (e.g. an *Individual* entering an *Authentication* output from an *OTP* device).
- Cryptographic devices that require *User* action (e.g. pushing a button or reinsertion) for each *Authentication* or re-authentication operation.

4.3.9 Restricted *Credential*s

TDIF Req: CSP-04-03-09; **Updated**: Mar-22; **Applicability**: C
If, at any time, the *Applicant* determines that a *Credential* is resulting in an unacceptable risk to any party, then they *MUST*, as soon as practical after the determination has been made, prevent continued use of that *Credential*. Such *Credentials* are referred to as *Restricted Credentials*.

TDIF Req: CSP-04-03-10; **Updated**: Jun-21; **Applicability**: C

If the *Applicant* supports the use of a *Restricted Credential*, it *MUST*:

1. Offer *Individuals* 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 Credential* and availability of alternative(s) that are not restricted
3. Address any additional risk to *Individuals* in its *security Risk Assessment*
4. Develop a migration plan for the possibility that the *Restricted Credential* is no longer acceptable at some point in the future.

4.4 *Credential* lifecycle management

4.4.1 *Credential* binding

TDIF Req: CSP-04-04-01; **Updated**: Jun-21; **Applicability**: C

A *Credential* *MUST* be bound to an *Individual's* account by either:

- Issuance by the *Applicant* as part of enrolment; or
- Associating a *User*-provided *Credential* that is acceptable to the *Applicant*.

TDIF Req: CSP-04-04-01a; **Updated**: Jun-21; **Applicability**: C

Throughout the *Digital Identity* lifecycle, the *Applicant* *MUST* maintain a record of all *Credentials* that are or have been associated with each *Digital Identity* account.

TDIF Req: CSP-04-04-01b; **Updated**: Jun-21; **Applicability**: C

The *Applicant* *MUST* maintain the information required for *Throttling Authentication* attempts when required.

TDIF Req: CSP-04-04-01c; **Updated**: Jun-21; **Applicability**: C

The record created by the *Applicant* *MUST* contain the date and time the *Credential* was bound to the account.

TDIF Req: CSP-04-04-01e; **Updated**: Jun-21; **Applicability**: C

The record *MUST* include information about the source of the binding (e.g. IP address, device identifier) of any device associated with the enrolment.

TDIF Req: CSP-04-04-01f; **Updated**: Jun-21; **Applicability**: C
The record *MUST* also contain information about the source of unsuccessful *Authentications* attempted with the *Credential*.

TDIF Req: CSP-04-04-01g; **Updated**: Jun-21; **Applicability**: C
When any new *Credential* is bound to an *Individual's* account, the *Applicant 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.

4.4.2 Binding at enrolment

TDIF Req: CSP-04-04-02; **Updated**: Jun-21; **Applicability**: C
For remote transactions where enrolment and binding cannot be completed in a single electronic transaction (i.e. within a single protected *Session*), the following requirements *MUST* be met to ensure that the same party acts as the *Individual* throughout the process:

- The *Individual 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 *Individual's* mobile phone number or email address.
- Long-term *Authentication* secrets *MUST* only be issued to the *Individual* within a protected *Session*.

TDIF Req: CSP-04-04-02a; **Updated**: Jun-21; **Applicability**: C
For in-person transactions where enrolment and binding cannot be completed in a single physical encounter (i.e. within a single protected *Session*), the following requirements *MUST* be met to ensure that the same party acts as the *Individual* throughout the process:

- The *Individual MUST* identify themselves in-person by either using a secret as described in CSP-04-04-02, or through use of a biometric that was recorded during the *identity proofing* process.
- Temporary secrets *MUST NOT* be reused
- If the *Applicant* 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 *individual* or delivered in a manner that confirms the *individual's* email address or mobile phone number.

4.4.3 Binding additional *Credentials*

TDIF Req: CSP-04-04-03; **Updated**: Jun-21; **Applicability**: C
If the *Applicant* supports the *Binding* of additional *Credentials* to an *Individual's* account, then it *MUST* implement the following requirements when *Binding* additional *Credentials* to an *individual's* account.

TDIF Req: CSP-04-04-03a; **Updated**: Jun-21; **Applicability**: C
Before *Binding* an additional *Credential* to an *Individual's* account, the *Applicant* *MUST* first require the *Individual* to authenticate at the *CL* (or a higher *CL*) at which the new *Credential* will be used.

TDIF Req: CSP-04-04-03b; **Updated**: Jun-21; **Applicability**: C
When a *Credential* is added, the *Applicant* *MAY* send a notification to the *Individual* via a mechanism that is independent of the transaction *Binding* the new *Credential* (e.g. email to an address previously associated with the *Individual*).

TDIF Req: CSP-04-04-03c; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MAY* limit the number of *Credentials* that may be bound in this manner.

4.4.4 Binding to a User-provided Credential

TDIF Req: CSP-04-04-06; **Updated**: Mar-22; **Applicability**: C
Subject to the requirements in section 4.4.1, the *Applicant* *MAY*, where practical, accommodate the use of a *User*-provided *Credential* to relieve the burden to the *User* of managing a large number of *Credentials*.

TDIF Req: CSP-04-04-06a; **Updated**: Mar-22; **Applicability**: C
The *Applicant* *MUST* verify the *Credential* type of a *User*-provided *Credential* (e.g. *Single-factor Cryptographic Device* vs. *Multi-factor Cryptographic Device*) so the *Applicant* can determine compliance with requirements at each CL.

4.4.5 Renewal

TDIF Req: CSP-04-04-07; **Updated**: Mar-22; **Applicability**: C

If the *Applicant* issues *Credentials* which expire, the *Applicant* *MUST* bind an updated *Credential* a reasonable amount of time before an existing *Credential's* expiration.

TDIF Req: CSP-04-04-08; **Updated**: Jun-21; **Applicability**: C
Following successful use of the new *Credential*, the *Applicant* *MAY* revoke the *Credential* that it is replacing.

4.5 Loss, theft, damage and unauthorised duplication

TDIF Req: CSP-04-05-01; **Updated**: Jun-21; **Applicability**: C
The suspension, revocation or destruction of a compromised *Credential* *MUST* occur as promptly as practical following the detection or report of loss, theft, damage or unauthorised duplication of a *Credential*.

TDIF Req: CSP-04-05-02; **Updated**: Jun-21; **Applicability**: C
To facilitate secure reporting of the loss, theft or damage to a *Credential*, the *Applicant* *MAY* provide the *Individual* with a method of authenticating to the *Applicant* using a backup or alternate *Credential*.

TDIF Req: CSP-04-05-03; **Updated**: Jun-21; **Applicability**: C
If the *Applicant* implements CSP-04-05-02, then the backup *Credential* *MUST* be either a *Memorised Secret* or a physical *Credential*.

TDIF Req: CSP-04-05-04; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MAY* choose to *validate* a *User*'s contact details (i.e. email, mobile phone number) and *MUST* suspend a *Credential* reported to have been compromised.

TDIF Req: CSP-04-05-05; **Updated**: Mar-22; **Applicability**: C
The *Applicant* *MAY* set a time limit after which a suspended *Credential* can no longer be reactivated.

4.6 Credential expiration

TDIF Req: CSP-04-06-01; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MAY* issue *Credentials* that expire.

TDIF Req: CSP-04-06-01a; **Updated**: Jun-21; **Applicability**: C
When a *Credential* expires, it *MUST NOT* be usable for *Authentication*.

TDIF Req: CSP-04-06-01b; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* require an *Individual* to surrender or prove destruction of any physical *Credential* containing *Attribute* certificates signed by the *Applicant* as soon as practical after expiration or receipt of a renewed *Credential*.

4.7 Credential revocation and termination

TDIF Req: CSP-04-07-01; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* revoke the *Binding* of a *Credential* promptly when an account ceases to exist (e.g. an *Individual's* death, discovery of a fraudulent account), when requested by the *Individual*, or when the *Applicant* determines that the *Individual* no longer meets its eligibility requirements.

TDIF Req: CSP-04-07-02; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* require an *Individual* to surrender or certify destruction of any physical *Credential* containing certified *Attribute*s signed by the *Applicant* as soon as practical after revocation or termination takes place. This is necessary to block the use of the *Credential's* certified *Attributes* in offline situations between revocation or termination and expiration of the certification.

4.8 *Session* management

TDIF Req: CSP-04-08-01; **Updated**: Jun-21; **Applicability**: C
A *Session* *MAY* be started in response to an *Authentication Event* and continue until such time that it is terminated.

TDIF Req: CSP-04-08-01a; **Updated**: Jun-21; **Applicability**: C
A *Session* *MAY* be terminated for any number of reasons, including but not limited to an inactivity timeout, an explicit logout event or other means.

TDIF Req: CSP-04-08-01b; **Updated**: Jun-21; **Applicability**: C
The *Session* *MAY* be continued through a re-authentication in accordance with the requirements in section 4.9.

4.9 Re-authentication

TDIF Req: CSP-04-09-01; **Updated**: Jun-21; **Applicability**: C
Continuity of authenticated *Sessions* *MUST* be based upon the possession of a *Session* secret issued by the *Applicant* at the time of *Authentication* and optionally refreshed during the *Session*.

TDIF Req: CSP-04-09-01a; **Updated**: Jun-21; **Applicability**: C
Session secrets *MUST* be non-persistent.

TDIF Req: CSP-04-09-01b; **Updated**: Jun-21; **Applicability**: C
Session secrets *MUST NOT* be retained across a restart of the associated application or a reboot of the host device.

TDIF Req: CSP-04-09-01c; **Updated**: Jun-21; **Applicability**: C
Periodic re-authentication of *Sessions* *MUST* be performed to confirm the continued presence of the *Individual* at an authenticated *Session* (i.e. that the *Individual* has not walked away without logging out).

TDIF Req: CSP-04-09-01d; **Updated**: Jun-21; **Applicability**: C
When a *Session* has been terminated, due to a time-out or other action, the *Individual* *MUST* be required to establish a new *Session* by authenticating again.

4.10 *Credential* Step-Up

TDIF Req: CSP-04-10-01; **Updated**: Jun-21; **Applicability**: C
If the *Applicant* supports a *User* to *Step-Up* the *Credential Level* that can be asserted as a result of an authentication event to a higher *Credential Level* supported by the *Applicant*, then it *MUST* implement the following requirements for the operation of *Step-Up* for all *Credential Levels*.

TDIF Req: CSP-04-10-01a; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* be accredited to assert the higher *Credential Level.*

TDIF Req: CSP-04-10-01b; **Updated**: Jun-21; **Applicability**: C
If a *Credential* is added to the *User's Digital Identity* account as a result of *Step-up*, the *Applicant* *MUST* ensure that the new *Credential*:

a) is capable of meeting all the applicable requirements of the higher *Credential Level*;
b) is a type of *Credential* supported by the *Applicant's Identity System*; and
c) meets all the requirements for that *Credential* type.

TDIF Req: CSP-04-10-*02*; **Updated**: Mar-20; **Applicability**: C
The *Applicant* *MUST* ensure that an *Individual* can prove ownership of their existing *Digital Identity* by authenticating with their *Credential* to their account prior to commencing the *Credential Step-Up* process.

4.11 Certification Authorities

TDIF Req: CSP-04-11-01; **Updated**: Jun-21; **Applicability**: C
If *Certification Authorities* are supported, then the *Applicant* *MUST* implement all of the following requirements to operate as a *Certification Authority.*

TDIF Req: CSP-04-11-02; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* ensure all:

a. *Certification Practice Statements (CPS)* and *Certificate Policies (CP)* conform to Request for Comment (RFC) 3647
b. *Digital Certificates* conform to the (RFC) 5280 format
c. *Certificate Revocation Lists (CRLs*) conform to the X.509 version 2 profile as described in RFC 5280
d. Online Certificate Status Protocol (OCSP) responses conform to RFC 6960.

TDIF Req: CSP-04-11-03; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* ensure the *Root Certification Authority* (CA) *Private Key* is not used to digitally sign *Digital Certificates,* except in the following cases:

- Self-signed *Digital Certificates* to represent the *Root CA* itself.
- *Digital Certificates* for *Subordinate CAs* and *Cross Certificates*.

- *Digital Certificates* for infrastructure purposes (for example, administrative role certificates and *OCSP Digital Certificates*).
- *Digital Certificates* issued solely for the purpose of testing software with *Digital Certificates* issued by the *Root CA*.

TDIF Req: CSP-04-11-04; **Updated**: Jun-21; **Applicability**: C
The *Applicant* MUST implement a process to allow *Individuals* to request revocation of their *Digital Certificate.*

TDIF Req: CSP-04-11-04a; **Updated**: Jun-21; **Applicability**: C
The *Applicant* MUST implement revocation procedures for the following situations:

- The *Individual* notifies the *Applicant* that a *Digital Certificate* request was not authorised by them.
- The *Applicant* obtains evidence that a *Digital Certificate*'s *Private Key* suffered a *Key* compromise or no longer complies with the requirements outlined in the *Certificate Policy*.
- The *Applicant* obtains evidence that a *Digital Certificate* it has issued has been misused.
- The *Applicant* is made aware that an *Individual* has violated one or more of their usage terms (for example, those set out in ROLE-02-01-01).
- The *Applicant* is made aware that the *Certificate* was not issued in accordance with its *Certification Practice Statements* or *Certificate Policy*.
- The *Applicant* determines that any information set out in the *Digital Certificate* is inaccurate or misleading.
- The *Applicant* obtains evidence of a suspected or actual compromise of a subordinate *CA's Private Key*.

5 Attribute Service Provider Requirements

All *Attribute* lifecycle management operations must be informed by the *Applicant's Fraud Control Plan* (FRAUD-02-02-01), *Privacy Policy* (PRIV-03-02-03) and *System Security Plan* (PROT-04-01-11a). These requirements can be found in *TDIF 04 Functional Requirements*.

The TDIF supports a variety of configurations for how *Attribute Service Providers* can participate in *Identity Systems*, such as:

- An *Attribute Service Provider* directly connecting to an *Identity Service Provider*,
- An *Attribute Service Provider* connecting indirectly to a *Relying Party* via an *Identity Exchange*.

5.1 Attribute Classes

TDIF Req: ASP-05-01-01; **Updated**: Mar-20; **Applicability**: A

The *Applicant* MUST support at least one *Attribute Class* as described in Table 6.

Table 5: Attribute Classes

Attribute Class	Description
Authorisation	An *Individual* gives a permission, delegation or privilege for someone to act on their behalf. (e.g. an *Individual* authorised to act on behalf of their children when applying for a government service).
Qualification	A statement of attainment by an education or training organization consistent with the *AQF*[21] (e.g. a bachelor's degree from an Australian university).
Entitlement	Meeting a set of conditions which enables a *Individual* to have a right to something (e.g. an *Individual* is a resident of an Australian state or territory aged over 60 years and not working more than a set number of hours per week is entitled to a Seniors Card).
Assumed Self-asserted	Unverified *Attributes* provided by an *Individual* that can assist with service delivery, such as prefilling online forms. This *Attribute Class* can be used for 'Tell Us Once' services.

[21] Australian Qualifications Framework. Further information is available at https://www.aqf.edu.au/

Platform	*Attributes* which uniquely identify platforms and ICT systems that connect into the *Australian Government's Digital Identity System*. For example, MyGov.

TDIF Req: ASP-05-01-02; **Updated**: Mar-22; **Applicability**: A, I

Beyond the minimum dataset required to associate *Identity Attributes* with *Attributes* related to *Attribute Classes*, the *Applicant* *MUST NOT* store *Attributes* held by an *Identity Service Provider* and *Attribute Service Provider* together in the one repository.[22]

5.2 General requirements

TDIF Req: ASP-05-02-01; **Updated**: Mar-20; **Applicability**: A

The *Applicant* *MUST* either be an *Authoritative Source* for *Attributes* it issues or have approval from the *Authoritative Source* to manage *Attributes* on their behalf.

TDIF Req: ASP-05-02-01a; **Updated**: Mar-22; **Applicability**: A

Where the *Applicant* manages *Attributes* on behalf of an *Authoritative Source*, it *MUST* provide evidence of this arrangement to *Finance*.[23]

TDIF Req: ASP-05-02-02; **Updated**: Mar-20; **Applicability**: A

The *Applicant* *MUST* ensure every *Attribute* it issues or manages is uniquely identifiable.

TDIF Req: ASP-05-02-03; **Updated**: Mar-20; **Applicability**: A

The *Applicant* *MUST* manage and provide up-to-date, relevant and accurate *Attributes*.

TDIF Req: ASP-05-02-04; **Updated**: Mar-20; **Applicability**: A

If the *Applicant* is an *Authoritative Source* for an *Attribute*, the *Applicant* *MUST* verify all requests to update relevant *Attributes* prior to making changes.

TDIF Req: ASP-05-02-05; **Updated**: Mar-22; **Applicability**: A

The *Applicant* *MUST* take reasonable measures to prevent the continued use of an

[22] This includes circumstances where the entity is both an identity service provider and attribute service provider in an *Identity System*.

[23] Evidence of this arrangement will be requested by *Finance* as part of initial accreditation and annually thereafter as part of the *Annual Assessment*.

Attribute (e.g. suspension, deactivation) when requested to do so by a User, *Authorised Representative* or *Authoritative Source*.

TDIF Req: ASP-05-02-05a; **Updated**: Mar-22; **Applicability**: A
The *Applicant* *MUST* confirm the legitimacy of the request from an *Authorised Representative* or *Authoritative Source* in accordance with ASP-05-02-05, prior to actioning the request.

TDIF Req: ASP-05-02-06; **Updated**: Mar-22; **Applicability**: A
The *Applicant* *MAY* support issuing or linking multiple *Attributes* and *Attribute Classes* to an *Individual*.

TDIF Req: ASP-05-02-06a; **Updated**: Mar-22; **Applicability**: A
The *Applicant* *MAY* support issuing or linking multiple *Attributes* relating to the same entity to an *Individual*.

TDIF Req: ASP-05-02-06b; **Updated**: Mar-22; **Applicability**: A
The *Applicant* *MAY* support issuing or linking multiple *Individuals* to the same *Attribute*.

6 Identity Exchange Requirements

All *Identity Exchange* operations must be informed by the *Applicant's Fraud Control Plan* (FRAUD-02-02-01), *Privacy Policy* (PRIV-03-02-03) and *System Security Plan* (PROT-04-01-11a). These requirements can be found in *TDIF 04 Functional Requirements*.

6.1 *Audit Log*ging Requirements

TDIF Req: IDX-06-01-01**; Updated:** Jun-21**; Applicability:** X
The *Applicant* MUST generate a unique audit Id for an *Authentication Request* from a *Relying Party* to be used as the unique interaction identifier for the interaction.

TDIF Req: IDX-06-01-02**; Updated:** Jun-21**; Applicability:** X
The *Applicant* MUST log all related interactions between *Relying Parties* and *Identity Service Providers* using this unique audit id (this includes *Attribute Service Providers* acting as *Relying Parties*).

6.2 Consent Management

TDIF Req: IDX-06-02-01; **Updated:** Mar-22; **Applicability:** X
In accordance with PRIV-03-09-03, the *Applicant* MUST maintain the following information as part of its *Audit Logs*:

- Timestamp
- Where an *entity* records consent on behalf of an *IdP* or *ASP*, the duration of *Consent*. (including any time limit on the consent)
- The name of the *Relying Party* that requested the relevant *attributes*.
- The *Identifier* that identifies the *User* at the *Relying Party* authorised to receive the *Attribute*s
- *Identity Service Provider/Attribute Service Provider* from which the *Attribute*s were sourced
- The *Identifier* that identifies the *Identity* at the source of the *Attribute*s
- Name of any *Attribute* or *Attribute* set authorised
- *Consent* decision. This may be "grant", "deny", or "ongoing"

6.3 *Single Sign On*/Single *Logout*

Single Sign On is an optional feature that an *Applicant* may implement in their system.

TDIF Req: IDX-06-03-01; **Updated**: Jun-21; **Applicability**: X
If *Single Sign On* is supported, then the *Applicant* *MUST* implement the following requirements to operate *Single Sign On*.

TDIF Req: IDX-06-03-02**; Updated:** Jun-21**; Applicability:** X
The *Applicant* *MUST* support the ability for a *Relying Party* to request that a *User* authenticates regardless of whether a pre-existing *Session* exists.

TDIF Req: IDX-06-03-02a**; Updated:** Jun-21**; Applicability:** X
The *Applicant* *MUST* implement a *single Logout* mechanism according to the *Federation Protocol* that it supports.

TDIF Req: IDX-06-03-03**; Updated:** Jun-21**; Applicability:** X
The *Applicant* *MAY* securely cache *Attributes* from an *Identity Service Provider* for the duration of an authenticated *Session* to support *Single Sign On*.

TDIF Req: IDX-06-03-03a**; Updated:** Jun-21**; Applicability:** X
If the *Applicant* securely caches *Attribute*s as per IDX-06-03-03, these *Attribute*s *MUST NOT* be accessible to the *Applicant's Personnel*.

TDIF Req: IDX-06-03-04**; Updated:** Jun-21**; Applicability:** X
The *Applicant* *MAY* restrict the expiration period for an *Authentication Session* to manage *Cyber Security Risks*.

6.4 User Dashboard

A *User Dashboard* is a way for an *Individual* to view their *Consumer History* and manage their *Express Consent*. A *User Dashboard is* an optional feature that an *Applicant* may implement in their *Identity System*.

TDIF Req: IDX-06-04-01; **Updated:** Jun-21**; Applicability:** X
If a *User Dashboard* is supported, then the *Applicant* MUST implement the following requirements for the operation of a *User Dashboard.*

TDIF Req: IDX-06-04-02**; Updated:** Jun-21**; Applicability:** X
The *Applicant* MUST display to the *Individual* their *Consumer History* and enable the *Individual* to view the *Express Consent* they have provided to share *Attributes* with a *Relying Party* or any third party.

TDIF Req: IDX-06-04-03**; Updated:** Mar-22**; Applicability:** X
The *Applicant* MUST NOT store *Attributes* of the *Individual* after the *Individual's* session at the *User Dashboard* has been terminated.

6.5 IdP Selection

The *Applicant 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.*

TDIF Req: IDX-06-05-01; **Updated**: Jun-21; **Applicability**: X
If *IdP Selection* is supported, then the *Applicant* MUST implement the following requirements for the operation of *IdP Selection.*

TDIF Req: IDX-06-05-02; **Updated**: Jun-21; **Applicability**: X
The list of *Identity Service Providers* presented by the *Applicant* to the *User* MUST be capable of meeting the *Credential Level* and *Identity Proofing Level* requested in the *Authentication Request*.

TDIF Req: IDX-06-05-03**; Updated:** Jun-21**; Applicability:** X
The *Applicant* MAY provide a mechanism for an *Individual's* selection of an *Identity Service Provider* to be remembered so the *Individual* does not have to select an *Identity Service Provider* (again) when accessing a *Relying Party*.

TDIF Req: IDX-06-05-03a**; Updated:** Jun-21**; Applicability:** X
Express Consent MUST be obtained from the *Individual* prior to offering the mechanism described in IDX-06-05-03.

TDIF Req: IDX-06-05-03b**; Updated:** Jun-21**; Applicability:** X

The *Individual* ***MUST*** have the ability to opt out of using the mechanism described in IDX-06-05-03.

Appendix A: Evidence types and verification methods

This Appendix sets out the *EoI document* types and the verification methods that an *Applicant* may support to confirm a claimed *Identity* is *legitimate* (*Legitimacy Objective*), confirm the operation of the *Identity* in the Australian community over time (*Operation Objective*), and confirm the link between the *Individual* and the *Identity* being claimed (*Binding Objective*).

Table 6 lists the *EoI document* types and the verification methods that an *Applicant* may support. A description of the verification methods is available in *TDIF 05A Role Guidance*. *EoI document* types and verification methods may need to change in the future as *Applicants* update *Identity Proofing* processes, security practices and the methods of provision.

Table 6: Evidence types and verification methods

Type of Evidence	Notes	Verification method
Legitimacy Objective - confirm the claimed *Identity* is legitimate		
Commencement of Identity documents		
Australian birth certificate	Issued by an Australian State or Territory Government Register of Births, Deaths and Marriages.	Source Visual
Australian Passport[24]	Issued in the *individual's* name or former name, within 3 years of the expiry date.	Source Technical Visual
Australian citizenship certificate	Issued in the *individual's* name or former name. If their name appears on their parents' certificate, they can use that.	Source Visual
Australian Visa	*Source Verified* using a Foreign Passport - A current passport issued by another country, with a valid entry stamp or visa	Source

[24] Although an Australia Passport in not evidence of *Commencement of Identity* in Australia, it can be used as proxy at *IP 2, IP 2 Plus* and *IP 3,* but not for *IP 4*. Use of the Australian Passport to provide evidence of *Commencement of Identity* should be considered on a risk management basis. Australian Passports are generally valid for 10 years and so will not always reflect changes of name. By contrast, many *RBDMs* are now updating birth records where a change of name has occurred and issuing a new certificate. This would mean that old birth records in the previous name could not be electronically verified.

Type of Evidence	Notes	Verification method
DFAT issued Certificate of Identity	Issued in the *individual's* name or former name by the Department of Foreign Affairs and Trade.	Source Visual
DFAT issued Document of Identity	Issued in the *individual's* name or former name by the Department of Foreign Affairs and Trade.	Source Visual
UN Convention Travel document (*Titre de Voyage*)	Issued in the *Individual's* name or former name by the Department of Foreign Affairs and Trade.	Source[25] Visual
Immicard	A card issued in the *individual's* name or former name by the Department of Home Affairs.	Source Visual
Aboriginal and/or Torres Strait Islander descent records	This includes proof of Aboriginal and/or Torres Strait Islander heritage	Visual
Certificate of Registration by Descent	Issued by the Australian Government as a verifiable citizenship certificate	Source Visual
Linking documents		
Australian marriage certificate	Issued by an Australian State or Territory Government	Source Visual
Change of Name Certificate	Legal change of name or deed poll certificate.	Source Visual
Australian divorce papers	In your name or former name. For example, a Decree Nisi or Decree Absolute.	Visual
Commonwealth victims certificate	Issued by a magistrate in Issued by an Australian State or Territory Government.	Visual
Australian birth certificate	Issued by a State or Territory Government Register of Births, Deaths and Marriages.	Source Visual
Operation Objective – confirm the operation of the *Identity* in the Australian community over time		
Use in the Community documents		
Concession and Health Care Cards	Issued by Services Australia.	Source Visual
Medicare Card	Issued by Services Australia.	Source Visual

[25] Note that the *DVS* can verify a UN Convention Travel Document as an *Australian travel document* or as an Australian Visa. In both cases, it should still be treated as a single document for the purposes of *Identity Proofing,*

Type of Evidence	Notes	Verification method
Student ID card	A current student ID card issued by an Australian secondary school, TAFE, university or Registered Training Organisation which includes the *Individual's* name and may also include their photo.	Visual
Bank or financial institution card, passbook, statement	Issued by a bank, credit union or building society. Card statements or passbooks must cover at least 6 months of financial transactions and be in the *Individual's* name. The *Individual's* signature must be on the card and their current address on the statement or passbook. Documents from foreign banks or institutions are not accepted.	Source Visual
Education certificate or certified academic transcript.	Issued by an Australian secondary school, TAFE, university or Registered Training Organisation which includes the *Individual's* name or former name.	Source Visual
Mortgage papers	For an Australian property in the name of the *Individual* or their former name. These need to be legally drawn.	Visual
Veterans Affairs card	A current card issued in the *Individual's* name.	Visual
Tenancy agreement or lease	A current formal agreement or lease in the *Individual's* name showing their address.	Visual
Motor vehicle registration	Current registration papers with the *Individual's* name, address and proof of payment.	Source Visual
Rates notice	A paid rates notice issued in the *Individual's* name with their address that is less than 12 months old.	Visual
Electoral enrolment	Proof of electoral enrolment in the *Individual's* name and showing their current address.	Source Visual
Postal Records	A history of at least 6 months of postal deliveries.	Source Visual
Telephone Records	Records showing 6 months of phone usage.	Source Visual
Any document listed in the *Photo ID* category	A document listed as a *Photo ID* can be used to satisfy the requirement in Table 1 for a UITC document if that document has not	Source Technical Visual

Type of Evidence	Notes	Verification method
	already been provided to satisfy a separate requirement in Table 1.	
Utility account	Issued in the *Individual's* name, with their address, that is less than 6 months old.	Visual
Superannuation statement	Issued in the *Individual's* name, with their address, that is less than 6 months old.	Visual
Seniors card	Issued in the *Individual's* name.	Visual
Land titles office records	Issued in the *Individual's* name.	Visual
Insurance renewal	Current insurance renewal for house and contents, vehicle, boat, or similar insurance in the *Individual's* name held for over 12 months.	Source Visual
Binding Objective – confirm the link between the *Identity* and the *Individual* claiming the *Identity*		
Photo ID documents		
Australian Passport	Issued in the *Individual's* name or former name, within 3 years of the expiry date.	Source Technical Visual
Australian State or Territory issued Drivers licence includes a digital Drivers licence)	A licence issued by an Australian State or Territory Government in the *Individual's* name with their photo. For digital Drivers licence the security features must be tested to ensure authenticity.	Source Technical Visual
Foreign passport[26]	A passport issued by another country, with a *Source Verified* valid entry stamp or Australian Visa, where applicable.	Source Technical Visual
Foreign military ID card	An identification card issued in the name of an *Individual's* by a foreign government showing a picture of the *Individual* and identifying the *Individual* as a current member of the defence forces of that government	Visual
UN Convention Travel document (*Titre de Voyage*)	Issued in the *Individual's* name or former name by the Department of Foreign Affairs and Trade.	Source Visual

[26] The foreign passport can be used to satisfy the requirement in Table 1 for a UITC document if it has not already been provided as part of the Australian Visa verification in the Commencement of Identity category

Type of Evidence	Notes	Verification method
Australian citizenship certificate	Issued in the *Individual's* name or former name by the Department of Home Affairs.[27]	Source
Indigenous Community Card[28]	*EoI* used to provide confirmation of identity for Aboriginal or Torres Strait Islanders who have not provided other *Identity Documents*.	Visual
Shooter or firearm licence	A current card issued in the *Individual's* name and includes their photo.	Visual
Aviation Security Identity Card	A current card issued in the *Individual's* name and includes their photo.	Visual Source
Maritime Security Identity Card	A current card issued in the *Individual's* name and includes their photo.	Visual Source
Australian Government issued *Photo ID* card (employee ID)	A *Photo ID* card issued by the Commonwealth, or an Australian State or Territory Government issued in the *Individual's* name and includes their photo. The card may include a validity period.	Visual
Australian Department of Defence Highly Trusted Token	A current card issued in the *Individual's* name and includes their photo.	Technical Visual
Defence Force identity card	Issued by the Australian Defence Force and shows the *Individual's* name and photo.	Visual
Police identity card	A current card issued in the *Individual's* name and includes their photo.	Visual
Australian State or Territory issued trade (work or business) licence	A current card issued in the *Individual's* name and includes their photo (e.g. trade licences, real estate agents, security agents etc.)	Visual
Tangentyere Community ID card	A current card issued in the *Individual's* name and includes their photo.	Visual
Proof-of-Age card[29]	Issued by an Australian State or Territory Government in the *Individual's* name and includes their photo.	Visual
Australia Post Keypass	A current card issued in the *Individual's* name and includes their photo.	Source Visual

[27] NB. Citizenship certificate may not have an actual photo embedded, but an associated photo is stored in the source environment.

[28] The *IDP* must satisfy itself that the quality of the card and card issuance process is sufficient to support its use as a Ph*oto ID document*.

[29] NB. State names vary but they have the same fundamental intent e.g. NSW/WA Photo Card, ACT Proof of Identity, Qld Adult Proof of Age, TAS Personal Information, NT Evidence of Age, VIC/SA Proof of Age.

Type of Evidence	Notes	Verification method
Working with children/Vulnerable card	A current card issued in the *Individual's* name and includes their photo.	Source Visual