05 - Biometric Binding Requirements and Guidance

Trusted Digital Identity Framework (TDIF) Release 4 (R4)
January 2020, version 0.1

CONSULTATION DRAFT
Digital Transformation Agency

This work is copyright. Apart from any use as permitted under the Copyright Act 1968 and the rights explicitly granted below, all rights are reserved.

Licence

With the exception of the Commonwealth Coat of Arms and where otherwise noted, this product is provided under a Creative Commons Attribution 4.0 International Licence. (http://creativecommons.org/licenses/by/4.0/legalcode)

This licence lets you distribute, remix, tweak and build upon this work, even commercially, as long as they credit the DTA for the original creation. Except where otherwise noted, any reference to, reuse or distribution of part or all of this work must include the following attribution:

Trusted Digital Identity Framework (TDIF)™: 05 – Biometric Binding Requirements and Guidance © Commonwealth of Australia (Digital Transformation Agency) 2019

Use of the Coat of Arms

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

Conventions

TDIF documents referenced by this document are denoted in italics. For example, TDIF: 02 - Overview is a reference to the TDIF document titled ‘02 – Overview’.

The abbreviations and terms used in this document including the key words “MUST”, “MUST NOT”, and “MAY” are to be interpreted as described in the current published version of the TDIF: 01 – Glossary of Abbreviations and Terms.

Contact us

The Digital Transformation Agency is committed to providing web accessible content wherever possible. This document has undergone an accessibility check however, if you are having difficulties with accessing the document, or have questions or comments regarding the document please email the Director, Digital Identity Policy at identity@dta.gov.au.
Document management

The Trust Framework Accreditation Authority (TFAA) has reviewed and endorsed this document for release.

Change log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Description of the changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Jan 2020</td>
<td>BB/JCS</td>
<td>Initial version</td>
</tr>
</tbody>
</table>
Contents

1 Add to Glossary......................................................................................................................... 1

2 Add to Role Requirements 2.9................................................................................................ 3
   2.1 Requirements for biometric binding Usage terms ................................................................. 3
      2.1.1 Unsupervised Biometric binding.................................................................................. 3
      2.1.2 Requirements for presentation attack detection ............................................................ 3
      2.1.3 Specific Requirements of unsupervised biometric binding .......................................... 4
1 Add to Glossary

**Acquired image.** An image of the individual’s face that is used as the sample for biometric matching. Source: TDIF.

**Biometric binding.** The process of linking a biometric with a validated identity, for instance by performing a biometric match of the face recorded on the acquired image of the individual with the face recorded on the relevant photo ID. Source: TDIF.

**Biometric binding personnel.** Personnel within the Applicant's identity service that perform a function in the biometric binding process. Source: TDIF.

**Biometric capability.** The product used by the Applicant for the purposes of identity proofing and biometric binding. Source: TDIF.

**Document biometric matching.** The process of verifying that the individual’s acquired image biometrically matches the corresponding image recorded in the individual’s claimed document. This process includes only claimed documents that contain a government issued and cryptographically signed image, such as a passport. Source: TDIF.

**Liveness detection.** A type of presentation attack detection that measures and analyses anatomical characteristics, involuntary or voluntary reactions. Liveness detection is used in order to determine if a biometric sample is being captured from a living subject present at the point of capture. Source ISO 30107.

**Manual face comparison.** The process of Biometric Binding Personnel visually verifying that the physically present applicant’s likeness matches the corresponding image recorded in the individual’s photo ID. Source: TDIF.

**Presentation attack (against a biometric system).** The use of an artificial object to mimic the characteristics of a valid biometric in order to subvert a biometric system. Source ISO 30107.

**Presentation attack detection.** The automated detection of a presentation attack. Source ISO 30107.
Source biometric matching. The process of verifying that the individual’s acquired image biometrically matches the corresponding image recorded in the individual’s photo ID. Source matching is performed by the Biometric Capability. Source: TDIF.

Supervised biometric binding. Biometric binding performed with the individual in the physical presence of the IdP. Source: TDIF.

[update term] Technical Verification. The act of verifying documentation using a cryptographically secure technical mechanism of the document, such as a secure chip or pdf document signature. Document biometric matching is one type of Technical Verification. Source: TDIF.

Unsupervised biometric binding. Biometric binding performed remotely via the internet. Source: TDIF.
2 Role Specific Requirements (insert at 3.9)

2.1 Requirements for biometric binding

2.1.1 Unsupervised biometric binding

**TDIF Req:** ID-03-09-01; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST** restrict access to the control of any aspects of the biometric binding capability exclusively to personnel that have completed the appropriate training pertaining to the exercise of such control.

**TDIF Req:** ID-03-09-02; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST** acquire the image and complete source biometric matching or source document matching when performing unsupervised biometric binding.

**TDIF Req:** ID-03-09-03; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST** undertake presentation attack detection when performing unsupervised biometric binding.

**TDIF Req:** ID-03-09-04; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST** complete the image capture and presentation attack detection processes as part of the same process before submission to unsupervised biometric binding. This is to prevent attacks that would exploit the separation of the presentation attack detection and the image acquisition.

2.1.2 Requirements for presentation attack detection

**TDIF Req:** ID-03-09-05; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST** employ presentation attack detection technology to ensure the acquired image is of a living human subject present at the point of capture.

**TDIF Req:** ID-03-09-06; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST** include liveness detection processes as part of presentation attack detection.

**TDIF Req:** ID-03-09-07; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST** employ presentation attack detection technology that includes data capture and system level monitoring as described by ISO 30107-1.

**TDIF Req:** ID-03-09-08; **Updated:** Jan-2020; **Applicability:** I
The Applicant **MUST** ensure that the presentation attack detection technology meets the requirements of at least Evaluation Assurance Level 1 as described by ISO 30107-3.

**TDIF Req: ID-03-09-09; Updated: Jan-2020; Applicability: I**
The Applicant **MUST** employ a qualified third-party testing entity with experience in biometric testing and ISO 30107 to test that the presentation attack detection technology meets the requirements for at least Evaluation Assurance Level 1 of ISO 30107-3.

**TDIF Req: ID-03-09-09a; Updated: Jan-2020; Applicability: I**
The Applicant **MUST** determine presentation attack detection outcomes in a trusted computing environment.

**TDIF Req: ID-03-09-09b; Updated: Jan-2020; Applicability: I**
All testing performed by the Applicant **MUST** be performed on an end-to-end solution that includes the presentation attack detection technology.

**TDIF Req: ID-03-09-10; Updated: Jan-2020; Applicability: I**
The Applicant **MUST** provide a report to the TFAA from the qualified third-party testing entity outlining that the Applicant’s presentation attack detection technology has been suitably tested to the specifications of at least Evaluation Assurance Level 1 of ISO 30107-3 and the test cases that were completed.

**TDIF Req: ID-03-09-11; Updated: Jan-2020; Applicability: I**
The Applicant **MUST** provide the TFAA with a report describing the completed presentation attack detection evaluation and corresponding results.

**TDIF Req: ID-03-09-11a; Updated: Jan-2020; Applicability: I**
This report **MUST** provide results for each presentation attack type with the closest possible adherence to reporting specifications as described in ISO 30107-3.

**2.1.3 Specific Requirements of unsupervised biometric binding**

**TDIF Req: ID-03-09-12; Updated: Jan-2020; Applicability: I**
To complete unsupervised biometric binding the Applicant **MUST** either:

- send the acquired image to the Photo ID Issuing Authority (or proxy) in the case of from source biometric matching; or,
• perform *from document biometric matching* of the acquired image against the image read directly from the photo ID RFID chip.

### 2.1.3.1 Requirements of *from document biometric matching*

**TDIF Req:** ID-03-09-13; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST** verify the authenticity of the image read from the photo ID RFID chip according to the Photo ID Issuing Authority’s instructions.

**TDIF Req:** ID-03-09-14; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST** only process claimed documents through *from document biometric matching* that contain a government issued and cryptographically signed image, such as a passport.

**TDIF Req:** ID-03-09-15; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST** use a biometric matching algorithm to perform one-to-one (verification) matching between the acquired image and the photo ID image.

**TDIF Req:** ID-03-09-16; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST NOT** use a biometric matching algorithm to perform one-to-many matching against a database of reference images as part of the biometric binding process.

**TDIF Req:** ID-03-09-17; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST** ensure their biometric matching algorithm is tested to determine the failure to enroll rate (if applicable), failure to acquire rate, false match rate and false non-match rate of the capability as per the reporting specification described in ISO 19795.

**TDIF Req:** ID-03-09-17a; **Updated:** Jan-2020; **Applicability:** I

This testing **MUST** be of a statistically significant volume in a verification scenario with comparable image types to production expectations.

**TDIF Req:** ID-03-09-18; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST** achieve a false match rate equivalent to ISO 19795-5 test grade Level 2. This requires a false match rate of not more than 0.1% and a false non-match rate of not more than 5%.

**TDIF Req:** ID-03-09-018a; **Updated:** Jan-2020; **Applicability:** I
The Applicant **MUST** record biometric matching outcomes in a trusted computing environment.

**2.1.3.1 Photo ID specific requirements**

**TDIF Req:** ID-03-09-19; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST** perform a successful match of the acquired image against the image read directly from the photo ID RFID chip.

**TDIF Req:** ID-03-09-19a; **Updated:** Jan-2020; **Applicability:** I

The photo ID image used for biometric matching **MUST NOT** be from a scan of a physical document.

**TDIF Req:** ID-03-09-20; **Updated:** Jan-2020; **Applicability:** I

Where the photo ID used is an Australian ePassport, the Applicant **MUST** check the Country Signing Certification Authority (CSCA) Certificate as per ICAO document validation guidelines OR perform a DVS check. Where the Australian passport security certificate is checked, the Australian Certificate Revocation List must also be checked.

**TDIF Req:** ID-03-09-20a; **Updated:** Jan-2020; **Applicability:** I

A DVS check **MUST** be performed by the Applicant where the photo ID used has no readable RFID chip available or the document security is lower than that of the Australian passport.

**TDIF Req:** ID-03-09-20b; **Updated:** Jan-2020; **Applicability:** I

A DVS check **MUST** be performed by the Applicant where the photo ID used is a foreign passport to ensure that the foreign passport is linked to a current visa.

**2.1.3.2 Image Quality**

**TDIF Req:** ID-03-09-21; **Updated:** Jan-2020; **Applicability:** I

The Applicant **MUST** produce an acquired image quality profile which details a set of minimum standards that the acquired image must meet before biometric matching.

**TDIF Req:** ID-03-09-21a; **Updated:** Jan-2020; **Applicability:** I

The acquired image quality profile **MUST** be informed by the properties and characteristics described by ISO 29794-5.
The Applicant capability **MUST** include automated quality controls and appropriate user-interface instructions that directs applicants to provide an image that meets the acquired image quality profile.

### 2.1.4 Requirements for manual face comparison

**TDIF Req:** ID-03-09-23; **Updated:** Jan-2020; **Applicability:** I
The Applicant **MUST NOT** attempt manual face comparison except in cases where source biometric matching or document biometric matching are not possible.

**TDIF Req:** ID-03-09-24; **Updated:** Jan-2020; **Applicability:** I
The Applicant **MUST** perform a DVS check as part of the manual face comparison to confirm the authenticity of a photo ID.

**TDIF Req:** ID-03-09-25; **Updated:** Jan-2020; **Applicability:** I
The Applicant **MUST** train relevant biometric binding personnel on manual face comparison techniques including, but not limited to:

- Techniques for individual feature comparison
- Awareness of racial and cognitive biases
- Presentation attack indicators
- Guided matching examples

**TDIF Req:** ID-03-09-26; **Updated:** Jan-2020; **Applicability:** I
The Applicant **MUST** maintain the information associated with each individual biometric transaction, including a log of activities that details which personnel collected data, what data was collected, when and where the data was collected.

**TDIF Req:** ID-03-09-27; **Updated:** Jan-2020; **Applicability:** I
The Applicant **MUST** have in place audit or random checking procedures to help detect fraud or inadequate manual face comparison and verification by biometric binding personnel.

**TDIF Req:** ID-03-09-28; **Updated:** Jan-2020; **Applicability:** I
The Applicant **MAY** retain a copy of an image of the person captured in supervised biometric binding processes until it has undergone manual face comparison by a specialist examiner or undergoes random checking.

**TDIF Req:** ID-03-09-28a; **Updated:** Jan-2020; **Applicability:** I
If this process takes place, the image MUST then be destroyed consistent with TDIF Req: PRIV-03-08-02.
3 Role Specific Guidance (insert at 3.9)

3.1 Biometric Binding use case

The use case covers the IdP creation of an identity at IP 2 Plus. This includes the
generic use cases for unsupervised and supervised biometric binding. At a high level,
this includes a check of the document either via DVS, security certificate check, or
visual inspection, and a check of the face against either against the document RFID
chip, via FVS, or by visual inspection.

3.2 Roles

The roles associated with this use case are:

- Identity Service Provider
- Individual
- Governance Body
- Photo ID Issuing Authority

This use case covers the applicant’s provision of the acquired image, the IdP
processing of the acquired image, the matching of the acquired image to the image
held by the Photo ID Issuing Authority and the return of a matching result.

3.3 Pre-conditions

The individual has provided IP 2 plus information (two or more documents). (Note:
this is assumed to be legitimate and sufficient for this use case)

The individual is looking to establish IP 2 Plus.

The individual has access to IdP application.

3.4 Post conditions

The individual has obtained digital identity at IP2 Plus.
3.5 Basic Flow

1. The individual accesses the IdP capability.

2. The individual completes pre-required information fulfilment on IdP capability, including the provision of two or more documents.

3. The documents are verified either via DVS check, security certificate check (passport only), or visual inspection.

4. The individual provides the acquired image through the IdP capability’s face image acquisition process.

5. The IdP capability completes biometric quality assessment (unsupervised).

6. The IdP capability completes Presentation Attack Detection (unsupervised).

7. Matching is undertaken either against the document RFID chip, via FVS, or by visual inspection.

8. The IdP collects required data for audit (matching, presentation attack data, personnel details). Note that this does not include retention of face images.

9. IP2 Plus is granted to the individual’s digital identity.

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

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

3.6 Success Criteria

If the Applicant's acquired image matches the image stored in the Issuing Authority's gallery/database, verification is successful and IP2 Plus is provided.

Else IP2 Plus is not provided.
3.7 Flow Diagram

Applicant access to IdP capability

Provision of photo ID + additional documents

DVS check

Security certificate check

AND/OR

Acquire applicant face image

Supervised

Manual face comparison

Image quality assessment

Presentation attack detection

Biometric matching

Record Audit Data

Unsupervised

Handle Quality Issue (Recapture)

Handle Potential Malicious Actor

Handle Non-Verification