Document Authenticity Verification Requirements

Final Document, July 09, 2024

This version:

https://fidoalliance.org/specs/idv/docauth/document-authenticity-verification-requirements-v1.1-fd-20240709.html

Issue Tracking:

GitHub

Editors:

Stephanie Schuckers (Clarkson University)
Chris Algrove (UK Digital Cabinet Office)
Rayissa Armata (IDNow)
Mark Brady (AU10TIX)
Tim Brown (Idemia)
Hsin Hau Hanna (Thales)
Fernando Martin (Thales)
Santosh Rajvaidya (Jumio)
Prashant Sharma (MasterCard)
Amy Shuart (Onfido)
Teresa Wu (Idimia)

Abstract

This document contains the FIDO Document Authenticity Requirements and Test Procedures for the Document Authenticity Verification Certification Program.

Table of Contents

2. Introduction§

The FIDO Alliance's mission is "Stronger, Simpler Authentication to Solve the World's Password Problem". This mission has begun to succeed with the platform adoption of FIDO2 and UAF solutions, but these are incomplete without strong options for account creation and account recovery. Many internet services, including financial and government services, require validation of a user's identity before they are allowed to create an account and attach FIDO Authentication. Similarly, when a user attempts to create an account, reset a password, or recover account access, their identity should be validated again. Weak account creation and account recovery can undermine FIDO's value proposition for strong security.

In general, the user experience includes presenting a government-issued identity document via a camera, and then a "selfie" photo or a live video. The validation system checks the format of the document, the document image and the selfie to score the validity and consistency of the information provided. There are a variety of potential attacks against document authentication including fake documents, stolen documents and a variety of environmental variables including bad lighting and poor cameras that can make the validation difficult. These potential attacks and environmental factors must be balanced against the user experience to provide a "safe" and "simple" solution that is consistent with the FIDO brand.

This document contains the FIDO Document Authenticity Requirements and Test Procedures for the Document Authenticity Verification Certification Program.

2.1. Audience§

The intended audience of this document is the Certification Working Group (CWG), IDWG, FIDO Administration, the FIDO Board of Directors, Document Authentication Vendors and FIDO Accredited Laboratories.

The owner of this document is the Identity Verification and Binding Working Group (IDWG).

2.2. FIDO Roles§

Certification Working Group
: FIDO working group responsible for the approval of policy documents and ongoing maintenance of policy documents once a certification program is launched.

Identity Verification and Binding Working Group
: FIDO working group responsible for the creation and maintenance of these requirements.

Vendor
: Party seeking certification. These vendors provide identity verification services and are responsible for providing the testing harness to perform both online and offline testing that includes enrollment systems (with data capture sensor) and verification software.

FIDO Accredited Laboratory
: Party performing testing. Testing will be performed by third-party test laboratories Accredited by FIDO to perform Document Authenticity Certification Testing and/or Document Authenticity Certification.

FIDO Accredited Document Authenticity Verification Laboratory
: Laboratory that has been accredited by the FIDO Alliance to perform FIDO Document Authenticity Verification Testing for the Document Authenticity Verification Certification Program.

FIDO Member
: A company or organization that has joined the FIDO Alliance through the membership process.

2.2.1. Document Authenticity Data and Evaluation Terms

Genuine Document
the original version of an identity document in its physical form that has not fabricated or been tampered with

> NOTE: Also synonymous with Authentic Document

Identity Document
A document issued by a State authority to an individual for providing evidence of the identity of that individual [reference: https://ec.europa.eu/home-affairs/pages/glossary/identity-document_en]

Document Type
An individual document grouping requested by the vendor to be tested

Fraudulent Document:
A fabricated identity document or a tampered version of an existing document. These can be digital or physical documents.

> NOTE: Photocopies and scanned images of genuine documents are not considered as fraudulent documents or document tampering. See Document Liveness.

Document Fraud Attack:
The techniques used to create fraudulent documents. These can be digital or physical and could include document tampering or creation of a counterfeit document.

Document Fraud instrument (DFI)
Object or image used in a document fraud attack (e.g. forgery or counterfeit).

DFI species
Class of document fraud attack instruments created using a common production method and based on different persons.

Document Tampering
Digital or physical modifications made to a genuine identity document which renders that document materially different from the evidence of identity that the document was originally issued for

Counterfeit Documents
Any document attempting to reproduce a genuine document made outside of the issuing authority of the document.

Document Liveness
A live document is the is presence of the original physical original document.

> NOTE: See § 2.3.2.12 Document Liveness.

Document False Accept Rate (DFAR)
The proportion of document verification transactions with document fraud that are incorrectly confirmed as genuine.

Document False Reject Rate (DFRR)
The proportion of genuine document verification transactions with truthful claims of an genuine document that are incorrectly denied.

Document Failure-to-Acquire Rate (DFTA)
Proportion of document verification attempts for which the system fails to capture or locate an image or signal of sufficient quality.

Document True Reject Rate (DTRR)
The proportion of document fraud correctly identified by the system.

Target of Evaluation (TOE)
The product or system that is the subject of the evaluation. See theTOE Description section in this document.

TOE Description
A description of the TOE provided by the vendor to the laboratory in advance of the certification.

Test Subject
User whose biometric data is intended to be enrolled or compared as part of the evaluation. See Section 4.3.2 in [ISOIEC-19795-1].

Test Crew
Set of test subjects gathered for an evaluation. See Section 4.3.3 in[ISOIEC-19795-1].

Target Population
Set of users of the application for which performance is being evaluated. See Section 4.3.4 in[ISOIEC-19795-1].

Test Operator
Individual with function in the actual system. See Section 4.3.6 in[ISOIEC-19795-1].

Approved Evaluator
FIDO Accredited Laboratory personnel acting as the Test Operator.

Document Verification Transaction
Sequence of attempts on the part of a user for the purposes of document verification. See section 4.2.3 in[ISOIEC-19795-1].

Document Verification
Process by which the user submits an identity document and an accept or reject decision regarding the authenticity of the document.

Blur
An image of an ID document or photo that is not clearly visible or are not sufficiently sharp.

Glare
A photo of a document where there is a reflection of a light source that hides useful information from the image.

2.2.2. Key Words§

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC 2119]](https://fidoalliance.org/specs/biometric/requirements/#biblio-rfc2119).

- SHALL indicates an absolute requirement, as does MUST.
- SHALL NOT indicates an absolute prohibition, as does MUST NOT.
- SHOULD indicates a recommendation.
- MAY indicates an option.

2.3. Scope§

Complete automated, online document authenticity verification requires multiple steps, some of which are in scope of this document and some of which will be covered by other documents.:

In scope:

1. Automatically verifying identity document authenticity

   This document focuses on automatically verifying identity document authenticity (item #1 above) for existing vendor solutions and provides certification criteria for vendors and test procedures that FIDO-Accredited Laboratories can use for evaluating document authentication capabilities.

   > NOTE: The current version of the certification program handles only automated checks. It is difficult to ensure the integrity of the current test design when a manual check is included; a specific test design would need to be devised to appropriately assess the performance involving manual checks. The vendor may include a manual component as part of the commercial product. This test is intended to measure the performance only of the automated version. Future versions of the certification program may expand to manual checks.

Out of Scope. To be included in future requirements documents:

1. Verifying that identity document pictures match a selfie picture or video of the subject
2. Verifying the liveness of the subject in the selfie

Separate documents (to be defined) will define certification criteria for liveness checks and the biometric match of “selfie” photos against the photo on the presented document.

Figure 1 *Automated Document Authenticity Verification Steps*

The following sub-sections include background information on Document Sophistication tiers and the Classification of Threats, and outlines for both what is in scope, and out of scope for this requirements document.

2.3.1. Document Sophistication§

Security documents have different levels of sophistication. Depending on the document’s inherent security characteristics, each document is classified into a tier. However, the existence of a security feature does not imply that the documentation authentication method checks these security features, as all may not be visible by a user’s device using visible light.

These document authenticity requirements focus on Tier 4 and Tier 3 documents. Tier 5, Tier 2, and Tier 1 documents are out of scope, but have been included as examples. The FIDO Secretariat SHOULD maintain a list of government documents and their respective tiers. Tier 2 and Tier 1 documents are out of scope because these documents do not contain sufficient security features to facilitate scaleable and effective fraud detection using only software and through a mobile device.

Tier 5 - Documents of this tier are highly-secured documents with state-of-the-art security features that may require a digital, or non-visual reading. Documents in this tier SHALL include the following technologies:

- embedded chip technology (e.g., contact card, RFID, NFC)*
- machine readable zone (MRZ) or barcode from which access keys can be derived

Tier 5 also SHOULD meet requirements for Tier 4.

Tier 5 is in scope.

Tier 4 - Documents of this tier are highly-secured documents with state-of-the-art security features. Documents in this tier SHALL include one or more of the following technologies:

- optically variable ink (OVI), holograms, watergrams
- primary photo interacts with the substrate / background print
- personalization font with unique character sets and/or diacritical marks
- guilloché (e.g., intricate and subtle patterns of thin interwoven lines)
- tactile laser engraving
- micro printing
- ghost image

Tier 4 also SHOULD meet requirements for Tier 3.

> NOTE: The existence of a security feature does not imply that the documentation authentication method checks these security features. For example, some features are not visible by a user's device using visible light.

Tier 4 is in scope.

Tier 3 - Documents in this tier lack advanced security features and are easier to execute fraud attacks, but still carry sufficient security features to enable automated verification using data cross-comparison, checksums, and other logical checks that can be scaled using machine reading. Documents have a consistent template format and font within a version. Document in this tier SHALL Include one or more of the following features:

- machine readable zone (MRZ)
- barcode

Tier 3 also SHOULD meet requirements for Tier 2.

Tier 3 is in scope.

Tier 2 - A low security document where only basic fraud checks can be performed and confidence in authenticity (based on a digital photo) is low.

- No cross-comparison possible due to missing Machine-Readable Zone (MRZ) or barcode; and/or
- The documents may not have consistent template format and/or fonts.

Tier 2 is out of scope.

Tier 1 - No material security features available and no fraud evaluation can be performed. Extraction only. Documents in this tier sometimes include hand-written documents.

Tier 1 is out of scope.

These document authentication requirements focus on Tier 4 and 3 documents. FIDO secretariat should maintain a list of government documents and their respective tiers.

2.3.2. Classification of Threats

This section contains background information explaining the classification of threats, including fraud type, and what types of threats are in scope and out of scope for this requirements document.

2.3.2.1. Counterfeit

Counterfeit documents are any attempt (digital or physical) to reproduce a genuine document made outside the issuing authority of the document. When using the term counterfeit document, it is referring to the entire document.

Examples of counterfeit techniques include:

- Complete digital fabrications using templates available online
- Fantasy and camouflage documents (e.g. country does not exist)
- Specimen documents
- Complete physical reproductions printed on any substrate (plastic/paper/etc.)

Counterfeit detection testing is in scope.

2.3.2.2. Forgery/Tampering

Forged documents are changes made to the document such as:

- Changing/tampering with any variable information digitally or physically
- Insertion or replacement of the applicant picture
- Removing information
- Can be digital or physical
- Usually refers to an altered SECTION within an EXISTING GENUINE document

A forged document usually refers to an altered section within an existing genuine document.

Photocopies and scanned images of tampered documents are considered as fraudulent documents or document tampering and are in scope.

> NOTE: Photocopies and scanned images of genuine documents, used without edit, are not considered as fraudulent documents or document tampering. Such non-live images can make it easier to obscure tampering and may be easier to confuse with forgeries or counterfeit documents. This may be considered in future versions of the requirements.

Resistance to the video or image replay of genuine documents stolen through malware or other means is currently out of scope. This will be considered in future parts of the certification program which consider the security integrity of the system.

Scanned images of genuine documents are considered genuine documents as part of the Digital Document Images Test. A photo capture of a photocopied genuine document shall not be included in the genuine document test.

2.3.2.3. Digital Tampering

Digital tampering refers to manipulation of the captured image of a document.

For example, digital tampering may include changing the following:

- Text (e.g., incorrect font, misaligned text)
- Images
- Portrait
- The presence of "boxes" around characters / fields coupled with interruptions of background printing.
- Sudden changes in the color of the portrait.

2.3.2.3.1. Physical Tampering

Physical tampering refers to physical alteration or reproduction of an identity document.

For the purposes of testing, the FIDO Accredited Laboratory can obtain images of documents that have undergone physical tampering, as part of the Digital Document Test.

Direct testing as part of the Physical Document Test for identity documents that have undergone physical tampering are currently out of scope, pending clarification of legal constraints around the ability to obtain fraudulent documents.

Forgery detection which includes Digital and Physical tampering are within the scope of this requirements document.

2.3.2.4. Expired or Invalidated Document

Fraudulent document test may include genuine document that are expired or invalidated. For example, the issuing authority or user may invalidate the document (e.g. by punching a hole in a Driver's License). Similarity Fraud

Similarity fraud is threats relating to mismatching the user in front of the camera to the ID document. Similarity fraud is within the scope of this program but will be covered in a separate requirements document.

2.3.2.5. Technical/Security Attack

Technical/security attacks (e.g. on encryption or backend systems) are an attack on the integrity or security of the system.

Technical/security attacks are out of scope of this requirements document.

2.3.2.6. Procedural

Procedural attacks are on the identification procedure as well (e.g. timing attacks, swapping cards during the process). Examples include attacks which are run against systems that take several pictures of a document. They involve swapping the identity document (real or fake) between capturing document images of the front and back side, or when capturing data vs. security features.

Procedural attack detection testing is out of scope of this requirements document.

2.3.2.7. Facial Liveness

Facial liveness attacks are on the liveness detection of the user, formally called Presentation Attack Detection[ISO30107-1]. Liveness attacks are within the scope of this program but are covered in a separate Face Verification Requirements Document, currently under development.

2.3.2.8. Presentation Attack

Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system [ISOIEC-30107-3].

2.3.2.9. Injection Attack

Attacks which insert (false) data bypassing the biometric capture module.

> NOTE: Injection attacks are within the scope of this program but are covered in a separate Face Verification Requirements Document, currently under development.

2.3.2.10. Deepfake

Deepfakes refer to videos, images, audio or text created with artificial intelligence (AI) technologies such as Generative Adversarial Networks (GANs) or Recurrent Neural Networks (RNNs). These content synthesis technologies enable media representations of non-existent subjects as well as subjects doing or saying things they've never done or said. [DeepTrust Alliance, 2020].

> NOTE: In the context of these requirements, deepfakes are a method to create fraud. Deepfakes can be detected by presentation attack detection if presented to the capture devices. Alternatively, deepfake may be used as part of an injection attack, bypassing the capture device. Injection attacks are addressed through securing the communication between the biometric capture and further processing.

2.3.2.11. Face Morph

A face morph is the face image which is created as a combination of two individuals, either of which can match the face morph. This is an attack typically done on the reference image by way of identity document tampering.

> NOTE: This is handled in these requirements as part of document tampering which could include a face morph.

2.3.2.12. Document Liveness

A live document is presence of the original physical original document. This version of the certification program does not consider Document Liveness.

Photocopies and scanned images of genuine documents are not tested as fraudulent documents or document tampering since the test methods of this program relies on a database of digital images to represent fraudulent documents. Such non-live images can make it easier to obscure tampering and may be easier to confuse with forgeries or counterfeit documents. Document liveness may be considered in future versions of the requirements as part of the Physical Document Test. Fraudulent documents are further described in Section § 6.2.1.1 Test Set Preparation for Document Fraud Attacks.

Document Liveness is currently out of scope, but may be considered in future versions of the requirements.

Resistance to the video or image replay of genuine documents stolen through malware or other means is currently out of scope. This will be considered in future parts of the certification program which consider the security integrity of the system.

> NOTE: Scanned images of genuine documents are considered genuine documents as part of the Digital Document Images Test. A photo capture of a photocopied genuine document SHALL not be included in the genuine test sample for the digital document image test. A photo capture of a photocopied tampered document can be included in the test sample for the digital document image test as part of the fraudulent document images._

2.3.2.13. Misuse

A misuse refers to the simple misuse of the system. This misuse is not necessarily malicious or intentional.

Misuse detection is out of scope of this requirement document.

2.3.3. Document Types

A vendor shall specify the set of document types to be assessed. Document type is defined by the combination of the Country of origin and document classification. Document classification is the originating purpose of the document and may include national identity card, driving license, passport, residence permit, visa, voter identification card or any other issued identification document. Different printings (versions, year releases or iterations) will be considered within the same document type. Vendor requests for document type certifications shall follow the above pattern to specify the set of document types covered. Vendors may additionally request more specificity in the document types to be covered, defining each as the combination of country of origin,

domestic region of origin (such as state or province), and document classification. The set of document types requested by the vendor may be of any supported document sophistication tier. Tier 5 documents are in scope when the region or requested set under test requires them for a representation of the public document mix for that area.

> NOTE: For example a vendor may request specificity for "US Driver's Licenses" which doesn't contain Tier 5 document types, whereas "US Documents" or "North American Documents" would contain Tier 5 documents that need to be represented in the test set.

3. Criteria§

This chapter contains the requirements that are mandatory to be met by a product in order to obtain certification.

> NOTE: The following paragraphs assume specific requirements for the DFRR and the DFAR. Also, specific requirements for test sizes are derived from these values. The values have been briefly discussed within the FIDO IDWG and IDWG DocAuth How Sub Group, but it should be clearly mentioned that these values should only be seen as examples. Due to the need to derive test size requirements from the values for the error rates, it has not been easily possible to work with placeholders (like "X"). The final values for the requirements for DFRR and DFAR will need further discussion within the complete IDWG.

3.1. Performance Levels§

3.1.1. Document False Reject Rate (DFRR)§

The Document False Reject Rate (DFRR) section focuses on the error rate for genuine (legitimate) documents.

Document False Reject Rate SHALL meet the requirement of less than 10% for the upper bound of a 95% confidence interval. DFRR is measured at the transaction level, defined below.

The actual achieved DFRR SHALL be documented by the laboratory. Requirements on reporting for Digital Image Test can be found in section § 6.2.2 Digital Reporting Requirements, Requirements on reporting for Physical Document Test can be found in section § 7.2.4 Physical Reporting Requirements.

The threshold, or operational point, SHALL be fixed during testing for ALL document verification tests, as described in this requirements document. It shall be set in accordance with the descriptions in the § 4 TOE Description.

For Digital Document Images Test, the capture device is bypassed and the images of genuine and fraudulent documents are tested directly by the processing and decision components of the remote identity verification solution. Document Failure-to-Aquire Rate (DFTA) in this program is only relevant for the Physical Document Test.

For Physical Document Test testing described in section§ 7 Physical Document Tests, the number of attempts allowed per document verification transaction SHALL be fixed during testing. It is set by the vendor and documented in the TOE Description. The number of attempts SHALL be no more than 5. For the purposes of testing with human subjects, the total time of the transaction SHOULD be no longer than 200 seconds and the document processing time;, once request is sent to the document verification processing engine, SHOULD be less than 60 seconds.

DFRR SHALL be estimated by the following equation:

DFRR for the Digital Image Test (%) = (Number of Genuine Transactions for which the decision is reject)*100 / (Total Number of Genuine Document Verification Transactions Conducted)

DFRR for the Physical Document Test (%) = (Number of Genuine Transactions for which the decision is reject OR DFTA for all attempts)*100 / (Total Number of Genuine Document Verification Transactions Conducted)

All errors encountered during the testing SHALL be recorded.

3.1.2. Document False Accept Rate (DFAR)§

The Document False Accept Rate section focuses on the error rate for fraudulent documents.

Each of the selected Level A, B, and C Document Fraud Instrument (DFI) species SHALL achieve a DFAR of less than 10%. Levels A, B, and C are defined in section § 6.2.1.1 Test Set Preparation for Document Fraud Attacks. This section describes levels of sophistication of the document fraud attacks.

Document False Accept Rate SHALL meet the requirement of less than 10%. DFAR is measured at the transaction level.

The actual achieved DFAR SHALL be documented by the FIDO Accredited Laboratory. Requirements on reporting for Digital Image Tests can be found in section § 6.2.2 Digital Reporting Requirements. The threshold, or operational point, SHALL be fixed during testing for ALL Document Verification Tests, as described in this requirements document. It shall be set in accordance with the descriptions in the TOE Description.

The number of attempts allowed per document verification transaction SHALL be fixed during testing. It is set by the vendor and documented in the TOE Description.

3.1.2.1. Limitation§

The calculation of DFAR SHALL be based on the following equation:

DFAR (%) = (Number of Fraudulent Document Verification Transactions for which the Decision is Accept) * 100 / (Total Number of Fraudulent Document Verification Transactions Conducted)

3.2. Statistical Analysis§

The following description contains a stepwise description of the test:

1. An independent laboratory shall derive a test set S from their test database D that complies with the following requirements:
2. S shall only contain Images that are compliant to the requirements of the§ 4 TOE Description.
3. S shall contain images of at least 100 genuine documents.
4. S shall contain images of at least 300 fraud documents.
5. S shall be representative of the document types that the TOE claims to recognize; this specification means that S shall at least contain three images of genuine documents and three images of fraudulent documents for each document type that the TOE claims to recognize in its TOE Description.
6. For each image in S, the developer shall assign a number as the filename and maintain additional information (fraud, genuine, resolution, etc.) separately. The background of this requirement is that the TOE must not have any chance to recognize the type of image by its name.
7. The independent laboratory shall shuffle all images of S and submit them to the TOE one after the other. The answer of the TOE (genuine, fraud) shall be recorded along with any additional information.
8. After the test has been completed, the FIDO Accredited Laboratory SHALL rate all answers of the TOE and compile a list with a comprehensive test overview containing the following columns:

Test Overview Required Columns

Timestamp	image	expected result	result	comment
...	….	...	….	..

From the test list, the independent laboratory shall calculate:

- Observed DFAR
    1. The variance of the DFAR as follows n*p*q where q=(1-p), n is the number of attempts with images of fraudulent documents and p=observed DFAR
    2. The upper value P_U of the confidence interval (at 95% confidence) as follows $P_U = p + 1.96 * \sqrt{\frac{p(1-P)}{n}}$
- Observed DFRR
    1. The variance of the DFRR as follows n*p*q where q=(1-p), n is the number of attempts with images of fraudulent documents and p=observed DFRR
    2. The upper value P_U of the confidence interval (at 95% confidence) as follows $P_U = p + 1.96 * \sqrt{\frac{p(1-P)}{n}}$

The test has been passed if the upper bound of the confidence interval for the DFAR is below 10% and the upper bound of the confidence interval for the DFRR is below 10%.

> NOTE: Recommend using 95% confidence value which results in a c value of approx. 1.96.

> NOTE: Test sizes are designed in a way that for both test sets (genuine and fraudulent) may show one error and would still pass. If working with minimum numbers of the test sizes, the TOE would fail with two or more errors per test set._

4. TOE Description§

In the beginning of the certification process, the vendor shall provide a TOE Description to the laboratory and to FIDO. This TOE Description is intended to cover all relevant aspects of the TOE with respect to the certification. It serves the vendor, the Accredited Laboratory and FIDO to develop and document a common understanding of the system that shall be certified. After the certification is finished, this document is also helpful for relying parties as it contains a comprehensive description of all relevant information for the certification.

The TOE Description shall, at a minimum, cover the following topics:

- A description of the system seeking certification and its boundaries (the TOE).
- A description of the specific Tier 3, Tier 4, and Tier 5 documents that the TOE supports.
- A description of the requirements that the TOE has for images to process (e.g. minimum resolution); vendors can set different requirements to evaluate different document sophistication levels.
- A description of the transaction policy of the TOE (i.e. how many attempts are allowed per transaction).
- A description of any parameters that can be used to adjust the performance or security of the TOE and their chosen settings.
- A list of supported consumer device types, platforms and versions supported. The test is limited to consumer devices (mobile phones, tablets, personal computer). Dedicated document scanners are out of scope. Specific devices under test will be managed by the Test Laboratory with guidance from the FIDO Secretariat.

Additional TOE description for Tier 5 documents:

- For vendors that support Tier 5 documents, vendors SHALL indicate which forms of evaluation they seek: (1) the NFC chip read and/or (2) an optical image of the Tier 5 document.
- For evaluations of both NFC and optical for Tier 5 documents, evaluation of Tier 5 documents SHALL be performed separately for (1) the NFC chip read and (2) an optical image of the Tier 5 document. Results

SHALL be reported separately as Tier 5 (NFC) and Tier 5 (optical) and SHALL be indicated separately on the certificate.

- A description of how fallback occurs when NFC cannot be read for Tier 5 documents SHALL be provided.

> NOTE: Evaluation of Tier 5 (optical) should yield similar results to a Tier 4 assessment.

5. Common Test Harness§

For each system to be evaluated, the vendor SHALL provide to the FIDO Accredited Laboratory a solution which automatically verifies identity document authenticity without manual verification by a human, and, has at minimum:

1. For Digital Document Images Test: Functionality to perform the Digital Images tests for document-only evaluation, according to specifications defined in section § 6 Digital Document Images Test.
    1. Version of documentation authentication solution that supports:
        1. Either cloud or localized version which meets the following:
            1. The TOE SHALL be provided to the laboratory as a software container. This container can be hosted by the laboratory or a cloud service provider at the discretion of the laboratory. The lab must not dictate with cloud service provider must be used.
            2. The vendor and FIDO certified laboratory shall enter into an agreement specifying the terms and conditions:
            3. Vendor SHALL create a specific environment for testing, separate from the commercial or development environment.<\li>
            4. The TOE SHALL be in complete control of the FIDO Accredited Laboratory<\li>
            5. Laboratory SHALL have exclusive access to the TOE during the test. <\li>
            6. Testing images and any other personal data SHALL not be stored for later use by vendor or shared with the vendor in any other way.<\li> Note: For example, this can be accomplished by creating a virtual machine.
        2. Ability to accept an image
        3. Document image processing for document authentication purposes
        4. Providing results to the FIDO Accredited Laboratory, including:
            1. Document failure to acquire/process.
            2. Success/failure of document authentication.
2. For Physical Document test: Functionality to perform the Physical Image tests for document-only evaluation, according to specifications defined in section § 7 Physical Document Tests.
    1. Device application software for each supported platform that supports:
        1. Document image capture (either via on-device or connected camera).
        2. Document image processing for document authentication purposes
        3. Version of a cloud service provided to the laboratory, either cloud or localized version which is meets the following
            1. It SHALL be in complete control of the FIDO Accredited Laboratory,
            2. Vendor SHALL not have access during testing.
            3. Testing images and any other personal data SHALL not be stored for later use by vendor or shared with the vendor in any other way.
        4. Provides results to the FIDO Accredited Laboratory, including:

1. Document failure to acquire/process (optional).
2. Success/failure of document authentication.

NOTE: Any cloud version of software SHALL be in complete control of the vendor and which the vendor has no access during testing. This is required by [[!ISO17025:2017]], is to ensure the integrity of the test, and ensures privacy of test subjects._

5.1. Security Guidelines§

For security purposes, all test subject data collected by the FIDO Accredited Laboratory or the vendor during testing should be treated confidentiality and data shall be protected using cryptographic algorithms listed within the FIDO Authenticator Allowed Cryptography List.

The FIDO Accredited Laboratory and vendor SHALL report to FIDO the process used to help assure TOE consistency and security. See the [DA-CertPolicy] for details.

6. Digital Document Images Test§

This section provides a testing plan using digital images of identity documents, covering genuine documents and fraudulent documents.

Scanned images of genuine documents are considered genuine documents as part of the Digital Document Images Test. A photo capture of a photocopied _genuine_ document shall not be included in the test sample for the digital document image test. A photo capture of a photocopied _tampered_ document can be included in the test sample for the digital document image test as part of the fraudulent document images.

Fraudulent document images can be scanned/captured from fraudulent documents, or digitally manipulated document images.

The evaluation measures DFRR as well as the DFAR.

Digital Document Images Testing shall be completed using the following approach.

Digital Images tests shall not consider Failure-to-Acquire Rate, but shall assume that the FIDO Accredited Laboratory collects images that are suited for the vendor's specifications. Images rejected due to quality issues when images are compliant with vendor requirements should be considered false rejections if they are genuine or correct rejections if they are frauds.

6.1. Test Environment§

No test subjects are required. This procedure will require the document images to be properly classified.

Vendors SHOULD provide a tool to use to input the test samples in the defined format and organization, perform the document authentication process, and deliver a result as specified.

- Test samples are collected or prepared by the FIDO Accredited Laboratory, as described in section§ 6.2 Test Sets.
- Vendor tool will use as input the test samples properly structured and formatted as defined section§ 5 Common Test Harness.
- Vendor tool will provide a response for each test sample with the defined format.

6.2. Test Sets§

The Test Sets are:

- The set of fraudulent document images gathered for evaluation.
- The set of genuine document images gathered for evaluation.

The FIDO Accredited Laboratory is responsible for independent acquisition of the test set in advance of the tests, and vendors SHALL NOT have access to the test sets being used.

The test set SHALL cover every document type that the vendor has requested to be certified. The list SHALL specify document type and all versions that are in circulation of that ID document.

Fraudulent documents shall include examples of document frauds as described in § 6.2.1.1 Test Set Preparation for Document Fraud Attacks.

For genuine documents, the test set shall have a minimum size of 300 images.

At least one of each listed document type SHALL be included in the geniune test set. The composition of the test set for geniune documents SHOULD be reasonably balanced across document types and SHALL be approved by the FIDO Secretariat prior to testing. The exact composition of the test set SHALL be strictly confidential to the lab and FIDO and SHALL not be shared with the vendor prior to the test.

For fraudulant documents, the test set shall have a minimum size of 300 images.

At least one of each listed document SHALL be included in the fraudulant test set. The composition of the test set for fraudulant documents SHOULD be reasonably balanced across document types and SHALL be approved by the FIDO Secretariat prior to testing. The exact composition of the test set SHALL be strictly confidential to the lab and FIDO and SHALL not be shared with the vendor prior to the test.

The requirements on the test size have been developed under consideration of “Rule of 3” and “Rule of 30” as described in [ISOIEC-19795-1].

6.2.1. Quality of Images

Images SHALL be good enough quality to be processed. The lab SHALL ensure that the test set has realistic image quality requirements. Parameters shall be provided to vendor and at a minimum SHALL include:

- Resolution, at least 300 dpi.
- Minimal compression (lossless compression, or lossy compression with minimal artifacts)
- Absence of image noise such as glare, lighting and blur, , unless the lab purposely includes this as part of Document Fraud Attack.
- Consistent cropping
- Absence of visual obstruction
- Absence of damage to the document

The quality characteristics of the test set SHALL be documented by the FIDO Accredited Laboratory and reviewed by the FIDO Secretariat prior to testing. FIDO Secretariat SHALL ensure that image quality are relevantly consistent between FIDO accredited laboratories.

6.2.1.1. Test Set Preparation for Document Fraud Attacks

To test frauds, the FIDO Accredited Laboratory will create a dataset of images of Document Fraud Attacks. Typically, the FIDO Accredited Laboratory will create fraudulent documents, either digitally or capturing an image (either through a scanner or taking a photograph) of a physical document that has been tampered. Part of the test set SHALL include printing the digitally tampered document and recapturing through a scanner or mobile capture. This type of attack simulates a process that an attacker may follow. The FIDO Accredited Laboratory does NOT need to secure actual counterfeit documents to prepare the digital image database.

Document fraud attacks vary by fraud type and can be categorized by level of sophistication. The document

image test set will represent these types of attacks as described below.

6.2.1.2. Levels of Document Fraud Attack

Level A

Level A attacks involve the creation and use of simple fabricated identity documents either without security features or in which static security features are simply printed on the document and do not change. Other basic checks like checksums and MRZ codes may or may not be correct. Use of expired or specimen (i.e., sample) documents is also a level A attack.

Attacks for physically tampered documents involve very simple manipulation of a genuine identity document, such as gluing a different identity photo over the document identity photo or manipulating data fields using common household materials and tools (e.g. whiteout, paper glued over data field, etc.).

Attacks can include images of fraudulent documents that are deliberately blurred in order to obscure fraud.

Level A attacks are in scope for testing.

Level B

Level B attacks involve the creation and use of a more advanced counterfeit document that contains security features, but those features may not be correct for the type of document used. Checksums and MRZ codes are correct.

Attacks for physically or digitally tampered documents involve more sophisticated manipulation of a genuine identity document, such as modifications using professional photo editing software like Photoshop. Checksums and MRZ codes may not be correct. This could include more sophisticated methods of manipulating the facial image, like face morphing.

Attacks can include images of fraudulent documents that are deliberately blurred in order to obscure fraud.

Level B attacks are in scope for testing.

Level C

Level C attacks require expert creation of a fraudulent document that looks like the real document and has formatting as well as security features that emulate the genuine document. Checksums and Machine-Readable Zone (MRZ) codes have the correct format.

Attacks for physically or digitally tampered documents involve sophisticated modifications of a genuine identity document. Attackers may insert a new photo under security features, use specialized foils to recreate security features, or change data fields using the correct font and other sophisticated methods.

Attacks can include images of fraudulent documents that are deliberately blurred in order to obscure fraud.

Level C attacks are in scope for testing.

Level D

Level D attacks are typically state sponsored in nature, organized malicious actors with access to creation of genuine documents or large criminal organizations and involve very state-level counterfeit documents that can only be detected by specialized equipment or additional means such as black/white lists or origins tests. This includes creating attacks based on tampered or cloned identity chips (which may communicate with NFC).

Level D attacks are currently out of scope for testing.

6.2.2. Digital Reporting Requirements

The following SHALL be included in an Evaluation Report to the vendor:

- Summary of the FIDO Certification and Requirements, including versions of the Requirements (this document) and the [DA-CertPolicy] used at the time of testing
- List of documents supported and tested,
- Number of documents tested for each document supported
- Description of the test environment
- Description of the test platform
- Number of genuine document verification transactions
- Number of fraudulent document verification transactions
- Number and description of document fraud attacks
- Document False Acceptance Rate (DFAR) per level of sophistication
- Document False Rejection Rate (DFRR) per level of sophistication
- A final verdict on whether the TOE complies with the requirements

Please note that the log SHALL also include all information about the Fraud Detection tests.

6.3. Testing§

The vendor tool will be configured to use the samples set provided by the FIDO Accredited Laboratory and be executed to launch the document authentication process for each one of the samples.

For each test sample, the TOE will provide an authentication result (accept or reject), which will enable the FIDO Accredited Laboratory to confirm the correct or wrong authentication result.

Wrong results are when a sample where the expected output is to be genuine, and the response denies the authenticity (DFRR), or when a sample is a crafted image or any kind of fraudulent image and the tool response claims it is genuine (DFAR).

Vendors may have solutions which can adjust the threshold which changes the risk tolerance. The TOE shall be configured at a fixed threshold for certification and shall be used for the entire test. If a vendor would like certification at multiple settings, the vendor SHALL submit multiple TOEs for certification.

6.3.1. Evaluation with Genuine Document Images§

6.3.1.1. Document Verification Transaction§

For each document verification attempt, the test operator SHALL conduct a Document Verification Transaction for each genuine document Image. The transaction processing time SHOULD NOT exceed 30 seconds.

6.3.1.1.1. Genuine Document Errors§

A document failure to acquire SHALL be declared when the document authentication system is unable to process the document during a transaction. The document verification test harness SHALL indicate to the FIDO Accredited Laboratory when a failure to acquire has occurred. If at least one failure to process or acquire is recorded, the FIDO Accredited Laboratory SHALL confirm that the image format meets the criteria defined in the § 4 TOE Description. If the image format is confirmed to meet the requirements, each failure to acquire SHALL be counted as a genuine document error.

> NOTE: A failure to acquire in a digital image test is mostly likely a failure to process.

A genuine document error SHALL be declared if the document authentication system produces a reject decision.

The manner in which the FIDO Accredited Laboratory records failure to acquire and genuine document errors are left to the FIDO Accredited Laboratory, but SHALL be done automatically to avoid introducing human error.

6.3.1.1.2. Document False Reject Rate (DFRR)

Document False Reject Rate (DFRR) SHALL be calculated according to requirements in section § 3.1.1 Document False Reject Rate (DFRR).

6.3.2. Evaluation with Document Fraud Instruments (DFI) Images

A minimum of 300 images of Document Fraud Instruments (DFI) SHALL be created which reasonably covers varying geographies, document types and identities, based on the Level 3 and Level 4 documents that are supported by the TOE.

The Fraudulent Test Set SHALL contain:

1. At least 30% DFIs at Level A representing at least 10 or more DFI Species (e.g. varying font, physical versus digital tampering).
2. At least 30% DFIs at Level B representing at least 10 or more DFI Species (e.g. physical versus digital tampering).
3. At least 10% DFIs at Level C representing at least 1 or more DFI Species (e.g. physical versus digital tampering).

Procedures and materials to create the DFI SHALL be provided to the FIDO Secretariat. The FIDO Secretariat SHALL ensure that DFI species selected and created (1) reasonably cover geographies and document types and (2) are relatively equivalent between laboratories.

6.3.2.1. Document Verification Transaction

For each document verification attempt, the test operator SHALL conduct a Document Verification Transactions for each Document Fraud Instrument. The transaction processing time SHOULD NOT exceed 30 seconds.

6.3.2.1.1. Document Fraud Errors

A document failure to acquire SHALL be declared when the document authentication system is processing the document during a transaction. The document verification test harness SHALL indicate to the laboratory when a failure to acquire has occurred. Each failure to acquire SHALL be counted as a correct document fraud rejection.

> NOTE: A failure to acquire in a digital image test is mostly likely a failure to process.

A document fraud error SHALL be declared if the document authentication system produces an accept decision.

The manner in which the FIDO Accredited Laboratory records failure to acquire and impostor presentation attack errors are left to the FIDO Accredited Laboratory, but SHALL be done automatically to avoid introducing human error.

6.3.2.1.2. Document False Accept Rate (DFAR)

Document False Accept Rate (DFAR) SHALL be calculated according to requirements in section § 3.1.2 Document False Accept Rate (DFAR).

7. Physical Document Tests§

This section focuses on testing genuine physical documents. The purpose of the physical document test is as follows:

- Reveal a solution inherent end-to-end document rejections, including capture failures (failure-to-acquire)
- Assess the impact of the capture system on the performance of underlying algorithm

For example, if the capture system is artificially too easy, this will result in poor images sent to the underlying algorithm and result and increased errors of the underlying algorithm.

The testing SHALL be performed by the FIDO Accredited Laboratory on the TOE provided by the vendor. The evaluation measures the Document False Reject Rate (DFRR) and the Document Failure-To-Acquire rate (DFTA).

7.1. Test Environment§

The test environment for Physical Document Tests SHALL represent typical operating conditions for normal usage of the solution.

7.1.1. Capture Devices§

At least two device(s) shall be tested for each device category (laptop, tablet, mobile device) and platform supported by the solution provider. If the vendor supports web-browser and native apps, both SHALL be tested. The software provided by the vendor as part of the Test Harness SHALL be installed on the devices that the FIDO Accredited Laboratory provides.

The FIDO Accredited Laboratory SHALL maintain a collection of commonly used consumer devices of each device type and platform. The FIDO Accredited Laboratory SHALL periodically update the collection to reflect the current state of the device market, both for new and older devices.

7.1.2. Face Verification (Optional)§

A related FIDO Certification Program is focused on performing face recognition from the image captured from the document compared with a "selfie" face image of the test subject. For a TOE that is undergoing both the Document Authenticity Verification and Face Verification Certification programs, the image captured from the document SHALL ensure there is at least 90 pixels between the eyes of the photograph of the individual.

7.1.3. Lighting§

Lighting shall be representative of a typical office or residential environment.

7.1.4. Pre-Testing Activities§

The test organization shall take steps to ensure that the hardware/software is installed and configured appropriately and shall verify that the system is operating correctly.

> NOTE: Installation, configuration, and verification of system operations may involve supplier(s).

7.2. Test Sets§

The Test Set is the physical documents gathered for evaluation. The Test Crew shall provide their own identity documents for testing.

Any form of digital image (photocopies, printout of scanned image, scanned images) are out of scope as part of the Physical Document Test.

Photocopies and printouts of scanned images of genuine documents are not considered as fraudulent documents or document tampering. These are out of scope for the Physical Document Test since it is not a physical document.

A scanned image of a physical document is out of scope for the Physical Document Test.

Such non-live images can make it easier to obscure tampering and may be easier to confuse with forgeries or counterfeit documents. This may be considered in future versions of the requirements. Tampered or fraudulent documents are further described in section § 2.3.2.2 Forgery/Tampering.

Scanned images of genuine documents are considered genuine documents as part of the Physical Document Images Test. A photo capture of a photocopied _genuine_ document shall not be included in the test sample for the digital document image test. A photo capture of a photocopied _tampered_ document can be included in the test sample for the digital document image test as part of the fraudulent document images.

7.2.1. Size of Test Set

Number of genuine documents for each document type covered by a test SHALL be 100.

7.2.2. Test Crew and Associated Genuine Documents

The minimum number of subjects for a test (Test Crew) SHALL be 100. Each subject SHALL provide at least one genuine document from the list of supported documents provided by the vendor. The FIDO Accredited Laboratory SHALL make it clear to the test subject in the recruitment process that the test subject is required to bring a genuine document. For example, asking subjects to certify that their document is genuine prior to coming to the test. The FIDO Accredited Laboratory SHALL manually check the document to ensure it is a genuine document to the extent possible. The number of subjects may be decreased if a subject is able to provide multiple documents from the supported list, e.g. a passport and a driver's license.

Test subjects SHALL be recruited such that the test set represents the document requirement as follows. The test set SHALL cover all categories and sophistication levels of documents (e.g. passports, national IDs, drivers licenses, documents with NFC, etc.) that are claimed by the vendor as described in Section [[### Document Types]], as well as be balanced across document categories. Documents included in the test set SHALL be in circulation at the time of the test.

The proposed composition of the test set SHALL be approved by the FIDO Secretariat prior to testing.

The population SHALL be experienced with the TOE in general and SHALL be given a possibility to try and acquaint themselves with the TOE before starting to perform recorded document verification transactions. The population SHALL be motivated to succeed in their interaction with the TOE and they SHALL perform a large number of interactions with the TOE during a short period of time.

The laboratory test SHALL not damage the physical documents.

7.2.3. Population Demographics

The population SHALL be representative of the target market in relationship to age and gender. Age and gender recommendations are taken from [ISOIEC-19795-5] for access control applications (Section 5.5.1.2 and 5.5.1.3). The following targets SHALL be used for age and gender. Minor deviations from these numbers may be acceptable if agreed by the FIDO biometric secretariat.

Population Demographic Requirements for Age

Age	Distribution
< 18	0%
18-30	25-40%
31-50	25-40%
51-70	25-40%
> 70	0%

Population Demographic Requirements for Gender

Gender	Distribution
Male	40-60%
Female	40-60%

7.2.4. Physical Reporting Requirements§

The following SHALL be included in the Evaluation Report to FIDO and the Vendor:

- Summary of the FIDO Document Authenticity Verification Certification and Requirements, including versions of the Requirements (this document) and [DA-CertPolicy] used at the time of testing.
- Number of documents tested
- List documents tested (type, country, etc.)
- Test crew description (gender, age, etc.)
- Description of the test environment (devices used in testing, etc.)
- Description of the test platform
- Number of genuine verification transactions
- Distribution of Genuine Verification Transaction Time
- Failure to Acquire Rate
- Failure to Acquire Rate per level of sophistication
- Document False Rejection Rate (DFRR)
- Document False Rejection Rate (DFRR) per level of sophistication

*Note: Evaluation of Tier 5 documents are evaluated with and without NFC. Results SHALL be reported separately as Tier 5 (NFC) and Tier 5 (optical).

7.3. Genuine Testing§

Document authentication transactions SHALL be conducted without test operator assistance. Any kind of guidance SHALL be provided by the TOE in a similar way to the final application.

The document authentication process may be different depending on the TOE. For instance, this process MAY require documentation authentication after every attempt, or MAY allow for multiple image acquisition attempts before document authentication. For testing, this process SHALL be similar to the final application.

7.3.1. Genuine Document Authentication Transaction§

Genuine document authentication transactions SHALL be performed according to[ISOIEC-19795-1] section 7.4, inasmuch as these requirements map to document authentication. These requirements are a lightly edited version of [ISOIEC-19795-1]:

Genuine transaction data shall be collected in an environment, including noise, that closely approximates the target application. This test environment shall be consistent throughout the collection process. The motivation of test subjects, and their level of training and familiarity with the system, should also mirror that of the target application.

The collection process should ensure that presentation and channel effects are either uniform across all users or randomly varying across users. If the effects are held uniform across users, then the same presentation and channel controls in place during enrolment should be in place for the collection of the test data. Systematic variation of presentation and channel effects between enrolment and test data will lead to results distorted by these factors. If the presentation and channel effects are allowed to vary randomly across test subjects, there shall be no correlation in these effects between enrolment and test sessions across all users.

The sampling plan shall ensure that the data collected are not dominated by a small group of excessively frequent, but unrepresentative users.

Great care shall be taken to prevent data entry errors and to document any unusual circumstances surrounding the collection. Keystroke entry on the part of both test subjects and test administrators should be minimized. Data could be corrupted by impostors or genuine users who intentionally misuse the system. Every effort shall be made by test personnel to discourage these activities; however, data shall not be removed from the corpus unless external validation of the misuse of the system is available.

Users are sometimes unable to give a usable sample to the system as determined by either the test administrator or the quality control module. Test personnel should record information on failure-to-acquire attempts where these would otherwise not be logged. The failure-to-acquire rate measures the proportion of such attempts, and is quality threshold dependent. As with enrolment, quality thresholds should be set in accordance with vendor advice.

Test data shall be added to the corpus regardless of whether or not it matches [a supported document] template. Some vendor software does not record a measure from an enrolled user unless it matches the […] template. Data collection under such conditions would be severely biased in the direction of underestimating false non-match error rates. If this is the case, non-match errors shall be recorded by hand. Data shall be excluded only for predetermined causes independent of comparison scores.

All attempts, including failures-to-acquire, shall be recorded. In addition to recording the raw image data if practical, details shall be kept of the quality measures for each sample if available and, in the case of online testing, the matching score or scores.

Collection from remote subjects for DocAuth testing is possible, with the following caveats:

1. Vendor SHALL specify acceptable biometric or document reading capture devices, e.g. cameras on smartphone and NFC reading capability on smartphone.

> NOTE: Capture devices SHOULD be readily available to a majority of potential remote subjects, e.g. camera on a smartphone, version X through Y, within last five years.

1. The laboratory SHALL uniquely register Test subjects and this SHALL include details of the device they will use to ensure capability.
2. FIDO accredited laboratory SHALL observe the collection, complete action being taken on capture device, throughout the session which SHALL be recorded for auditing purposes only, e.g. typically with web meeting and video recording being completed on a separate device.
3. The laboratory SHALL provide a mechanism to enable linking the subject with their results.

7.3.1.1. Pre-Verification

Before genuine transactions test subjects MAY perform practice transactions.

7.3.1.2. Genuine Document Authentication Transaction

Test subjects SHALL conduct five (5) genuine document authentication transactions per document type. Transactions SHALL be conducted in good faith and without test operator guidance. Any kind of guidance SHALL be provided by the document authentication system in a similar manner to the final application.

For Tier 5 documents that contain NFC security features, five genuine transactions SHALL be performed using the NFC functionality. For vendors that have specified optical review of Tier 5 documents five genuine transactions using the optical approach SHALL be performed after blocking the NFC functionality. The blocking mechanism SHALL not interfere with the optical capture capabilities of the device. If the TOE does not allow an optical fallback, then the second test is not required.

> NOTE: NFC can be blocked in a method chosen by the laboratory. For example, a thick case or cover can be used to block the NFC output from the capture device.

The document authentication process MAY be different depending on the TOE. This process MAY require multiple presentations. For testing purposes, this process SHALL NOT have more than five attempts for each transaction. A transaction SHOULD NOT exceed 30 seconds.

The authenticator vendor SHALL describe to the FIDO Accredited Laboratory what constitutes the start and end of a document authentication transaction.

7.3.1.3. Genuine Document Document Verification Errors

A failure to acquire SHALL be declared when the document authentication system is not able to capture a document image during a verification attempt (an FTA MAY happen per attempt). The test harness SHALL indicate to the FIDO Accredited Laboratory when a failure to acquire has occurred. A document false rejection error SHALL be declared when the document authentication fails to authenticate the document after document after test subjects execute the complete verification transaction (which includes no more than five attempts). If a failure to acquire occurs for all attempts, a document false rejection error SHALL be declared.

The manner in which the FIDO Accredited Laboratory records failure to acquire, false rejects, and true accepts are left to the FIDO Accredited Laboratory, but SHALL be done automatically to avoid introducing human error.

7.3.1.4. Document False False Reject Rate

Document False False Reject Rate SHALL be calculated according to requirements in section § 7.2.1 Size of Test Set.

Appendix A: References

References

Cross-Reference	Title	Link
[DL Formats]	National Traffic Safety Institute (NTSI) State Driver's License Formats	https://ntsi.com/drivers-license-format/
[ISO/IEC	ISO/IEC 19794-1:2011 Information technology -	https://www.iso.org/standard/50862.html

Cross-Reference	Title	Link
19794-1]	Biometric data interchange formats — Part 1: Framework	
[ISO/IEC-19795-2]	ISO/IEC 19795-2:2007 Information technology – Biometric performance testing and reporting – Part 2: Testing methodologies for technology and scenario evaluation	https://www.iso.org/standard/41448.html
[NIST 800-63-3]	NIST SP 800-63-3 NIST Digital Identity Guidelines	https://pages.nist.gov/800-63-3/sp800-63-3.html
[NIST 800-63A]	NIST SP 800-63A NIST Digital Identity Guidelines: Enrollment and Identity Proofing	https://pages.nist.gov/800-63-3/sp800-63a.html
[NIST IR 8173]	NIST IR 8173 NIST Interagency/Internal Report Face In Video Evaluation	https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8173.pdf
[RFC 2119]	Key words for use in RFCs to Indicate Requirement Levels. March 1997. Best Current Practice.	https://tools.ietf.org/html/rfc2119

Appendix B: Research Sources§

For more information on the various subjects outlined in this requirements document please refer to the table below which includes recommended research sources.

Research Sources

*Type *	Link
Identity Proofing	NIST Digital Identity Guidelines (800-63-3): [SP800-63-3], NIST 800-63 Rev3 (IAL standards): [SP800-63A]
Alternative Identity Proofing Standards	Australian Government ID Proofing Doc (great starting point for some of our work):https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/Trusted%20digital%20identity%20framework%202/Identity%20Proofing%20Requirements.pdf UK Government ID Proofing Guide: https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual
Identity Proofing Working Groups and Orgs	W3C Verifiable Claims Working Group: https://www.w3.org/2017/vc/charter.html OpenID Connect for Identity Assurance: https://openid.net/wg/ekyc-ida/

Appendix C: Program Documents§

This Appendix includes the other companion documents and webpages for the Document Authenticity Verification Certification Program.

Program Documents

Cross-Reference	Title	URL
[Accredited Laboratory List]	FIDO Accredited Document Authenticity Verification Laboratories	To be created (FIDO Website)
[DocAuth MDS Req]	Document Authenticity Verification Metadata Requirements	TBD
[FIDO Getting Started Webpage]	FIDO Getting Started Webpage	https://fidoalliance.org/getting-started/
[FIDO Implementer Dashboard]	FIDO Implementer Dashboard	https://fidoalliance.org/certification/implementer-dashboard/ Implementer Account Required
[FIDO Laboratory Dashboard]	FIDO Laboratory Dashboard	https://fidoalliance.org/certification/lab-dashboard/ Laboratory Account Required
[Policy]	Document Authenticity Verification Certification Policy	https://fidoalliance.org/specs/certification/docauth/docauth-lab-policy-v1.0-fd-20211021.html
[Requirements]	Document Authenticity Verification Requirements	(This document)
[Allowed Cryptography List]	FIDO Authenticator Allowed Cryptography List	https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-allowed-cryptography-list-v1.3-fd-20201102.html

Appendix D: Terms & Abbreviations§

For other terms not used in this document, but may be used in relation to FIDO, please refer to the [FIDOGlossary].

Terms & Abbreviations

Term / Abbreviation	Definition
BCC	Board Certification Committee
**Blur*	An image of an identity document or photo that is not clearly visible or are not sufficiently sharp.
Board Certification Committee	Board-level certification committee that resolves certification issues that relate specific Certification Requirements or other Certification program documents. See also Certification Issue Resolution Team
Certification Issue	Board-level certification committee that resolves certification issues that relate specific Certification Requirements or other Certification program documents. See also Board

Term / Abbreviation	Definition
Resolution Certification Committee	The FIDO working group responsible for the approval of policy documents and ongoing maintenance of policy documents once a certification program is active.
CWG	Certification Working Group
DocAuth	Document Authenticity Verification
DFAR	Document False Accept Rate
DFI	Document Fraud Instruments
DFI species	Class of document attack instruments created using a common production method and based on different persons.
DFRR	Document False Reject Rate
DFTA	Document Failure-To-Acquire rate
Document Authenticity Verification Secretariat	The FIDO Alliance expert responsible for the coordination and final approval of evaluation reports from FIDO Accredited Laboratories.
Document Failure-to-Acquire Rate	Proportion of document verification attempts for which the system fails to capture or locate an image or signal of sufficient quality.
Document False Accept Rate	The proportion of document verification transactions with document fraud that are incorrectly confirmed as authentic.
Document False Reject Rate	The proportion of genuine document verification transactions with truthful claims of an genuine document that are incorrectly denied.
Document Fraud Attack	The techniques used to create fraudulent documents. These can be digital or physical.
Document Fraud Instrument	Object or image used in a document attack (e.g. forgery or counterfeit).
Document Type	The classification of one identity document type to be assessed by the certification. This consists of document classification, origin country and origin domestic region (where applicable and subject to vendor request).
Document Liveness	A live document is the physical original document. Photocopies and scanned images of genuine documents are not considered as fraudulent documents or document tampering.
Document True Reject Rate	The proportion of document fraud correctly identified by the system.
Document Verification	Process by which the user submits an identity document and an accept or reject decision regarding the authenticity of the document.
Document	Sequence of attempts on the part of a user for the purposes of document verification.

Term / Transaction Abbreviation	Definition
Verification	See section 4.2.3 in [ISOIEC-19795-1].
DTRR	Document True Reject Rate
FER	FIDO Evaluation Report
FIAR	FIDO Impact Analysis Report
FIDO Accredited Laboratory	Party performing testing. Testing MUST be performed by third-party test laboratories Accredited by FIDO to perform Document Authenticity Verification testing.
FIDO Secretariat	The FIDO Alliance certification expert responsible for administration of the FIDO Certification programs, including finalizing certification requests, updating product listings, and issuing program certificates.
FIDO Member	A company or organization that has joined the FIDO Alliance through the membership process.
Fraudulent Document	A fabricated identity document or a tampered version of an existing document. These can be digital or physical documents.
FTA	Failure To Acquire
Genuine Document	The original version of an identity document in its physical form that has not fabricated or been tampered with.
Glare	A photo of a document where there is a reflection of a light source that hides useful information from the image.
Identity Verification and Binding Working Group	The Working Group responsible for defining the Document Authenticity Verification Requirements to develop the Document Authenticity Verification Certification program and to act as subject matter experts following the launch of the program.
IDWG	Identity Verification and Binding Working Group
MDS	Metadata Service
RP	Relying Party
Target of Evaluation	The product or system that is the subject of the evaluation. See the§ 4 TOE Description section in this document.
Target Population	Set of users of the application for which performance is being evaluated. See Section 4.3.4 in [ISOIEC-19795-1].
Test Crew	Set of test subjects gathered for an evaluation. See Section 4.3.3 in[ISOIEC-19795-1].
Test Operator	Individual with function in the actual system. See Section 4.3.6 in[ISOIEC-19795-1].
Test Subject	User whose biometric data is intended to be enrolled or compared as part of the evaluation. See Section 4.3.2 in [ISOIEC-19795-1].
TMLA	Trademark License Agreement
TOE	Target Of Evaluation
TOE Description	A description of the TOE provided by the vendor to the laboratory in advance of the certification.
Vendor	Party seeking certification.

Term / Abbreviation	Definition
MRZ	Machine Readable Zone
Counterfeit Documents	Any document attempting to reproduce a genuine document made outside of the issuing authority of the document.
Document Tampering	Digital or physical modifications made to a genuine identity document which renders that document materially different from the evidence of identity that the document was originally issued for.
Digital Tampering	Manipulation of the captured image of the document.
Physical Tampering	Physical alteration or reproduction of a document.
Vendor Tool	Tool provided by the vendor for use by the FIDO Accredited Laboratory to input the test samples in the defined formation and organization, perform the document authentication process, and deliver a result as specified.
Test Set	Set of genuine and fraudulent documents gathered for evaluation.

References§

Normative References§

[DA-CertPolicy]
Document Authenticity Certification Policy. 21 OCT 2021. Final Draft. URL: https://fidoalliance.org/specs/certification/docauth/docauth-lab-policy-v1.0-fd-20211021.html

[FIDOGlossary]
R. Lindemann; et al. *FIDO Technical Glossary*. 23 May 2022. Proposed Standard. URL: https://fidoalliance.org/specs/common-specs/fido-glossary-v2.1-ps-20220523.html

[ISO30107-1]
ISO/IEC JTC 1/SC 37 Information Technology - Biometrics - Presentation attack detection - Part 1: Framework. URL: http://www.iso.org/iso/catalogue_detail.htm?csnumber=53227

[ISOIEC-19795-1]
ISO/IEC 19795-1:2021 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework. 2021. URL: https://www.iso.org/standard/73515.html

[ISOIEC-19795-5]
ISO/IEC 19795-5:2011 Information technology -- Biometric performance testing and reporting -- Part 5: Access control scenario and grading scheme. 2011. URL: https://www.iso.org/standard/51768.html

[ISOIEC-30107-3]
ISO/IEC 30107-3:2017 Information technology — Biometric presentation attack detection — Part 3: Testing and reporting. 2017. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:30107:-3:ed-1:v1:en

Informative References§

[SP800-63-3]
P. Grassi; M. Garcia; J. Fenton. *NIST Special Publication 800-63-3: Digital Identity Guidelines* June 2017. URL: https://doi.org/10.6028/NIST.SP.800-63-3

[SP800-63A]
P. Grassi; et al. *NIST Special Publication 800-63A: Digital Identity Guidelines - Enrollment and Identity Proofing Requirements*. June 2017. URL: https://doi.org/10.6028/NIST.SP.800-63a