Document Authenticity Certification Policy

Final Document, October 21, 2021

This version:
https://fidoalliance.org/specs/certification/docauth/docauth-lab-policy-v1.0-fd-20211021.html

Issue Tracking:
GitHub

Editor:
Certification Working Group (CWG) (FIDO Alliance)

Abstract

This document outlines the Policies and Procedures for the DocAuth Certification program.

Table of Contents

1. Revision History§

Revision History

Date	Version	Description	Sunset Date
16 November 2021	1.0	Initial Release and Document Approval	-

2. Introduction§

This document gives an overview of the policies that govern Document Authenticity (DocAuth) Certification as part of the DocAuth Certification Program. FIDO administers other Certification programs, and each has their own policy and requirements documents.

The policies contained herein are the requirements and operational rules that guide the administration, process, and ongoing operation of the DocAuth Certification program and dictates the overall framework for the DocAuth Certification Program to operate within.

Vendors seeking DocAuth Certification may be FIDO members, or non-member organizations.

All vendors SHALL follow the policy outlined in this document when completing the FIDO DocAuth Certification process.

2.1. Audience§

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

The policies herein apply to Vendors and Laboratories that are undergoing or part of FIDO DocAuth Certification.

The owner of this document is the Certification Working Group.

The FIDO Certification Webpage will reflect the information in this document and is intended to help Vendors understand the process for receiving certification and the policies surrounding FIDO DocAuth Certification. This document is the complete policy for this program, while the website may act as an introduction.

2.2. Support§

For help and support, contact the FIDO Certification Secretariat atcertification@fidoalliance.org.

2.3. Roles & Responsibilities§

The FIDO DocAuth Certification Program as a whole is the responsibility of the FIDO Certification Working Group (CWG) in partnership with the Identity Verification and Binding Working Group (IDWG), with necessary oversight and approvals from the FIDO Board, and collaboration with other FIDO Working Groups where needed.

The CWG and IDWG MAY, at the discretion of its chair and members, create subcommittees and delegate responsibilities for all or some portion of FIDO Certification Program responsibilities to those subcommittees.

The **Certification Working Group (CWG)** is the FIDO working group responsible for the approval of policy documents and ongoing maintenance of policy documents once a certification program is active.

The **Identity Verification and Binding Working Group** is the Working Group responsible for defining the DocAuth Requirements to develop the DocAuth Certification program and to act as subject matter experts following the launch of the program.

The **Vendor** party seeking certification. Responsible for providing the implementation to the FIDO Accredited Document Authentication (DocAuth) Laboratory for testing.

The **Certification Troubleshooting Team** is an ad-hoc CWG-appointed team consisting of FIDO staff and members common to all FIDO Certification Programs to diagnose, dispatch, and resolve policy and operational issues as they arise.

FIDO Accredited Laboratories are Testing Laboratories that have successfully completed the FIDO Laboratory Accreditation Program, and are found on the FIDO Accredited DocAuth Laboratories list. The FIDO Accredited Laboratory is the party performing testing. FIDO Laboratory Accreditation is specialized to each certification program. Testing MUST be performed by third-party test laboratories Accredited by FIDO to perform DocAuth testing.

DocAuth Secretariat is the FIDO Alliance expert responsible for the coordination and final approval of evaluation reports from FIDO Accredited Laboratories.

FIDO Certification Secretariat is the FIDO Alliance certification expert responsible for administration of the FIDO Certification Programs, including finalizing certification requests, updating product listings, and issuing

program certificates. For any questions related to this document or the FIDO Certification programs, please contact the FIDO Certification Secretariat at certification@fidoalliance.org.

FIDO member is a company or organization that has joined the FIDO Alliance through the Membership process.

2.4. 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 [RFC2119].

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

3. Program Documents§

This section outlines and defines the documents that govern the DocAuth Certification Program.

3.1. Certification Policy§

The DocAuth Certification Policy is the governing document for the DocAuth Certification Program. The Policy document outlines the process vendors must complete in order to receive and maintain DocAuth Certification for their implementation.

3.2. Laboratory Accreditation Policy§

The DocAuth Laboratory Accreditation Policy provides guidance on the requirements for a laboratory to become accredited to perform testing for the DocAuth Certification Program [DA-LabAccreditationPolicy].

3.3. Requirements§

The DocAuth Requirements document outlines the requirements the implementation must meet in order to achieve DocAuth Certification. It includes the test procedures and additional information on document authenticity verification. Vendors and FIDO Accredited Laboratories will use these requirements when preparing for and completing the FIDO Identity DocAuth Certification [DA-Requirements].

4. Certification Process§

The goal of the DocAuth Certification Process is to determine if a document is authentic, the implementation seeking certification will be herein referred to as the TOE (Target of Evaluation). Please see the Identity DocAuth Requirements [DA-Requirements] for the specific requirements and test procedures for this program.

FIDO DocAuth Certification is independent of other FIDO Certification Programs. There are no FIDO Certification prerequisites to apply for DocAuth Certification.

4.1. Process Overview§

A FIDO Implementation seeking DocAuth Certification must complete the following steps and meet the requirements in order to receive DocAuth Certification. The steps are as follows:

Preparation

- The vendor seeking certification should review and come to understand all requirements and testing procedures [DA-Requirements]. The vendor should also begin discussions with a FIDO Accredited Laboratory associated with this program, FIDO Accredited DocAuth Laboratories.
- Prepares the Target of Evaluation (TOE) Description using theIDV DA Test Plan TOE Description Template.

Application

- The vendor completes the application to start FIDO Certification process and provides a TOE Description.
- The vendor enters a contract with aFIDO Accredited DocAuth Laboratory.
- The Certification Secretariat reviews the Application, and notifies the Vendor that it is Approved, Rejected, or requires clarification. If Approved, the Vendor can proceed to the pre-testing and testing phase.

Pre-Testing and Testing

- The vendor provides the following to the FIDO Accredited DocAuth Laboratory:
  - TOE Description
  - Test Plans
  - Other information as specified in the DocAuth Requirements[DA-Requirements].
- The FIDO Accredited DocAuth Laboratory will be responsible for testing against the requirements for both Digital and Physical Document testing. Testing will be completed according to the DocAuth Requirements [DA-Requirements].
  - Labs seeking FIDO Accreditation SHALL follow the DocAuth Laboratory Accreditation Policy[DA-LabAccreditationPolicy]. A list of FIDO Accredited DocAuth Laboratories will be available on the FIDO Website, FIDO Accredited DocAuth Laboratories.
- The FIDO Accredited DocAuth Laboratory SHALL prepare a test plan and submit the concept to the FIDO Certification Secretariat for approval before starting any testing. The test concept shall follow the structure as provided in IDV DA Test Plan TOE Description Template.
- Data collected from Test Subjects SHALL be maintained in a secure manner by the Accredited Laboratory. Biometric data MAY be provided to Vendor under an agreement between the Vendor and the Test Laboratory, pursuant to laws of the jurisdiction(s) of the parties. Aside from the Vendor, the Accredited Laboratory SHALL NOT provide the biometric data to any other third parties or FIDO, except as needed for purposes of an audit of the Accredited Laboratory by FIDO.
- The Accredited Laboratory SHALL only collect data that relates specifically to the Requirements for Testing under this program.
- The Accredited Laboratory SHALL retain testing data under this FIDO Certification Program for at least one (1) year.

Laboratory Report

- Accredited Laboratory performs testing and returns Laboratory Report to Vendor and DocAuth Secretariat.
- DocAuth Secretariat reviews the Laboratory Report and makes a decision to Approve, Reject, or ask for clarification.

Certification Request

- If Laboratory Report is Approved, Vendor completes a Certification Request to describe the Certified Product and be added to the product listing page.

- The Vendor signs the TMLA if they wish to use the Certification Mark or FIDO Logo.

Certification Issuance

- FIDO Reviews and, if complete, Approves the Certification Request and issues an DocAuth Certificate.

4.1.1. Step-by-Step Process§

The FIDO Certification Steps Table summarizes the step-by-step process to complete FIDO DocAuth Certification.

FIDO Certification Steps

Process Step	Responsible Party	Process Steps
Preparation	Vendor	Develops implementation according to the program requirements.
	Accredited Laboratory	Vendor contacts and hires a FIDO Accredited Laboratory.
Application	Vendor	Submits FIDO Certification Application to FIDO Certification Secretariat. Completes the Vendor NDA and submits to FIDO Certification Secretariat.
	FIDO Certification Secretariat	Reviews and approves the Application based on readiness to begin the certification process. Signs FIDO portion of the Vendor NDA and returns to the Vendor.
Pre-Testing and Testing	Vendor	Notifies the selected FIDO Accredited Security Laboratory that the Application meets FIDO's criteria and enters a contract with the Laboratory.
	Accredited Laboratory	Develops a test plan and provides it to the FIDO DocAuth Secretariat for approval.
	Accredited Laboratory	Executes the test procedures as outlined in the DocAuth Requirements. Completes FIDO Evaluation Report and submits to Vendor and FIDO DocAuth Secretariat.
	FIDO DocAuth Secretariat	Reviews the FIDO Evaluation Report and • Approves • Rejects, or • Requests Clarification When a decision is made, returns the FIDO Evaluation Report to the Accredited Laboratory and the Vendor.
Certification Issuance	Vendor	When Laboratory Report is Approved, completes a Certification Request, including: • Approved FIDO Evaluation Report • Optionally signs FIDO Trademark License Agreement and/or a Certification Announcement with FIDO Marketing.
	FIDO Certification Secretariat	Reviews the Certification Request, and if complete, issues a Certificate. Updates Certified Products on FIDO website to reflect the Certification.

4.2. Application§

To begin FIDO Certification, the Vendor completes the Certification Application [Application].

The Application is available on the program webpage.

As part of the application, the vendor SHALL provide a TOE Description to the Accredited Laboratory and to FIDO. This TOE Description is intended to cover all relevant aspects of the Target of Evaluation (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 applying for certification. A template for the TOE Description will be available on the program webpage.

The FIDO Certification Secretariat is responsible for reviewing and approving the Certification Application and, if approved as complete, returning it to the Vendor.

4.3. Pre-testing and Testing§

All pre-testing and testing activities SHALL be executed by a FIDO Accredited Laboratory in accordance with the requirements and test procedures specified in the DocAuth Requirements [DA-Requirements].

4.4. Evaluation Report§

The FIDO Accredited Laboratory completing the evaluation will execute a FIDO Evaluation Report based upon their testing and evaluation of the product and submit to the Vendor and the DocAuth Secretariat. The report will identify the labs final assessment of the product by indicating pass, fail, or additional details needed. The DocAuth Secretariat will make the decision to Approve, Reject, or ask for clarification on the FIDO Evaluation Report. The decision will be communicated to the Vendor and the Laboratory.

4.5. Certification Issuance§

If the Laboratory Report is Approved, the Vendor completes a Certification Request via the certification program webpage.

4.5.1. Requests§

When submitting for DocAuth Certification, Vendors must:

1. Have passed testing requirements.
2. If a member of FIDO, be in good standing with all dues and invoices paid in full.
3. Be willing to adhere to all policies.

In order to receive DocAuth Certification, Vendors must submit the following for each implementation being certified:

1. Completed FIDO Evaluation Report
2. Certification Fees

OPTIONALLY, Vendors can submit the following along with their Certification Request:

- Signed FIDO Trademark License Agreement
- Request for a Certification Announcement jointly with or by the FIDO Marketing Team.

If it is found that reports or other documentation has been falsified; if implementations have been modified, or if

any other policy is violated, intentionally or unintentionally, the violations are subject to review by FIDO Board of Directors. The Board of Directors may choose a suitable recourse, ranging from requiring that an implementation go through the Certification Process again to become certified to revoking FIDO membership and / or previous certifications, depending on the severity of the transgression.

The FIDO Certification Secretariat will be responsible for verifying all submitted documentation as well as:

1. Ensuring that all disputes have been resolved and that the resolutions do not prevent the certification of the implementation
2. Noting any changes in specifications or process that would impact the ability to certify the implementation

Turn-around time for certification will be as soon as reasonably possible and no more than 30 days from the Vendor's submission of final documentation to FIDO. There are four possible outcomes to certification; Approval, Rejection, Delay, and Failure. The outcomes are described in more detail in the Certificate Request Actions Table.

Certificate Request Actions

Outcome	Description
Approval	The Vendor's Certification request is Approved and the implementation is certified. Approval will only be granted if the implementation has all the required documentation. Upon approval, the certified implementation will be registered in the certification database and the Vendor will be notified by email. Notification will include a certification number for future reference.
Rejection	Rejection may occur if any document is missing or invalid; or if any other condition exists that would prevent certification. If a certification request is rejected, the Vendor will be notified by email with the corresponding reason(s) for rejection and will have the opportunity to resubmit. The FIDO Certification Secretariat will make every reasonable attempt to ensure that all errors in a submission are identified so that they can be addressed in parallel, rather than sequentially. An implementation may be resubmitted three times before it is considered a failed certification attempt, and the implementation would need to be resubmitted and certification fees paid again.
Delay	The request has been delayed beyond the typical 30-day certification window because of pending events (e.g. a dispute that is still pending resolution).
Failure	The request was rejected because the request was inappropriate or impossible and it would be inappropriate to resubmit.

Should a certification request be rejected, delayed, or failed, the submitting Vendor will have the right to submit a Dispute Resolution Request, which will follow the Dispute Resolution Process described in Dispute Resolution Process.

4.5.2. Certification Issuance§

When a Certificate is issued, it will contain the following information:

- The name of the organization that has been certified
- The name of the implementation that has been certified
- Certification Program (i.e., DocAuth)
- Document type claimed – detailed list of documents (i.e., New York DL, etc.)
- Documents tested – a subset of the claimed list
- Threshold numbers
- The Certification Program Policy version the product was certified against
- The FIDO Requirements version the product was certified against

- The document types tested (documents supported that the vendor claims were tested)
- The date that FIDO Evaluation Report was approved
- The Accredited Laboratory that performed the evaluation
- A certification number of the format FFFVVVV-SSSS-DDDDDDDDNNN where:
    - FFF is the abbreviation of the FIDO Certification Program (i.e., DocAuth)
    - VVVV is the version of FIDO specification
    - Threshold numbers
    - RRRR is the version of the DocAuth Requirements
    - DDDDDDDD is the date of issuance (year, month, day)
    - NNN is the sequential number of certifications issued that day

FIDO Certified Products will be viewable and searchable by FIDO membership and the public-at-large, with the exception of certifications that are confidential (see Confidential).

5. Certification Maintenance and Updates§

Over time, changes to the Certified implementation MAY occur, and those changes MAY affect the FIDO DocAuth Requirements. FIDO MUST be notified of any changes to a Certified implementation. These changes can be categorized as non-interfering, minor, and major. The categorization of the change will determine whether the implementation requires a Derivative, Delta, or a new Certification.

5.1. Impact Analysis Report (FIAR)§

Vendors are REQUIRED to disclose any changes to a Certified implementation to FIDO by completing a FIDO Impact Analysis Report. The Vendor MUST describe all the changes made to the implementation in order to determine their impact on the DocAuth Requirements.

The FIAR review process is composed of four steps:

1. **Submission**: The Vendor completes the FIAR document based on the FIAR Template and submits it to the FIDO Certification Secretariat via the FIDO Implementer Dashboard.
2. **Review**: The FIDO Certification Secretariat reviews the submitted FIAR for completeness and analyses the changes to determine their impact on the DocAuth Requirements.
3. **Conclusion**: The FIDO Certification Secretariat will provide judgement based on the characteristics of the changes made to the Certified implementation. The conclusion will indicate that the changes are either: Non-interfering, Minor, or Major.
4. **Certification**: Non-interfering changes MAY complete the Derivative Certification Process, Minor changes MAY complete the Delta Certification process, and Major changes MAY start the certification process over with the implementation as a new certification.

5.1.1. Types of Changes§

Post-certification changes can be categorized into three types, and the type of change dictates the next steps for the vendor in the Certification process.

Non-Interfering Change

A non-interfering change has no impacts on the DocAuth Requirements coverage. Typical changes that would be categorized as a non-interfering change are bug fixes related to functional features, performance optimization, or

an updated name or look. A Vendor with changes that the Certification Secretariat determines are non-interfering MAY follow the Derivative Certification process.

Minor Change

A minor change has an impact that is sufficiently minimal but requires the implementation to be re-certified. Typical changes that would be categorized as a minor change are bug fixes indirectly related to the items tested within the DocAuth Requirements, or a security strength optimization. A vendor with changes that the Certification Secretariat determines are minor MAY follow the follow the Delta Certification process.

Major Change

A major change has an impact on one or more of the DocAuth Requirements. Typical changes could be a change to the cryptographic algorithm, or a change to the security architecture. In some cases, an update that includes several minor changes could lead to a major impact on the DocAuth Requirements, thereby leading the Certification Secretariat to classify it as a major change. A Vendor with changes that the Certification Secretariat determines are major changes MUST complete a new Certification (i.e. start the Certification process over with the changed implementation as the TOE).

5.2. Derivative Certification§

Derivative Certification is possible when a new implementation has been created based off of a Certified implementation and the Vendor wishes to re-use the original Certification for this new implementation because there have been **no changes** to the Certified functionality. The intent of the Derivative Certification process is to reduce the burden for receiving certification for implementations that are substantially the same.

A Derivative implementation SHALL NOT modify, expand, or remove functionality tested in the FIDO DocAuth Certification process. Derivative implementations are bound to the DocAuth Policy at the time of the original (base) certification. Derivatives will be issued their own Certification and can be listed as a separate product.

Derivative Certification requires an assertion from the Vendor that the Derivative implementation does not modify, expand, or remove functionality that was tested during the original certification. This assertion is reviewed and approved by the Certification Secretariat as part of the Derivative Certification Request.

5.3. Delta Certification§

Delta Certification is when the Vendor has made changes to the original certified implementation and the Vendor wishes for that implementation to remain certified. The Certification Secretariat will work with the Vendor and original FIDO Accredited Laboratory to determine an appropriate Test Plan based on the changes made to the implementation to complete the Delta Certification Requirements. This will be done on a case-by-case basis due to the variety of changes that may be made to an implementation.

Once a Delta Test Plan has been approved by the Certification Secretariat, the Vendor and Accredited Laboratory will follow the certification process to apply for Delta Certification and complete testing according to the Delta Test Plan.

6. Program Administration§

The CWG will be responsible for maintaining these policies and will have the authority to change them as they see fit. The CWG should take care, to any extent possible, to ensure that any revisions to these policies fall within the current statement of work between the FIDO Certification Secretariat and FIDO Alliance; or that the statement of work be amended as appropriate.

6.1. Sensitive Information§

The FIDO DocAuth Secretariat and FIDO Certification Secretariat are responsible for protecting sensitive information during transit and storage.

When submitting electronic documentation to FIDO, it must be PGP encrypted and securely uploaded using forms on the FIDO website. All FIDO Certification forms, Evaluation Reports, and their attachments will be stored within an encrypted database only accessible by the Certification Secretariat and will not be shared.

Unless a previous agreement has been made between the FIDO Certification Secretariat and the Vendor or Laboratory, all documents sent via email will not be reviewed and will be deleted.

Data captured from Test Subjects SHALL be maintained in a secure manner by the Accredited DocAuth Laboratory. Personal data MAY be provided to Vendor under an agreement between the Vendor and Test Laboratory, pursuant to laws of the jurisdiction(s) of the parties. Aside from the Vendor, the Accredited Laboratory SHALL NOT provide test data to any other third parties or FIDO, except as needed for purposes of an audit of the Accredited Laboratory by FIDO. Additional logical security requirements are provided in the Logical Security section of the FIDO DocAuth Laboratory Accreditation Policy [DA-LabAccreditationPolicy].

6.2. Certification States§

No Vendor, Accredited Laboratory, nor other third-party may refer to a product, service, or facility as FIDO approved, accredited, certified, nor otherwise state or imply that FIDO (or any agent of FIDO) has in whole or part approved, accredited, or certified a Vendor, Laboratory, or other third-party of its products, services, or facilities, except to the extent and subject to the terms, conditions, and restrictions expressly set forth within the certificate issued by FIDO.

A list of Certified products will be maintained by the FIDO Certification Secretariat and a public list will be available on FIDO Website, FIDO Certified Products. Certification may be in the following states: Active, Confidential, Certified, Suspended, or Revoked.

6.2.1. Active§

Once an application is submitted to FIDO, the Certification state becomes “Active”. Active applies to initial Certification and Delta Certification.

This state is not shared outside of the FIDO Certification Secretariat and the FIDO Accredited Laboratory chosen by the Vendor.

6.2.1.1. Confidential§

Confidential Certification is allowed for companies that wish to complete FIDO Certification process confidentially. Vendors can request their certification remain confidential when applying for Certification.

During a Confidential Certification, only FIDO Certification Secretariat, FIDO DocAuth Secretariat and FIDO Executive Directors have any knowledge of the existence or details of the product. Any Accredited Laboratory involved in certification will also have knowledge of the product. FIDO Working Groups and FIDO Board of Directors will not have knowledge of the product until Confidentiality is withdrawn. The Certificate will not be announced and will not appear on FIDO Website until Confidentiality is withdrawn.

Confidentiality may be withdrawn at the request of the Vendor by submitting a written request to the FIDO Certification Secretariat with the corresponding certification number. The FIDO Certification Secretariat will contact Vendors of confidential certifications once every three months to verify that certifications should retain the confidential status.

The requirements for an implementation to pass Confidential Certification are the same as for any other implementation.

6.2.2. Certified§

An implementation with a “Certified” status is one that has been issued a Certificate and is in good standing.

Certified implementations will be listed on the FIDO Certified Products list, unless the Certification was completed as a Confidential Certification.

6.2.3. Suspended§

A Certificate may be suspended, for more information on the Suspension process, see Certification Suspension.

6.2.4. Revoked§

A Certificate may be revoked, for more information on Revocation, see Revocation.

6.3. Certification Suspension§

A certification MAY be suspended by the FIDO Certification Secretariat.

In the event that the Certification Secretariat becomes aware of a suspension event, the Certification Secretariat will investigate the claim to determine if the event is cause for Suspension.

The Certification Secretariat will determine if:

- No further action is required and the certification will remain “Active.”
- A Delta Certification is required to verify the implementation still meets the DocAuth Requirements.

Vendors will be given at least 30-day notice prior to updating the certification from Active to Suspended, along with the necessary steps to prevent and/or remove the Suspension.

Any implementations completing Delta Certification will automatically be changed from “Active” to “Suspended” upon approval of the Delta Certification Request.

The suspended status will not be publicly shared, but the implementation will be removed from the FIDO Certified Products list while the Certificate status is Suspended.

If a certificate remains in the Suspended state for more than 180 days it MAY be revoked.

6.4. Certification Revocation§

A Certificate may be revoked by the FIDO Certification Secretariat.

In the event that the Certification Secretariat becomes aware of a revocation event, the Certification Secretariat will investigate the claim to determine if the event is cause for Revocation.

The Certification Secretariat will determine if:

- The Certificate has expired, and can therefore be revoked and removed from the FIDO Certified Products list.
- The Certificate has remained in a Suspended status for more than 180 days and is therefore eligible for revocation.

Revocation is an indication that the Certificate is no longer certified and must undergo a New Certification to be Certified.

The Certification Secretariat will provide 30-day notice prior to updating the Certificate status to Revoked.

If not already completed due to a Suspension, any Revoked Certificates will be removed from the FIDO Certified Products list.

6.5. Publication and Disclosure of Certification Status

This section outlines how and what a Vendor can say about their FIDO Certified product.

6.5.1. Trademark and Licensing Agreements

6.5.1.1. Usage

Certified implementations are invited and encouraged to use FIDO® Certified mark and logo to promote their products conformance with FIDO Certification Program. These certification marks are reserved for FIDO Certified products to enable quick identification of products that are exemplars of FIDO values: stronger, simpler, authentication.

FIDO Certification Mark(s) may only be used in conjunction with products that have the approved corresponding certification, and where the Vendor has executed FIDO Trademark License Agreement. As mentioned previously, the certification mark cannot be used in conjunction with a product that is certified under Confidential Certification until after the confidential certification has been withdrawn.

6.5.1.2. Violation Reporting

In the event that the FIDO Certified mark is being misused, a report can be filed by completing the FIDO Certification Logo Violation Form and submitting a URL and a photo of the misuse of FIDO Certified logo.

6.5.1.3. Enforcement

The FIDO Certification Secretariat will be responsible for a monthly review of certification mark usage and usage of FIDO® Certified terminology to ensure that usage is compliant with the TMLA. This review will use online search engines or other methods to find usage of certification marks, whence the FIDO Certification Secretariat will ensure that the mark usage is appropriate and that the corresponding products has indeed been certified for the claimed functionality. Should a certification mark violation be found, it will be referred to the Board of Directors.

Reasonable attempts will be made to contact any party that is using the certification mark outside of policy or the TMLA. If the party contacted is a FIDO member and they disagree with the assessment that the certification mark is being used in a way that violates FIDO Certification Program Policy or DocAuth Certification Policy, they will have the right to submit a FIDO Dispute Report that will follow the Dispute Resolution Process (Section 4.6.1).

6.6. Product Documentation

Only implementations that have a FIDO Certificate can claim to be a FIDO® Certified product. This includes, but is not limited to, within data sheets, marketing materials, websites, and product packaging.

6.6.1. Guidelines§

All documentation referencing FIDO DocAuth Certification should include the following, and match the information listed on the Certificate issued by FIDO:

- Date of DocAuth Certification
- Version of the Requirements
- Version of the DocAuth Certification Policy

6.6.2. Violation Reporting§

In the event that a reference to FIDO® Certified or FIDO® Certified Product is being misused, a report can be filed by contacting FIDO Certification Secretariat.

6.6.3. Enforcement§

The FIDO Certification Secretariat will be responsible for a monthly review of the usage of FIDO® Certified terminology to ensure that usage is compliant with these guidelines.

Reasonable attempts will be made to contact any party that is using the certification terminology in an unapproved fashion. If the party contacted is a FIDO member and they disagree with the assessment that the certification mark is being used in a way that violates policy, they will have the right to submit a Dispute Report that will follow the Dispute Resolution Process. Should a violation be found, and no action is taken after reasonable attempts to contact the vendor, it will be referred to the Certification Working Group (CWG).

6.7. Requirements Versioning§

Every certification issued by FIDO Alliance must be against an Active Version of the DocAuth Requirements. Version history, including the Active Version(s) and their descriptions, will be maintained on FIDO Website.

The Document Hierarchy dictates that Version of the Document Authenticity Verification Requirements (including the Test Procedures), as the lowest level, will always be updated. Therefore, it is the revision of the Version of the DocAuth Requirements that will trigger the following versioning process.

6.7.1. DocAuth Requirements§

DocAuth Requirements refers to the document that outlines the requirements for FIDO DocAuth Certification. This document includes:

1. Requirements
2. Test Procedures

6.7.2. Active Version(s)§

The Active Version(s) of the DocAuth Requirements refers to a version or versions that are currently published and will be accepted for Certification. A new version of the DocAuth Requirements is published and available for certification on an Evaluation Availability Date specific to that version. After this date the version becomes Active, and there will be a Transition Period where the previous version of the DocAuth Requirements are being phased out to a Sunset Date. A version is no longer considered Active once the Sunset Date has passed.

The example below in the Example Active and Sunset Date Table is a scenario for a Version 2.0 release. In this scenario, the DocAuth Requirements Version 2.0 has an Evaluation Availability date of June 1, 2023. The Sunset

Date for Version 1.0 is then assigned to be one year from that date, June 1, 2024. A vendor wishing to complete Certification between June 1, 2023 and June 1, 2024 has the option to apply for Certification against the two versions of the DocAuth Requirements that are active, 1.0 and 2.0. This is considered the transition period for Version 1.0. On June 2, 2024, the only Active Version will be 2.0. Once the Sunset Date for Version 1.0 has passed, the vendor must comply with the Version 2.0 DocAuth Requirements for any new or Delta Certifications.

Example Active and Sunset Date

Requirements Version	Evaluation Availability Date	Sunset Date
2.0	June 1, 2023	-
1.0	January 1, 2022	June 1, 2024

6.7.2.1. Evaluation Availability Date

DocAuth Requirements will be assigned an Evaluation Availability Date that is equivalent to the first day the version is available for DocAuth evaluation. The Evaluation Availability Date is the date at which the version becomes an Active Version.

DocAuth Requirements MUST include a Version Release Statement to document the requirements that have changed from the previous version.

6.7.2.2. Transition Period

DocAuth Certification is associated with a particular version of the DocAuth Requirements. When a new version of the DocAuth Requirements is available for evaluation (i.e., is an Active Version), the previous version will enter a Transition Period where it is available for Certification only up to an assigned Sunset Date.

6.7.2.3. Sunset Date

A Sunset Date is the date at which a version of the DocAuth Requirements is no longer an Active Version accepted for Certification. New and Delta Certifications can only be made against an Active Version of DocAuth Requirements [DA-Requirements].

The Sunset Date is not an indication that a certified DocAuth implementation becomes untrustworthy on this date. It only means that the DocAuth Requirements have been updated, and the Active version(s) is required for Certification. DocAuth Requirements are updated when new requirements or test procedures enter the ecosystem. Test procedures may also be updated to improve testing techniques.

When changes are made to the DocAuth Requirements it must be determined how quickly these should be implemented for all evaluations. The scope and type of changes are used to determine the Sunset Date for previous versions.

There are three classifications of changes which allow to gauge the time period which should be assigned for the Sunset Date: Major changes, Minor changes, and Emergency changes.

Major changes would generally be noted by a change in the major version number for the Procedures. The expectation of a major change version would include a change to Requirements and/or Test Procedure(s). Major changes will be assigned a Sunset Date of 1 year to the previous version of the DocAuth Requirements.

Minor changes would generally be noted by a change in the minor version number for the Procedures. The expectation of a minor change would be clarifications to the procedures, but which do not impact the government-issued identity document and validation functionality. Minor changes will be assigned a Sunset Date of 6 months to the previous version of the DocAuth Requirements.

Emergency changes would generally be only done under extreme circumstances such as a widespread threat that has an immediate impact on FIDO clients. When such a scenario occurs that requires changes to the DocAuth Requirements, an immediate Sunset Date for previous versions would be assigned. Due to the extreme nature of the Sunset Date, changes required through an Emergency Sunset must be limited specifically to those needed to ensure the meet the requirements defined by the emergency; no other changes are allowed to be included. Implementations certified against a version of the Requirements that is issued an Emergency Sunset MUST complete a Delta Certification to update their implementations and maintain certification.

6.7.2.3.1. Sunset Dates and Products Already Under Evaluation§

It is important to note that any implementation with an application that has been approved by the FIDO Certification Secretariat prior to the Sunset Date will be allowed to complete the evaluation, for Major or Minor Sunset Dates. For Emergency Sunset Dates, even products under evaluation will be required to comply with the changes included in the new version with the Emergency Sunset Date.

6.7.2.3.2. Sunset Date Voting§

The Sunset Date for an DocAuth Requirements version will be recommended by the FIDO DocAuth Secretariat and approved by a majority vote of the CWG. The Sunset Date is assigned when a new version of the Requirements becomes Active.

6.8. Resolving Conflict§

There may be cases where a vendor disagrees with a decision or results from the certification process. The Organization for Internet Safety guidelines includes recommendations on how to resolve such conflicts in the context of an organization's published vulnerability disclosure process [[ISO-29147:2018]].

In summary:

- Leave the process only after exhausting reasonable efforts to resolve the disagreement;
- Leave the process only after providing notice to the other party;
- Resume the process once the disagreement is resolved.

If the certification is rejected, failed, or delayed, the Vendor will have the option of submitting a FIDO Dispute Report.

6.8.1. Dispute Resolution Process§

In the event a vendor disputes the results of the FIDO DocAuth Secretariat, a FIDO Dispute Report is submitted to the FIDO Certification Secretariat via FIDO website. Upon receipt of a Dispute Report, the FIDO Certification Secretariat forwards the Dispute Report to the Certification Troubleshooting Team. The Certification Troubleshooting Team is responsible for determining the validity of the request and the appropriate routing of the request. The FIDO Certification Secretariat notifies the Certification Working Group of all Dispute Reports and their resolution.

If the certification has outstanding disputes or other issues, the certification may be delayed. Should the certification be delayed, the Vendor must be notified.

6.9. Program Management§

In order to provide continuity of operations between the FIDO Certification Secretariat and FIDO Alliance, the FIDO Certification Secretariat will attend CWG meetings and any joint meetings or other meeting where topics around certification are on the agenda. The FIDO Certification Secretariat will not have voting rights, but may participate in conversation and deliberations. Meeting notes, scheduling, logistics and other aspects of FIDO CWG meetings will be arranged in the same manner as other Working Groups and not by the FIDO Certification Secretariat.

In order to provide transparency and ensure appropriate managerial oversight, the FIDO Certification Secretariat will report to the CWG and / or the Board of Directors at each plenary meeting or as requested. Operational reports will include:

- the number of certification requests,
- the number of certifications granted,
- a breakdown of the implementation types that have been certified,
- a report of any disputes and their resolutions,
- any process updates,
- certification mark or TMLA violations,
- any other notable events or operational metrics.

Any reporting performed by the FIDO Certification Secretariat will be performed at the aggregate level to preserve confidentiality and will not include the specific name or details of any implementation or small set of implementations.

7. Liability§

FIDO performs Certification on a best-effort basis and does not guarantee or provide any warranties for any product provider's products, and the Certification process does not relieve vendors from the need to make their own investigations to ensure the security or fitness or purpose of any products.

FIDO Alliance will NOT take any liability or enter into any contract with a Relying Party where it takes legal or financial responsibility for losses due to a successful attack on a certified product. This is true for all types of and levels of certification that FIDO Alliance issues.

Appendix A: Program Documents§

Program Documents

Title	**Location**
DocAuth Certification Application	FIDO DocAuth Certification Program webpage
Certification Request	FIDO DocAuth Certification Program webpage
FIDO Certified Products	FIDO Website: FIDO Certified
Dispute Report	FIDO DocAuth Certification Program webpage
FIDO Evaluation Report (FER) prepared by the FIDO Accredited Laboratory	
FIDO Certification Overview	FIDO Website: Certification Overview
FIDO DocAuth Laboratory Accreditation Program Policy	FIDO DocAuth Certification Program webpage
FIDO Certified Logo Violation Form	FIDO Website: Certified Logo Violation

Document Authenticity Verification Certification Policy	FIDO DocAuth Certification Program webpage
Document Authenticity Verification Requirements	FIDO DocAuth Certification Program webpage
IDV DA Test Plan TOE Description Template prepared by the FIDO Accredited Laboratory	FIDO DocAuth Certification Program webpage
FIDO Alliance Trademark License Agreement	FIDO Website: Mark Usage
FIDO Trademark and Service Mark Usage Agreement for Websites	FIDO Website: TMLA for Websites

Appendix B: Terms & Abbreviations§

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

Terms & Abbreviations

Term / Abbreviation	**Definition**
Certification Issue Resolution Team	Board-level certification committee that resolves certification issues that relate specific Certification Requirements or other Certification program documents. See also Certification Working Group (CWG).
Certification Working Group	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	DocAuth
DocAuth Secretariat	The FIDO Alliance expert responsible for the coordination and final approval of evaluation reports from FIDO Accredited Laboratories.
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 Certification 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.
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
RP	Relying Party
TMLA	Trademark License Agreement
TOE	Target Of Evaluation
Vendor	Party seeking certification

References§

Normative References§

[DA-Requirements]

Document Authenticity Verification Requirements. 15 AUG 2022. Final Draft. URL: https://fidoalliance.org/specs/idv/docauth/document-authenticity-verification-requirements-v1.0-fd-20220815.html

[RFC2119]
S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. March 1997. Best Current Practice. URL: https://tools.ietf.org/html/rfc2119

Informative References§

[DA-LabAccreditationPolicy]
Document Authenticity Laboratory Accreditation 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

↑

→