FIDO Certification
Security Laboratory Accreditation
Program

Version 1.1

May 2017

Revision History

Date	Version	Description
2017-03-09	1.0	Approved by CWG.
2017-04-04	1.0	Approved by the Board Certification Committee
2017-05-26	1.1	Added ISCCC as an approved Third Party Accreditation for L2. Approved by CWG on May 26, 2017.

1 Table of Contents

2 Introduction

This document gives an overview of the policies that govern Laboratory Requirements for those seeking Security Accreditation for FIDO Certification Program.

It also defines the relationship between FIDO and its Accredited Security Laboratories.

2.1 Audience

This policy document is intended for Laboratories seeking or maintaining FIDO Laboratory Accreditation for the FIDO Certification Program.

2.2 Support

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

3 Overview

This document covers the FIDO Security Laboratory Accreditation process and requirements for FIDO Certification. FIDO may issue other types of Laboratory Accreditation in the future, such Accreditation would be maintained as part of their own Accreditation Program and are outside the scope of this document.

Laboratories that have been Accredited by the FIDO Alliance via the process outlined herein will evaluate the security of implementations according to the Authenticator Certification Policy.

The FIDO Laboratory Accreditation process focuses on the necessary aspects of a Laboratory to evaluate an implementation for areas with security impact.

All Laboratories shall follow the process outlined in this document in order to apply for and maintain their Active status as an Accredited Security Laboratory.

3.1 Roles & Responsibilities

3.1.1 FIDO Alliance

The FIDO (Fast IDentity Online) Alliance is a 501(c)6 nonprofit organization nominally formed in July 2012 to address the lack of interoperability among strong authentication devices as well as the problems users face with creating and remembering multiple usernames and passwords. The FIDO Alliance plans to change the nature of authentication by developing specifications that define open, scalable, and interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. This new standard for security devices and browser plugins will allow any website or cloud application to interface with a broad variety of existing and future FIDO-enabled devices that the user has for online security.

3.1.1.1 Certification Working Group (CWG)

The Security Laboratory Accreditation program is a responsibility of the FIDO Certification Working Group (CWG) in partnership with the Security Requirements Working Group (SRWG), with necessary oversights and approvals from the FIDO Board of Directors and collaboration with other FIDO Working Groups where needed.

The CWG may, at the discretion of its members, create subcommittees and delegate responsibilities for all or some portion of the CWG’s certification program responsibilities to those subcommittees. The Certification Secretariat is responsible for implementing, operating, and managing the certification program defined by the CWG.

3.1.1.2 Security Requirements Working Group (SRWG)

The Security Requirements Working Group is responsible for defining and maintaining the Security Requirements for Authenticator Certification and acts as Security Experts for FIDO.

3.1.1.3 Certification Secretariat

FIDO Staff responsible for implementing, operating, and managing FIDO Certification Programs.

3.1.1.4 Security Secretariat

FIDO Staff responsible for reviewing applications, questionnaires, monitoring security threats, and acting as an independent FIDO security expert for the FIDO Certification Program. The FIDO Staff that make up the Security Secretariat are: Technical Director, Security Certification Advisor, Certification Program Development, and individuals designated as Certification Secretariat.

The Security Secretariat will provide an unbiased assessment of the *Laboratory Accreditation Application*.

3.1.2 Laboratory

FIDO Laboratory Accreditation is available to public and private testing laboratories, including commercial laboratories; university laboratories; and federal, state, and local government laboratories.

3.1.2.1 Authorized Representative

Laboratory-appointed Representative to act as the main point of contact for FIDO.

3.1.2.2 Approved Evaluators

Accredited Security Laboratory personnel that have participated in FIDO Training and satisfactorily completed the Knowledge Test.

3.1.3 FIDO Certification Program

The FIDO Certification Program is intended to certify the security characteristics of authenticators conforming to FIDO specifications (e.g. UAF and U2F authenticators). Level 1 ensures implementations are conformant to the specifications, are interoperable, and meet basic security and privacy considerations. Level 1 is tested by FIDO. Level 2 and above require evaluation and/or testing by a FIDO Accredited Security Laboratory.

4 Laboratory Requirements

Accreditation is granted following the successful completion of the Accreditation process which includes submission of an application, payment of fees, assessments, FIDO Training, and Knowledge Tests.

Laboratories are Accredited for a specific site location. Laboratories will be assessed based on the criteria listed in Laboratory Requirements depending on the requested Scope of Accreditation.

The Accreditation is formalized through issuance of a Certification of Accreditation.

Laboratories are required to maintain their Accreditation status through participation in the FIDO Alliance Accredited Security Laboratory Group, and successfully complete FIDO Training and Knowledge Testing as new requirements or specification versions are released.

Accreditation must be renewed with proof of continuous support of the latest standards and practices every 3 year(s).

There will be a public list of FIDO Accredited Security Laboratories on the FIDO Website.

4.1 Third Party Accreditation Requirements

The FIDO Authenticator Certification Program is divided into Levels, for each level there are different Laboratory requirements.

4.1.1 Level 1

The Level 1 Security Requirements will be tested and evaluated by the FIDO Certification and Security Secretariats.

4.1.2 Level 2

Level 2 Security Requirements will be evaluated by FIDO Accredited Security Laboratories.

Compliance to ISO 17025 is a prerequisite requirement for all laboratories. The scope must cover the Information Technology Security Testing (ITST).

A laboratory must have Accreditation from at least one of these ISO 17025 programs:

ISO 17025 Accreditation - Accepted Programs

Scope	Program	Area of Accreditation
ISO/IEC 17025:2005 - ITST	Cryptographic and Security Testing	Basic Cryptographic and Security Testing Cryptographic Modules - HW & SW Testing
ISO/IEC 17025:2005 - ITST	Common Criteria Testing	CC Testing

ISO 17025:2005 - Useful References

Program	Accreditation	URL
ISO	ISO/IEC 17025:2005	● A2LA http://www.a2la.org/dirsearchnew/newsearch.cfm ● NVLAP http://ts.nist.gov/standards/scopes/programs.htm ● ANAB (formerly ACLASS) http://search.anab.org/search-accredited-companies.aspx ● PJLA http://www.pjlabs.com/search-accredited-labs ● IAS http://www.iasonline.org/Calibration_Laboratories/CL.html ● L-A-B http://search.l-a-b.com/ ● ILAC http://ilac.org/ilac-mra-and-signatories/ Link to the Catalogues: http://www.iso.org/iso/catalogue_detail?csnumber=39883

In addition to ISO 17025, the following Lab Accreditations are recognized as fulfilling FIDO Lab Accreditation Requirements for Level 2 and can be used as evidence during the *Accreditation Application*.

A laboratory must have Accreditation from at least one of these Accepted Programs.

Third Party Accreditation - Accepted Programs

Program	Accreditation	URL
Common Criteria	CC Licensed Lab	https://www.commoncriteriaportal.org/labs/
FIPS 140-2	NVLAP Information Technology Security Testing (ITST) Cryptographic and Security Testing	https://www-s.nist.gov/niws/index.cfm?event=directory.search#no-back
CCTL	NVLAP Information Technology Security Testing (ITST) Common Criteria Testing	https://www-s.nist.gov/niws/index.cfm?event=directory.search#no-back
GlobalPlatform TEE	TEE Accredited Laboratory	https://www.globalplatform.org/teecertificationlaboratory.asp
TCG TPM	N/A	http://www.trustedcomputinggroup.org/certification/
EMVCo	EMVCo Lab Accreditation	https://www.emvco.com/approvals.aspx?id=104
China Information Security Certification Center (ISCCC)	National Information Security Product Certification Organization Information Security Risk Assessment Service Qualification Organization	http://www.isccc.gov.cn/zxjs/zxjs/index.shtml#intro

4.1.3 Level 3+

Security Level 3 and above are not currently available for Accreditation.

For information on Level 3+ development FIDO members that are sponsors or above can join SRWG. For more information on membership see https://fidoalliance.org/membership/.

4.2 Business Requirements

This section describes the overall business requirements which a Laboratory must meet.

4.2.1 Legal

The Laboratory must be recognized as a legal entity and must be (or must be a part of) an organization that is registered as a tax-paying business or as having a tax exempt status or as a legal entity in some form with a national body.

The Laboratory must be able to sign and abide by all FIDO legal agreements for Accredited Security Laboratories, including the FIDO *Laboratory Evaluation Agreement*.

4.2.2 Public Communications

The Laboratory agrees to abide by FIDO's policy that evaluation and/or testing performed at any FIDO Accredited Security Laboratory is acceptable for Authenticator Certification, and must make no claims to the contrary in its marketing material.

A Laboratory must not, under any circumstances, communicate nor disclose to any third party, including to the vendor or other entity submitting an implementation for testing, that an implementation has or has not been Certified by FIDO. FIDO, not the Laboratory, shall be the final party to determine whether a particular implementation conforms to the FIDO Specifications or FIDO Certification Program Policies.

4.2.3 Independence

The Laboratory must be able to demonstrate independence in test case analysis methodology and testing processes from the party involved in the design or manufacturing of the implementation under test.

- The Laboratory must not be owned by an implementation vendor without prior agreement from FIDO.
- The Laboratory must not evaluate an implementation that they have been involved in designing except that they may provide quality assurance testing (debug sessions) prior to the vendor submitting the product for official FIDO evaluation.

4.3 Security Requirements

This section describes the security requirements that a Laboratory must meet.

4.3.1 Physical

The Laboratory must maintain and comply with a physical security policy that includes, at a minimum, the following requirements.

4.3.1.1 Physical Layout

The Laboratory must have sufficient security measures to prevent unauthorized people from entering the building. If the Laboratory is part of a shared building or complex, there must be sufficient security measures to prevent unauthorized people from entering the Laboratory or offices.

4.3.1.2 Evaluation Areas

Areas in the Laboratory facilities in which products, components, or data are tested or stored must be restricted to authorized personnel. Authorized personnel are defined by the Laboratory as part of ISO 17025.

4.3.1.3 Storage

Within the Laboratory there must be sufficient (according to ISO 17025) secure storage space to provide adequate protection for all ongoing work. Secure storage must be provided for all materials retained by the Laboratory after evaluation has been completed.

4.3.2 Logical Security

The Laboratory must maintain and comply with a logical security policy that includes, at a minimum, the following requirements.

4.3.2.1 Classified Materials and Information

Test samples and documents must be handled with care and the materials must be controlled and stored securely whether in electronic or paper format.

Classified material must be stored in secure containers, where unauthorized access is prevented by appropriate measures (e.g. alarms, surveillance, and sufficient mechanical protection).

Disclosure of FIDO or vendor data and documents to third parties must be authorized in writing by an officer of the company that owns the data or documents to be released. Classified documents must be stored according to their classification level. When a vendor grants permission to the Laboratory to release classified information concerning the vendor's implementation to FIDO, this information may be released only to FIDO. The FIDO Security or Certification Secretariat will release the information to appropriate working group members within FIDO.

4.3.2.2 Evaluation Reports

All Evaluation Reports must be stored securely.

The Laboratory must store samples and all reports and logs the test sessions (whether paper or electronic) for a period of three years from the date the *FIDO Evaluation Report* was submitted to FIDO.

When submitting electronic Evaluation Reports to FIDO, the report must, be PGP encrypted and securely uploaded using the *FIDO Evaluation Report Submission Form*. All FIDO Certification forms and Evaluation Reports will be stored within an encrypted database only accessible by the FIDO Security Secretariat, and will not be shared.

Unless a previous agreement has been made between the Security Secretariat and the Laboratory, all evaluation reports sent via email will not be reviewed and will be deleted.

4.4 Administrative Requirements

This section describes the administrative requirements that a Laboratory must meet.

4.4.1 Quality Assurance

The Laboratory must have a quality system based upon ISO requirements, providing documented procedures defining processes to ensure a high quality of testing and test reproducibility. A Laboratory is required to comply with ISO 17025, and must also comply with the requirements stated elsewhere in this document.

4.4.2 Personnel

The Laboratory must maintain a list of their FIDO-qualified test personnel consisting of a description of their role in the organization, their qualifications, and their experience. The Laboratory must have procedures in place to ensure a match between staff training and and roles in the performance of FIDO activities.

The individual(s) performing the evaluation must be included on the Evaluation Reports submitted to FIDO. These Approved Evaluators will be required to maintain knowledge of FIDO Specifications and FIDO Certification Program Policies.

4.5 Technical Requirements

4.5.1 Technical Expertise

The Laboratory must have at least two years of experience of testing in the domain for which it is seeking Accreditation.

Prior experience with FIDO Specifications is strongly recommended as Laboratory employees that wish to be Approved Evaluators are required to pass a Knowledge Test in order to receive accreditation.

5 Laboratory Accreditation Process

This section introduces the process required to apply for a new FIDO Laboratory Accreditation.

5.1 New Accreditation Process

Step	Responsible Party	Process Requirement
FIDO Accreditation Application	Laboratory	Completes the *Laboratory Accreditation Application*.
	FIDO Security Secretariat	Completes review of *Laboratory Accreditation Application*. Informs Laboratory if the Application meets FIDO requirements, by providing an *Accreditation Assessment Report* to the Laboratory, notifying the Laboratory if it may proceed with the Accreditation process. Provides the Laboratory with the *FIDO Laboratory Evaluation Agreement*.
Legal Agreements	Laboratory	Schedules an appointment with the FIDO Security Secretariat and makes the financial and legal arrangements with the Security Secretariat to complete the Accreditation Assessment. Signs Laboratory portion of the *FIDO Laboratory Evaluation Agreement*.
FIDO Accreditation Training	Laboratory	Onboarding Call with FIDO Security Secretariat. FIDO Training and Knowledge Test.
Accreditation Issuance	Laboratory	Pays Accreditation Fees.
	FIDO Certification Secretariat	If the Accreditation Assessment and Knowledge Test meets all requirements: ● Signs the FIDO portion of the *FIDO Laboratory Evaluation Agreement*. ● Issues a *Laboratory Accreditation Certificate*. ● Adds the Laboratory to the list of Accredited Security Laboratories on the FIDO website.

6 FIDO Accreditation Application

To officially start the accreditation process the Laboratory must complete the *Accreditation Application* by providing documentation for the following areas:

6.1 Proposed Scope of Accreditation

Proposed list of the FIDO Certification Programs or Levels within those Programs for which the Laboratory is applying for Accreditation.

Scope of Accreditation can be changed later following the Accreditation Scope Change process.

6.2 Authorized Representative

An applicant Laboratory must designate an Authorized Representative that will act as the main contact for FIDO.

6.3 Business Practices

The Laboratory should provide evidence of business practices in the form of a written report describing:

- Services of the organization
- Structure of the organization, demonstrating the isolation between the Laboratory and other areas of the organization (e.g. design area).
- Percentage of revenue received from each of the Laboratory's top ten vendor customers relative to the total revenue of the Laboratory.
- Certificate of ownership and/or tax identification number.

6.4 Physical & Logical Security

The Laboratory should provide evidence of physical and logical security. This must be provided to FIDO either within the Laboratory procedures and documentation or a written report describing:

- Laboratory security policy with particular focus on the physical and logical network security measures.
- Personnel background check security policies.
- Confidential data protection practices.

6.5 Administrative Conformance

The Laboratory should provide evidence of administrative conformance in the form of a written report describing:

- Description of the Laboratory's quality assurance system.
- Overview of the Laboratory personnel and the qualifications of Laboratory personnel involved in the performance of any testing or administrative duties connected with this Accreditation.
- Overview of the Laboratory equipment and techniques.
- Description of the Laboratory security policy with particular focus on the procedures for identification and recording of test samples.
- Overview of Laboratory asset management system for documentation and equipment.

6.6 Technical Expertise

Technical expertise summary describing:

- Experience with FIDO Specifications.
- List of and evidence of other Formal Accreditations held by the Laboratory relevant to the proposed Scope of Accreditation.

6.7 Application Review

The Security Secretariat will review the *Laboratory Accreditation Application* and will assess the Laboratory's fulfillment of all applicable requirements within the proposed Scope of Accreditation.

The Security Secretariat will inform Laboratory if the Application meets FIDO requirements, by providing an *Accreditation Assessment Report* to the Laboratory, notifying the Laboratory if it may proceed with the Accreditation process.

7 Legal Agreements

7.1 Laboratory Evaluation Agreement

The Authorized Representative must sign the *Laboratory Evaluation Agreement*.

7.2 Confidentiality

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

7.3 Consistent Business Practices

It is mandatory that any evaluation and/or test results from any FIDO Accredited Security Laboratory be recognized by all other FIDO Accredited Security Laboratories without any further investigation.

8 FIDO Accreditation Training

8.1 Onboarding Call

An introduction to FIDO Specifications and FIDO Certification Programs will be given by the FIDO Security Secretariat.

8.2 FIDO Training

FIDO Training will be conducted by FIDO for the Laboratory Personnel requesting recognition as Approved Evaluators. A minimum of one Approved Evaluator is required for Laboratory Accreditation. This training will prepare individuals to pass the Knowledge Test.

8.3 Knowledge Test

To become an Approved Evaluator, the Laboratory Personnel must pass a Knowledge Test on FIDO Specifications, Security Requirements, Security Test Procedures, and Program Policies.

9 Accreditation Issuance

9.1 Fees

Laboratories must pay all Accreditation fees before a *Laboratory Accreditation Certificate* will be issued.

9.2 Laboratory Accreditation Certificate

Once at least one individual from the Laboratory has satisfactorily completed the Knowledge Test, the Authorized Representative can file an *Accreditation Certificate Application*.

The Certification Secretariat will be responsible for verifying all submitted documentation and issuing Laboratory Accreditation Certificates.

Turn-around time for Accreditation Certificates will be as soon as reasonably possible and no more than 30 days from the submission of the Application.

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

- The Company name of the Laboratory that has been Accredited
- The address of the Laboratory
- The Scope of Accreditation
- The version of the Security Laboratory Accreditation Policy at the time of Accreditation
- The Expiration Date of the Accreditation
- Any restrictions, as necessary
- The Issuance Date of the Accreditation
- The Certificate Number in the format LAPPPPPPYYYYMMDDNNN, where:
    - LA = Lab Accreditation
    - PPPPPP = Policy Version in the format MMNNRR where:
        - MM = Major Number,
        - NN = Minor Number,
        - RR = Revision Number
    - YYYY = Year Issued
    - MM = Month issued
    - DD = Day issued
    - NNN = Sequential Number of Certificates issued that day

The Laboratory's Accreditation is valid for 3 years after the issuance date.

9.3 Decision Appeals

If FIDO decides that a Laboratory is initially denied Accreditation, FIDO shall notify the Laboratory of the decision and will provide the reasons for not granting Accreditation. If the Laboratory disagrees with the reasons given for not granting Accreditation, it may appeal the decision. Appeal actions shall be initiated within 30 days of the notification of the decision not to grant accreditation.

10 Accreditation Maintenance

10.1 Group Participation

Laboratories are required to participate in the Accredited Security Laboratory Group and maintain voting rights.

If a Laboratory loses its voting rights it will be issued a written warning by FIDO, and the Laboratory will be given the opportunity to regain voting rights. If the Laboratory fails to regain voting rights within the timeline specified in the written warning the Laboratory will be suspended.

10.2 Test Procedure Version Maintenance

The Laboratory will be required to maintain support of all active versions of the Security Test Procedures For new versions, Laboratories will be required to support the version 90 days after the public release of the version.

10.3 Transparency of Testing Practices and Results

Records of testing should include, at a minimum, the Reference Devices used and the test configurations. All other information regarding testing should be included as required in the FIDO Evaluation Report. FIDO may request more information on how testing was performed or reported, and detailed records should be kept for a minimum of three years from the date the FIDO Evaluation Report was submitted to FIDO.

10.4 Knowledge Tests

Training sessions and knowledge tests will be required as new requirements or specification versions are released. The knowledge test must be satisfactorily completed by at least one Approved Evaluator before completing an evaluation against the new version, or within 90 days of publication, whichever comes first.

In order to maintain Accreditation, Approved Evaluators are required to satisfactorily complete Knowledge Tests every three years as part of the renewal process.

10.5 Disclosure of Security Vulnerabilities

If at any time the Accredited Security Laboratory encounters a Security Vulnerability within the Authenticator Boundary the Laboratory should make the best effort to notify the FIDO Security Secretariat and the Vendor within 48 hours.

The vulnerability will be triaged and handled according to the Security Vulnerability Assessment process outlined in the Authenticator Certification Policy.

10.6 Proficiency Assessments

At any time, at the discretion of FIDO, a Proficiency Assessment may be required.

FIDO will inform the Laboratory that the Proficiency Evaluation must be performed, the requirements of the assessment, and the date by which the assessment must be completed. The scope of the Proficiency Assessment will include a Laboratory’s capabilities and compliance with the Security Test Procedures.

If an Accredited Security Laboratory does not complete the assessment to the satisfaction of FIDO by the date required, FIDO may suspend or revoke its Accreditation.

A Proficiency Assessment follows the process outlined in the Renewal Assessment, but instead is initiated by FIDO.

11 Accreditation Renewal

A Laboratory must be validated through a Renewal Assessment every 3 years to maintain FIDO Accreditation.

11.1 Renewal Assessment

The Renewal Assessment must be completed before the expiration date of the Laboratory's Accreditation. It is the responsibility of the Laboratory to renew its Accreditation before it expires. If a Laboratory does not renew its Accreditation, FIDO may revoke its Accreditation.

Responsible Party	Process Steps
Laboratory	Completes FIDO *Renewal Request*
FIDO Security Secretariat	Completes assessment of the *Renewal Request*. Informs Laboratory if the *Renewal Request* meets FIDO requirements and if it may proceed with the Renewal process. Identifies the Renewal Assessment requirements and informs the Laboratory.
Laboratory	Schedules an appointment with a FIDO Security Secretariat and makes the arrangements with the Security Secretariat for the Renewal Assessment. Satisfactory completion of the Knowledge Test by at least one Approved Evaluator.
FIDO Security Secretariat	Completes the *Renewal Assessment Report* and provides the document with the Approved or Rejected decision to the Laboratory.
FIDO Certification Secretariat	If the *Renewal Assessment Report* is Approved by FIDO: ● Issues an updated *Laboratory Accreditation Certificate*. ● Updates the Laboratory information on the FIDO Website, if necessary.

12 Modification or Termination of Accreditation

A Laboratory's Accreditation may be modified or terminated.

The following sections outline reasons for modification or termination of Accreditation.

12.1 Laboratory Change in Testing Services Offered

At any time, a Laboratory may decide to change the testing services it offers. If this occurs, the Laboratory is required to notify FIDO.

If a Laboratory decides to cease offering one or more of many FIDO testing services, the Laboratory must send a notice to FIDO using the *Accreditation Change Request Form*. Upon receipt of such a request, FIDO will modify the Laboratory's Scope of Accreditation accordingly, re-issue a Certificate of Accreditation (without changing the expiration date), and update the details in the list of Accredited Security Laboratories on the FIDO website.

If the Laboratory decides to cease offering their only FIDO testing service, FIDO Laboratory Accreditation will be Revoked.

12.2 Laboratory Change - Other

The Laboratory must notify FIDO immediately of any changes in personnel (including Approved Evaluators), ownership, legal status, location or other change that may impact the Accreditation. The Laboratory should use the FIDO *Change Request* to notify FIDO of these changes.

12.3 Accreditation Scope Change

In the case where a Laboratory requests to add a new type of Accreditation evaluation and/or testing (i.e. add to the Scope of Accreditation), an Accreditation Scope Assessment is required. The existing renewal date for the Laboratory's Accreditation does not change.

The requirements for an Accreditation Scope Assessment are determined by FIDO at the time of the Assessment. The scope of the Assessment is a whole or subset of the Accreditation Assessment.

The Accreditation Scope Change process follows the Accreditation Assessment process, but instead starts by completing a *Change Request*.

12.4 Laboratory Termination of Accreditation

At any time, a Laboratory may request termination of its Evaluation Agreement with FIDO.

The Laboratory should complete an *Accreditation Change Request* to notify FIDO. Upon receipt of such request, FIDO will confirm termination of the Accreditation and Evaluation Agreement and remove the Laboratory's name from the FIDO website.

12.5 Nonconformance

Nonconformance refers to an Accredited Security Laboratory’s failure to conform to the policies or requirements listed herein.

If FIDO finds a Laboratory to be in nonconformance the Laboratory will be contacted and given a deadline to provide further information or correct the nonconformance. If the Laboratory fails to respond to FIDO or does not adequately correct the nonconformance the Accreditation will be suspended for further investigation or to allow the Laboratory to correct their non-conformance. Accreditation may be revoked if the non-conformance is not resolved.

If the Laboratory disagrees with a non-conformance decision the Laboratory has the option to file a formal appeal or complaint to Certification Secretariat to be reviewed by the Crisis Response Team.

13 Accreditation Status

13.1 Pending

Laboratory that has started the Accreditation process but has not yet received an Accreditation Certificate or notice of a decision not to Accredit the Laboratory.

13.2 Active

Accredited Security Laboratory in good standing with FIDO.

13.3 Inactive

Inactive status is given to a Laboratory that has voluntarily requested in writing that their Accreditation be placed on hold due to unforeseen or unavoidable circumstances that temporarily prevent the Laboratory from adhering to the FIDO Laboratory Accreditation policy.

Inactive Laboratories will not be listed on the FIDO Website.

A Laboratory may have an Inactive status for no longer than one year.

If the Laboratory does not become Active after one year the Laboratory Accreditation shall be Suspended.

13.4 Suspended

At any time, at FIDO's discretion, FIDO may suspend a Laboratory's Accreditation:

- Based on the results of an Assessment
- Due to a Laboratory's Non-conformance
- If a Laboratory fails to complete a Proficiency Assessment

If the Laboratory is suspended:

- The Laboratory will receive written notice of the suspension along with the actions required to return to Active status.
- The Laboratory will be removed from the FIDO Website.
- FIDO will set the requirements and date by which a Proficiency Assessment must be completed.

If the Laboratory remains in a suspended state for a period of 180 days the Laboratory Accreditation will be Revoked. 90, 60, and 30 days prior to this deadline notices will be sent to the Suspended Laboratory.

13.5 Revoked

At any time, at FIDO's discretion, FIDO may revoke a Laboratory's accreditation:

- Based on the results of an Assessment
- Due to a Laboratory's Non-conformance
- If a Laboratory fails to renew its Accreditation before the expiration date.
- If a Laboratory has not performed testing on FIDO products within the last 3 years.

If the Laboratory is revoked:

- The Laboratory will receive written notice of the Revocation.
- The Laboratory will be removed from the FIDO Website.
- The Laboratory Evaluation Agreement will be terminated.
- The Laboratory must make available to FIDO all evaluation reports for implementations already certified by FIDO or currently in testing for Certification within 30 days of the notice of revocation.
- The Laboratory must promptly return to FIDO all FIDO property and all confidential information. Alternatively, if so directed by FIDO, the Laboratory must destroy all confidential information, and all copies thereof, in the Laboratory's possession or control, and must provide a certificate signed by the Authorized Representative of the Laboratory that certifies such destruction in detail acceptable to FIDO.

14 Appendix A: Terms & Abbreviations

Term / Abbreviation	Definition
MDS	Metadata Service
HSV	Handset Vendor
MNO	Mobile Network Operator
CWG	Certification Working Group
SRWG	Security Requirements Working Group
Accreditation	Formal recognition that a Laboratory has and continues to demonstrate fulfillment of competence and other requirements in this document.
Certificate of Accreditation OR Laboratory Accreditation Certificate	Document issued by FIDO to a Laboratory that has been granted FIDO Accreditation.
Customer	Any person or organization that engages in the services of a testing Laboratory. See also, Vendor.
Revocation	Removal of the Accredited status of a Laboratory if the Laboratory is found to have violated the conditions for Accreditation.
Scope of Accreditation	Portion of the Certificate of Accreditation that lists the FIDO Certification Programs or Levels within those Programs for which the Laboratory is Accredited.
Suspension	Temporary removal by FIDO of the Accredited status of a Laboratory for all or part of its scope of accreditation when it is determined (by the Laboratory, or by FIDO) that the Laboratory does not meet the conditions of accreditation.
Certification Working Group	FIDO Working Group composed of FIDO member companies that oversee the FIDO Certification Programs.
Security Requirements	FIDO Working Group composed of FIDO member companies that

Working Group	define the requirements for Authenticator Certification and act as Security Experts for FIDO.
Certification Secretariat	FIDO Staff responsible for implementing, operating, and managing FIDO Certification Programs.
Security Secretariat	FIDO Staff responsible for reviewing applications, questionnaires, monitoring security threats, and acts as an independent FIDO security expert for the FIDO Certification Program.
Crisis Response Team	FIDO Staff group responsible for responding to identified security vulnerabilities. The group is composed of the Executive Director, Marketing Director, Technology Director, Certification Secretariat, and Security Secretariat.
Certification Troubleshooting Team	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.
Accredited Security Laboratories	Laboratories that have successfully completed the FIDO Laboratory Accreditation Process and have a valid Certificate of Accreditation.
Vendor	FIDO member organization or non-member organization seeking FIDO Certification.
Partner Programs	Independent certification programs with which FIDO has entered a relationship in order to offer joint certification programs to lessen the certification burden on Vendors. Partner programs can be found within Security Level 2 and above.
Approved Evaluator	Laboratory Personnel that have been trained by FIDO and satisfactorily completed the required Knowledge Test(s) as required by the Laboratory Accreditation Policy.
Authorized Representative	Laboratory Personnel or Legal Representative authorized to sign on behalf of the Laboratory.
Accredited Security Laboratory Group	Closed group available only to Accredited Security Laboratory employees used to discuss Security Requirements and Security Threats.

15 Appendix B: Program Artifacts

Step	Responsible Party	Artifact
FIDO Accreditation Application	Laboratory	FIDO Accreditation Application
	FIDO Security Secretariat	FIDO Laboratory Evaluation Agreement
Legal Agreements	Laboratory	FIDO Laboratory Evaluation Agreement
Accreditation Assessment	FIDO Security Secretariat	Accreditation Assessment Report
	Laboratory	FIDO Training Knowledge Test
Accreditation Issuance	FIDO Certification Secretariat	FIDO Laboratory Evaluation Agreement Accreditation Certificate Application Laboratory Accreditation Certificate Accredited Security Laboratory List (on the FIDO website)
Modification or Termination of Accreditation	Laboratory	Renewal Request Change Request
	FIDO Security Secretariat	Proficiency Assessment Report
Security Evaluations (described in Authenticator Certification Policy)	Laboratory	FIDO Evaluation Report Evaluation Report Submission Form