FIDO Certification

Laboratory Accreditation Application

January 2018

Version 1.1

Contents

1 Introduction

This Application is part of the FIDO Accredited Security Laboratory Program. It is intended for Security Laboratories that wish to complete evaluations and testing as part of the FIDO Certification Program for Level 2 and above.

1.1 FIDO Alliance

FIDO Alliance is an industry consortium defining the specifications supporting a full range of authentication technologies, including biometrics such as fingerprint and iris scanners, voice and facial recognition, in addition to existing Restricted Operating Environments (ROE) standards such as Trusted Platform Modules (TPM), Trusted Execution Environment (TEE) and Security Elements (SE).

FIDO's Certification Program is intended to assess the security of the existing implementations compliant with FIDO specifications. This process requires a third-party lab to be involved for Certifications at Level 2 and above to conduct the Security Evaluation. For this purpose, FIDO created a Security Laboratory Accreditation Program.

1.2 Roles & Responsibilities

The **Certification Secretariat** is FIDO Staff responsible for implementing, operating, and managing all FIDO Certification Programs.

The **Security Secretariat** is FIDO Staff responsible for reviewing applications, questionnaires, monitoring security threats, and will act 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.

Accredited Security Laboratories are Security Testing Laboratories that have successfully completed FIDO Laboratory Accreditation.

Vendors seeking Certification may be FIDO member organizations or non-member organizations. This document governs all such requests for L2 and above Certification.

1.3 Audience

This Application is intended for Laboratories to request a FIDO Security Laboratory Accreditation.

1.4 Scoring Criteria

The Application will be scored for each requirement as follows:

- PASSED = The information provided by the lab sufficiently meets the requirement
- INCONCLUSIVE = The information provided by the lab is incomplete or not sufficient to meet the requirement.
- FAILED = The information provided does not meet the requirement.

For INCONCLUSIVE and FAILED results the Security Secretariat will provide additional information as an informative recommendation.

A laboratory must have all requirements as PASSED to be Approved by the Security Secretariat.

1.5 Instructions

Laboratories should complete all questions in this Application. If attachments are to be included with the application please indicate them in the file name as [LaboratoryName]-AccreditationApplication-[Application Section].

Existing L2 Accredited Security Laboratories can refer to their previous application contents whenever it is relevant.

1.6 Submission Instructions

Please PGP encrypt and submit the application and any supporting documents to the FIDO Certification Secretariat at certification@fidoalliance.org with the subject "Security Accreditation Application [Laboratory Name]".

1.7 Support

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

2 Application

2.1 Contact Information

Please provide the following contact information:

Contact Information	
Company Name	
Physical Address	
Mailing Address (If different than above)	
Zip Code	
Country	
Phone Number	
Authorized Representative	
Authorized Rep. Title	
Authorized Rep. Email	
Authorized Rep. Phone	

2.2 Proposed Scope of Accreditation

Please indicate the scope of Accreditation you wish to perform as an Accredited Laboratory:

Scope of Accreditation	
Security Level(s) Requested	

Note: At this time, **Level 2, Level 3 and 3+** are the available options for this question. As the Certification Program expands additional levels will be added.

2.3 Business

Please provide the following evidence of business practices:

Business		
Laboratory Services		
Structure of the Organization (including Design Area)		
Top 10 Vendors and percentage of revenue received for each Vendor relative to Total Revenue	Vendor	Revenue Percentage
	1.	
	2.	
	3.	
	4.	
	5.	

Business		
	6.	
	7.	
	8.	
	9.	
	10.	
Certificate of Ownership and/or Tax Identification Number		

2.4 Physical & Logical Security

Please provide the following evidence of physical and logical security:

Note: Evidence from ISO 17025 or CC Audit Reports may be used.

Physical & Logical Security	
Physical and Logical Network Security Measures	

Physical & Logical Security	
Personnel Background Check Security Policies	
Confidential Data Protection Practices	

2.5 Administrative Conformance

Please provide the following evidence of administrative conformance:

Note: Evidence from ISO 17025 or CC Audit Reports may be used.

Administrative Conformance	
Quality Assurance System	

Administrative Conformance	
Laboratory Personnel & Qualifications	
Proposed Approved Evaluators **Note:** One Approved Evaluator is required. Evaluators must complete the FIDO Training and Knowledge Test to be considered Approved Evaluators.	Evaluator Name
	1.
	2.
	3.
	4.
	5.
	6.
	7.
	8.
	9.
	10.

Administrative Conformance	
Laboratory Equipment and Techniques	
Laboratory Security Policy	

Administrative Conformance	
Laboratory Asset Management System	

2.6 Technical Expertise

Please provide the following evidence of technical expertise:

<table>
<tr><th colspan="3">Technical Expertise</th></tr>
<tr><td>Experience with FIDO Specifications or similar technologies
(Please include statement of the evaluation projects, scope, and work carried out)</td><td colspan="2"></td></tr>
<tr><td rowspan="3">ISO 17025 Accreditation Program (Security Accreditation)

(Provide the accreditation certificate provided by an internationally recognized national information security body)

Note: At least one of the following ISO area of accreditations is required:
• ISO/IEC 17025:2005 – ITST Cryptographic and Security Testing
o Basic Cryptographic and Security Testing</td><td>ISO Program</td><td>Date Received / Expiration Date</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>

<table>
<tr><td>

o Cryptographic Modules - HW & SW Testing

• ISO/IEC 17025:2005 – ITST

o Common Criteria Testing

</td><td></td><td></td></tr>
<tr><td rowspan="8">Approved Accreditation (Security Accreditation)

(Provide the accreditation certificate)

Note: At least one of the Approved Accreditations is Required:
- Common Criteria – CC Licensed Lab
- FIPS 140-2 – NVLAP Information Technology Security Testing (ITST) Cryptographic and Security Testing
- CCTL – NVLAP Information Technology Security Testing (ITST) Common Criteria Testing
- GlobalPlatform TEE – TEE Accredited Laboratory
- TCG TPM
- EMVCO Lab Accreditation
- China Information Security Certification Center (ISCCC)</td><td>Approved Accreditation</td><td>Date Received / Expiration Date</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>

L3 and L3+ Approved Accreditation (Security Accreditation): For a Laboratory to qualify for the Scope of Level 3 or 3+ Common Criteria the Laboratory must have at least one of each of the following Third-Party Accreditations: (Provide the accreditation certificate) **Step 1:** At least one of the Approved Accreditations is Required (Basic Partner Program Testing Capabilities): - ISO/IEC 17025-2005 – ITST – Common Criteria Testing - Common Criteria – CC Licensed Lab - China Information Security Certification Center (ISCCC) – National Information Security Product Certification Organization Information Security Risk Assessment Service Qualification Organization **Step 2:** At least one of the Approved Accreditations is Required (Smart Card & AVA_VAN.3+ capability): - SOG-IS – qualified for EAL1-7 for "smartcards and similar devices" - GB/T 31057-2015 – Information security technology	Approved Accreditation	Date Received / Expiration Date

Other Accreditations (Optional)		

- End of Application -

3 Results and Recommendations

This section will be completed by the Security Secretariat and returned to the Laboratory once the review of the Application is complete.

The Application will be scored for each requirement as follows:

- PASSED = The information provided by the lab sufficiently meets the requirement
- INCONCLUSIVE = The information provided by the lab is incomplete or not sufficient to meet the requirement.
- FAILED = The information provided does not meet the requirement.

For INCONCLUSIVE and FAILED results the Security Secretariat will provide additional information as an informative recommendation.

The Application Result will be Approved, or Rejected with Reasoning. When an Application is Rejected with Reasoning the Laboratory should review the recommendations provided and update the application as necessary and resubmit the Application.

Security Secretariat Information		
Name		
Email		
Date Review Completed		
Requirements Review	Result	Recommendation
Scope of Accreditation		
Business Practices		

Physical & Logical Security		
Administrative Conformance		
Technical Expertise		
Application Result		

- End of Results & Application -