FIDO Allowed Integration Document (FAID)

Version 1.5

November 2021

Revision History

Date	Version	Description
2019-05-15	0.9	Initial version
20199-05-23	1.0	First complete version
2019-06-06	1.1	Feedback from ELLIT
2020-02-15	1.2	Minor changes in chapter 3 to require information on the transaction concept
2020-06-19	1.3	Minor changes for the environment of the TOE
2020-01-02	1.4	Minor changes
2021-11-28	1.5	Updates for the requirements on the TOE description (chapter 3.1) and TOE hardware (chapter 4.1)

Contents

1 Introduction

This document defines the FIDO Allowed Integration Document (FAID) scope and contents. It shall serve as a template for an FAID for a Biometric developer while starting an evaluation of a FIDO Biometric Authenticator.

The guidelines contained herein are intended to provide a common ground and structure for all developers to prepare their Allowed Integration Document (FAID) for certifications.

1.1 Audience

The primary audience of this document are developers of biometric components undergoing certifications according to the FIDO biometric component certification program, but it may be useful to all the parties involved in the FIDO Authenticator Certification Program willing to have a deeper understanding of the Biometric Evaluation process.

1.2 Confidentiality & Copyright notice

This document must be strictly confidential for only the FIDO certification team, the Accredited Laboratory, and the Vendor concerned in the current evaluation.

It is expected that the developer commits to share this document with parties having a legit interest in the certification of the biometric component.

1.3 Contact

1.3.1 FIDO Security Secretariat

The FIDO Biometric Secretariat is responsible for reviewing applications, questionnaires, monitoring security threats, and acts as an independent expert for the FIDO Biometric Component Certification Program.

For help and support, visit the FIDO Website [FIDO Cert] or contact the FIDO Biometric Secretariat at biometric-certification@fidoalliance.org.

1.4 FAID Instructions and Structure

The FIDO Allowed Integration Document (FAID) must be completed by a developer seeking to obtain certification for a biometric component according to the FIDO biometric criteria.

2 Formal Information

Please provide the following details.

2.1 Laboratory Details

Laboratory Name:	
Evaluator(s) Name:	

2.2 Biometric Component Details

Vendor Company Name:	
Vendor Contact Name:	
Vendor Contact Email:	
Implementation Name for the biometric component:	
Biometric Modality (Fingerprint, Face, Voice,...)	
Version of the biometric component	
FIDO Biometric component certification criteria Version:	
Do you opt for self attestation?	
If you opt for self-attestation, please indicate the target FAR	

3 TOE Overview

This chapter is intended to provide an overview over the Biometric Component that should be certified. This component is also referred to as “Target of Evaluation (TOE)” in this context.

3.1 Overview

Please provide a short overview over the TOE and its use case. Please make sure to cover

- A general overview,
-
- the process of enrolment and indication of a failure to enroll,
- the process of verification and indication of failure to acquire,
- specific information about the transaction concept of the TOE (i.e. how many attempts are allowed per transaction),
- all timeouts that may occur during operation (including their values),
- the logging capabilities,
- the storage of biometric information,
- is there a fixed operating point? If not, document the selected operating point(s).

In case that a TOE comes in multiple configurations (e.g. with different sensors), sufficient information shall be provided for all configurations. This will allow the laboratory to develop a dedicated test concept covering all allowed configurations or the range of allowed configurations.

3.2 Verification of the version information

Please give a short description, how a user can verify/check the version information of the biometric component.

4 Intended Environment

This chapter should specify the intended environment for the TOE in terms of hardware, software and other environmental factors.

4.1 Hardware

Please describe, which hardware the TOE needs in its immediate environment. Examples could be a camera with a certain resolution or a CPU with a certain performance characteristics.

The definition of hardware can be addressed in two different manners:

1) By a complete definition of the hardware: e.g. “The TOE runs only on the mobile phone X from vendor Y, version 1”
2) By a dedicated definition of all relevant hardware characteristics that the TOE needs

While the 2nd solution allows a greater flexibility, please note that this kind of definition is also more challenging. The laboratory will set up a test plan based on these descriptions and the developer shall make sure that the TOE really works on a hardware platform meeting the characteristics.

In case a needed hardware cannot be defined exactly but needs to be addressed in a more generic manner, sufficient information about the relevant characteristics shall be provided (including the limits for these characteristics).

Example:

Insufficient description: “The TOE requires a camera”

Sufficient description: “The TOE requires a camera with a resolution between 640x480 pixels and 1024x768 pixels. The SNR of the camera shall not be below X”

4.2 Software

Please describe, which software the TOE needs in its immediate environment. Examples could be an Android or iOS Operating System or also certain other software. Please note that the required software has to be clearly identified, including version information. While it is possible to specify that the TOE is intended to be used on a certain OS ranging from version x to version Y, it is not possible to specify that the TOE is intended to be used on an OS version X or higher (as this would include unknown versions).

The software that is needed by the TOE can best be specified in the form of a table as the following.

Software	Version	Used for

4.3 Physical Environment

Please briefly describe the environment that the TOE is intended to be used in. This specifically includes the definition of all environmental aspects that are relevant for the performance of the biometric mechanism.

Examples of such aspects include sound levels for voice modalities, lighting conditions for facial and contactless fingerprint modalities, and power constraints (such as if the device can be only operated on

battery or can be operated with a power source). Please note however that this list is not meant to be complete.

If the TOE is intended for use in multiple environments, please specify each environment in a separate subchapter and provide a speaking name. The intended environment(s) that is chosen for testing, will be identified on the certificate using this name.

5 Allowed changes to the TOE

A FIDO certification is granted for a certain version of a TOE. This means that any changes to the TOE will require a re-certification if the certification should be extended to the new version.

In rare cases, it is however possible that certain aspects of the TOE can be changed during the integration into an authenticator component without requiring re-certification.

If the developer claims that such changes are possible, they shall be described in this chapter.

6 Appendix A: References

Reference	Title	URL
[FIDO Cert]	FIDO Certification Website	https://fidoalliance.org/certification/
[BiometricReq]	FIDO Biometrics Requirements	

7 Appendix B: Terms & Abbreviations

Term / Abbreviation	Definition
Authenticator Boundary	A vendor-defined boundary according to Security Requirement 1.1.
CC	Common Criteria
CWG	Certification Working Group
PP	Protection Profile
FER	FIDO Evaluation Report
RP	Relying Party
SRWG	Security Requirements Working Group
Security Requirements Working Group	FIDO Working Group composed of FIDO member companies that define the requirements for the Security Certification Program and act as Security Experts for FIDO.
Accredited 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.
Security Secretariat	FIDO Staff responsible for reviewing applications, questionnaires, monitoring security threats, and acts as an independent FIDO security expert for the FIDO Security Certification Program.
Accreditation	Formal recognition that a Laboratory is competent to carry out specific tests or calibrations of types of tests or calibrations. Accreditation does not imply any guarantee of Laboratory performance of test/calibration data.
Certificate of Accreditation	Document issued by FIDO to a Laboratory that has been granted FIDO Accreditation.
TOE	Target of Evaluation