CERTIFIED AUTHENTICATOR LEVELS

AUTHENTICATOR LEVEL 1

AUTHENTICATOR LEVEL 2

AUTHENTICATOR LEVEL 3

AUTHENTICATOR LEVEL 3+

COMPANION PROGRAMS

FIDO ACCREDITED SECURITY LABORATORIES

Implementer Dashboard >

Home / Certification Overview / Certified Authenticator Levels

Certified Authenticator Levels

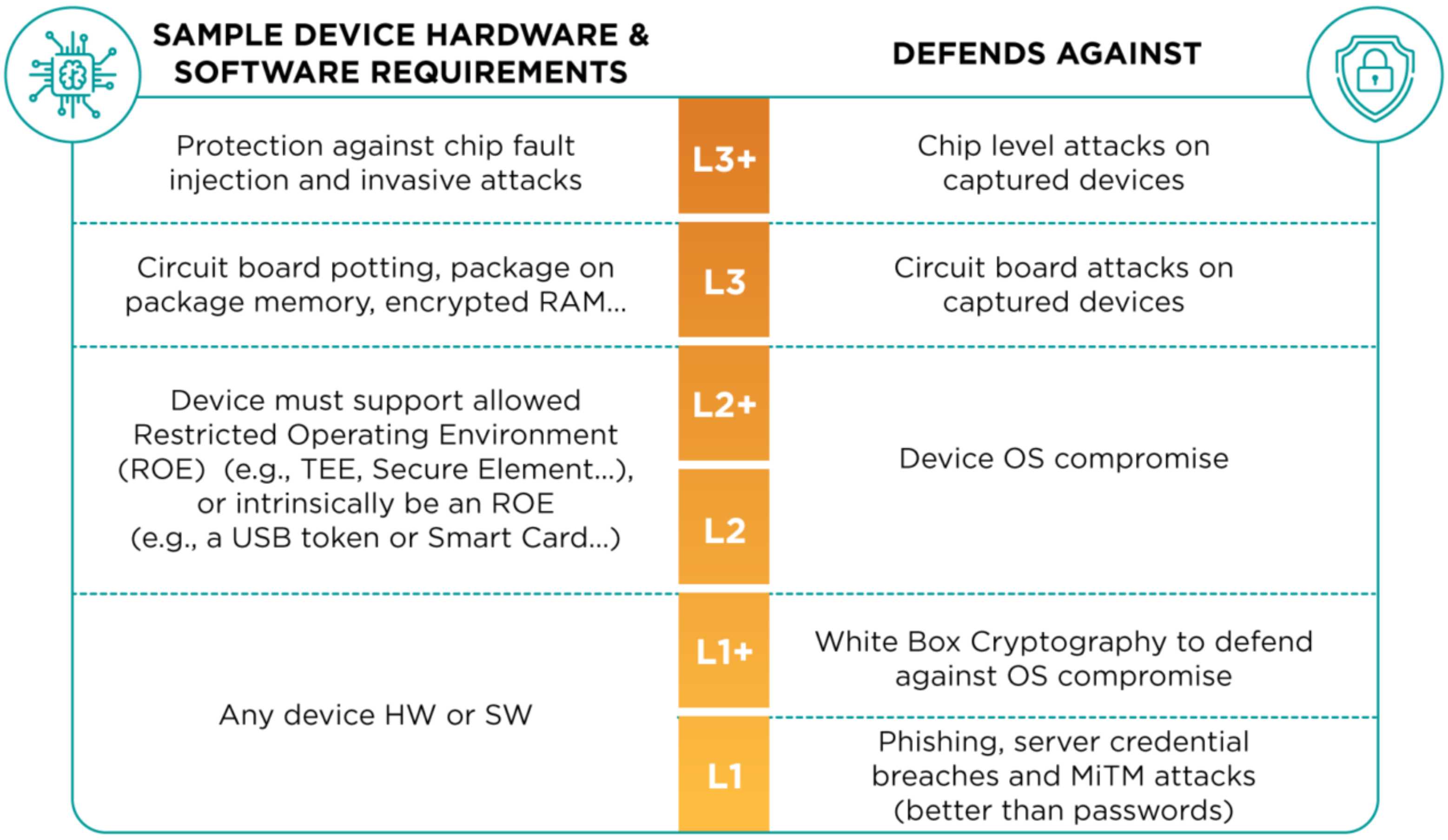
The Authenticator Certification Levels introduce Authenticator Security Requirements to the FIDO Certification Program. Authenticators must be certified to **at least** Authenticator Certification Level 1 (L1) for UAF, U2F, and FIDO2 certification.

Currently, the supported Certification Levels are:

- Level 1
- Level 2
- Level 3
- Level 3+

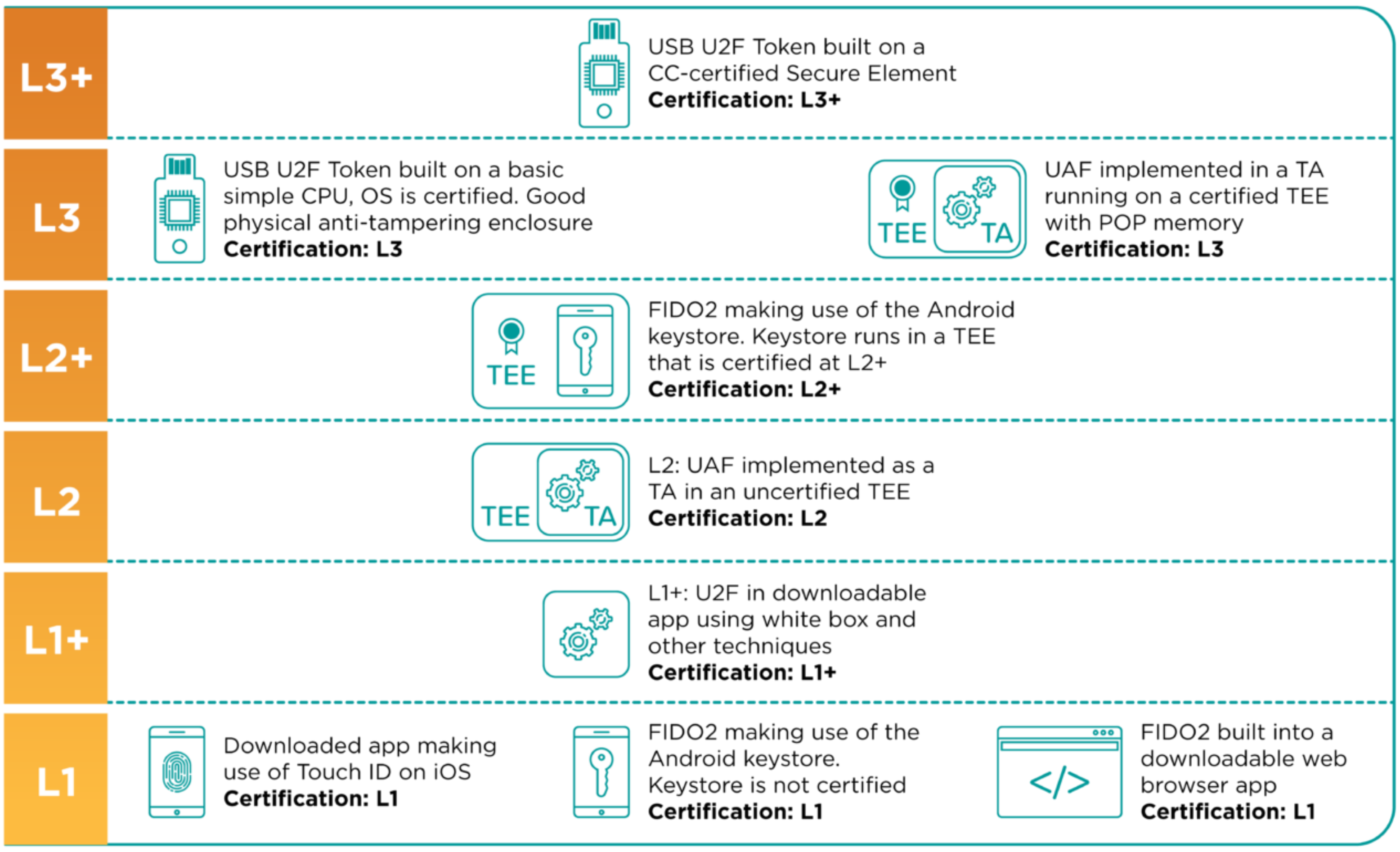
The Levels build on each other, so L2 includes all the requirements for L1, plus additional requirements for L2.

Higher levels are in active development by the FIDO Security & Privacy Requirements Working Group (SPWG).



SAMPLE DEVICE HARDWARE & SOFTWARE REQUIREMENTS		DEFENDS AGAINST
Protection against chip fault injection and invasive attacks	L3+	Chip level attacks on captured devices
Circuit board potting, package on package memory, encrypted RAM...	L3	Circuit board attacks on captured devices
Device must support allowed Restricted Operating Environment (ROE) (e.g., TEE, Secure Element...), or intrinsically be an ROE (e.g., a USB token or Smart Card...)	L2+	Device OS compromise
	L2	
Any device HW or SW	L1+	White Box Cryptography to defend against OS compromise
	L1	Phishing, server credential breaches and MiTM attacks (better than passwords)

FIDO AUTHENTICATOR CERTIFICATION EXAMPLES



L3+

USB U2F Token built on a CC-certified Secure Element
Certification: L3+

L3

USB U2F Token built on a basic simple CPU, OS is certified. Good physical anti-tampering enclosure
Certification: L3

UAF implemented in a TA running on a certified TEE with POP memory
Certification: L3

L2+

FIDO2 making use of the Android keystore. Keystore runs in a TEE that is certified at L2+
Certification: L2+

L2

L2: UAF implemented as a TA in an uncertified TEE
Certification: L2

L1+

L1+: U2F in downloadable app using white box and other techniques
Certification: L1+

L1

Downloaded app making use of Touch ID on iOS
Certification: L1

FIDO2 making use of the Android keystore. Keystore is not certified
Certification: L1

FIDO2 built into a downloadable web browser app
Certification: L1

This page contains the Policy and Requirements Documents and the Authenticator Certification Process.

Policy and Requirements Documents

The documents for Authenticator Certification include:

FIDO Authenticator Certification Policy

This policy governs the Authenticator Certification Levels as part of the FIDO Certification Program.

Download: PDF

FIDO Authenticator Security Requirements

This document outlines the Authenticator Security Requirements for the Authenticator Certification Levels. Example: Implementations seeking L1 Certification must meet the requirements labeled L1 and higher, Implementations seeking L2 Certification must meet the requirements labeled L1 and higher and L2 and higher, and so forth depending on Certification level seeking. This document also includes the Vendor Questionnaire and Test Procedure instructions for each requirement.

Download v1.3 (active): HTML | PDF

FIDO Authenticator Vendor NDA

Non-disclosure Agreement to be signed by Authenticator Vendors (Implemeters) completing Authenticator Certification.

Download: PDF

Vendor Questionnaire Worksheets

Non-normative companion excel worksheets of the Vendor Questionnaires are available to assist Implementers completing Authenticator Certification.

Download: Level 1 | Level 2 | Level 3/3+

Sample Vendor Questionnaire. This sample should be used as a reference only. It is being provided as a guide for completing the Vendor Questionnaire and to help make the evaluation process more efficient and effective.

FIDO Impact Analysis Report (FIAR)

This document defines the FIDO Impact Analysis Report (FIAR) template listing the scope and the structure of the expected contents. It describes the requirements for when changes are made to the authenticator and will help to determine whether the authenticator is eligible for derivative or delta certification. This report must be completed by Authenticator Vendors and submitted to the FIDO Security Secretariat.

Download: FIDO Impact Analysis Report (FIAR)

FIDO Allowed Cryptography List

This document defines Allowed Cryptography referenced in the Authenticator Security Requirements.

Download: HTML | PDF

FIDO Allowed Restricted Operating Environments List

This document defines the Allowed Restricted Operating Environments referenced in the Authenticator Security Requirements.

Download: HTML | PDF

FIDO Authenticator Metadata Requirements

This document defines the Authenticator Metadata Requirements referenced in the Authenticator Security Requirements.

Download: HTML | PDF

Authenticator Certification Process

The Authenticator Certification follows the Functional Certification process and the Authenticator Certification process adds the evaluation of a completed Vendor Questionnaire. The Vendor Questionnaire is how Vendors document how their implementation meets the Authenticator Security Requirements.

The high-level process steps are:

1. Preparation
2. Functional Certification Requirements
3. Authenticator Certification Application
4. Security Evaluation
   - Vendor Questionnaire
   - Security Secretariat (L1) or Accredited Security Laboratory (L2, L3, or L3+) Security Evaluation & FIDO Evaluation Report
5. Report Review
6. Certification Issuance
7. (Optional) Trademark Usage.
8. (Optional) Metadata Submission to MDS

Preparation
Implementations seeking FIDO Certification must fulfill the requirements specified in the documents above.

All Authenticator Vendors seeking Authenticator Certification must create an account for FIDO Certification, you can request an account, or login.

For Level 2 and higher, it is recommended that the Vendor contact a FIDO Accredited Security Laboratory early in order to work out contract and NDA details so the Vendor and the Lab are ready for the Security Evaluation process, and so the Accredited Security Laboratory can be listed as part of the Authenticator Certification Application step.

Functional Certification Requirements

Vendors must complete FIDO Functional Certification requirements for Authenticators, including the Conformance Self-Validation and Interoperability Testing, prior to submitting an application for FIDO Authenticator Certification.

For L1, this includes the L1 Interoperability Requirements that must be verified during Interoperabilty Testing.

Authenticator Certification Application

To begin FIDO Authenticator Certification, the Vendor completes the Authenticator Certification Application (through the Implementer Dashboard).

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

The Authenticator Certification Application must be approved before the Security Evaluation step can begin.

Security Evaluation

The Security Evaluation step includes the Vendor's attestation of how the implementation meets the Security Requirements and the Security Evaluation performed by FIDO Security Secretariat or a FIDO Accredited Security Laboratory to review the Vendor Questionnaire and complete the Test Procedures.

For L1, The Vendor Questionnaire is completed in two steps:

1. L1 Interoperability Requirements are verified during an Interoperability Event for a subset of the L1 Security Requirements. (This must be completed prior to the Authenticator Certification Application).
2. The Vendor completes the L1 Vendor Questionnaire by providing a rationale for the remainder of the requirements not verified at the Interoperability Event.

Once the Vendor Questionnaire is complete, it is submitted to the Security Secretariat. The Security Evaluation will be performed by the Security Secretariat by reviewing the completed Vendor Questionnaire and performing the Security Test Procedures. The Security Secretariat will prepare the FIDO Evaluation Report.

For L2 and higher, the Vendor will choose a FIDO Accredited Security Laboratory to perform Security Evaluation. The Vendor will submit the L2 and higher Vendor Questionnaire to the FIDO Accredited Security Laboratory and an Approved Evaluator will perform the Security Test Procedures. The Approved Evaluator will submit a FIDO Evaluation Report to the Security Secretariat.

Report Review

Once complete, the implementer reviews the FIDO Evaluation Report prepared by the FIDO Security Secretariat or Accredited Security Laboratory and submits to the Security Secretariat (through the Implementer Dashboard).

For L1, the approved Vendor Questionnaire and FIDO Evaluation Report must be submitted to the Security Secretariat.

For L2 and higher, only the FIDO Evaluation Report must be submitted to the Security Secretariat.

The FIDO Evaluation Report must be approved by the Security Secretariat before the Vendor can complete the Certification Request.

Certification Issuance

As part of submitting the required documents to FIDO, the Vendor will also submit the Certification Request. The Certification Request will be evaluated by the Certification Secretariat to ensure all requirements are met.

The Vendor must pay the Authenticator Certification Fees before a Certificate will be issued.

Trademark Usage (Optional)

After executing the Trademark License Agreement (TMLA), Vendors may use the FIDO® Certified mark and logo on their product, packaging, and marketing literature.

Metadata Submission to MDS (Optional)

The Vendor has the option to submit Metadata to the FIDO Metadata Service (MDS).

Implementer Dashboard

Implementers can Login to view their Dashboard.

Login

fido ALLIANCE simpler stronger authentication

Join the Community

GET THE LATEST UPDATES

PARTICIPATE IN FIDO-DEV FORUM