FIDO Authenticator Allowed Restricted Operating Environments List

FIDO Alliance Final Requirements Document 02 November 2021

This version:
https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-allowed-restricted-operating-environments-list-v1.3-fd-20211102.html
Previous version:
https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-allowed-restricted-operating-environments-list-v1.2-fd-20201102.html
Editors:
Laurence Lundblade, Qualcomm
Meagan Karlsson, FIDO Alliance

Abstract

This document helps support the FIDO Authenticator Security Certification program. The FIDO Security Requirements requires authenticators to run in an Allowed Restricted Operating Environment (AROE) for level 2 and above. Authenticators *not* running in an AROE can qualify for level 1.

Status of This Document

This section describes the status of this document at the time of its publication. Other documents may supersede this document. The most recent version of this document can be found on the FIDO Alliance Website at https://fidoalliance.org.

This document was published by the FIDO Alliance as a Final Requirements Document. If you wish to make comments regarding this document, please Contact Us. All comments are welcome.

Table of Contents

- 1. Notation
  - 1.1 Version
- 2. Introduction
- 3. Requirements for Restricted Operating Environment to be Allowed
- 4. Allowed Restricted Operating Environments
- A. References
  - A.1 Normative references
  - A.2 Informative references

1. Notation

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].

1.1 Version

This document specifies version 1.1.0 of the allowed restricted operating environments.

2. Introduction

FIDO Authenticators can be implemented in various ways.

The FIDO Authenticator is typically implemented based on some hardware and firmware. For example, this might be a secure element as hardware with the basic secure element firmware in which the Authenticator Trusted Application runs. As another example it might also be a multifunctional device containing some CPUs which are securely shared between the firmware of the restricted operating environment and the high-level operating system.

It is important that by definition, all parts which are relevant for the FIDO Authenticator (e.g. underlying hardware, ...) are part of the Authenticator itself. So the FIDO Authenticator is more than just the Authenticator Application.

We use the term Authenticator Application to refer to the entity that combines the underlying hardware and firmware in a way that results in a FIDO Authenticator.

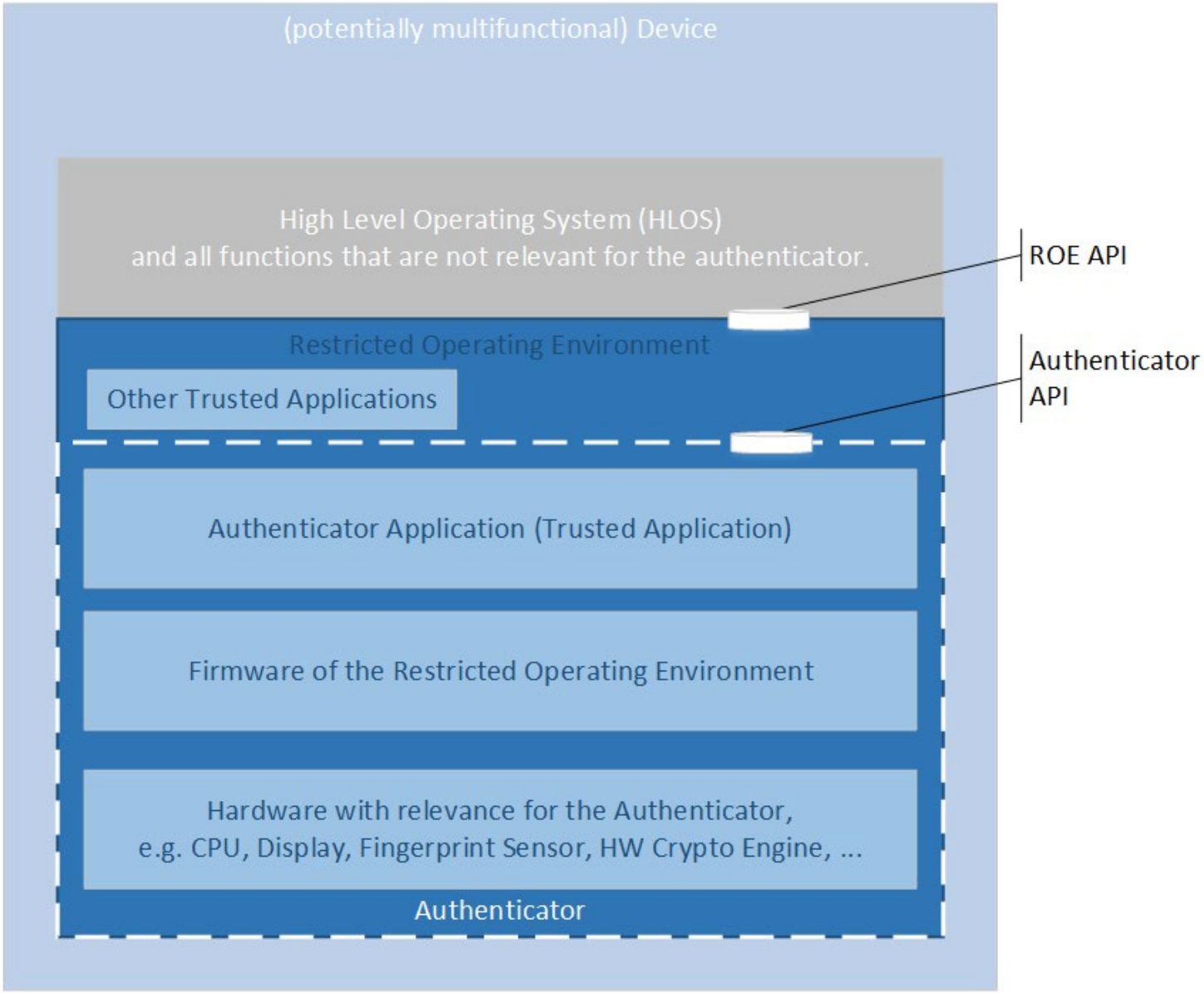

Fig. 1 Restricted Operating Environments Architectural Overview

We distinguish these components as the Restricted Operating Environment can be implemented in a way that it supports more than just the Authenticator Application. Additionally the security of the Restricted Operating Environment (***ROE***) (without the Authenticator Application) can be demonstrated or certified using existing programs (e.g. Common Criteria).

The FIDO Security Certification covers the various components with different depths. At FIDO Security Level 1, we are concenred about the protection against scalable attacks on the server side an on the communication channel. At FIDO Security Level 2, we are mostly concerned about the protection against client side scalable attacks (e.g. malware). At FIDO Security Levels 3 and 3+ we also require protection against physical attacks.

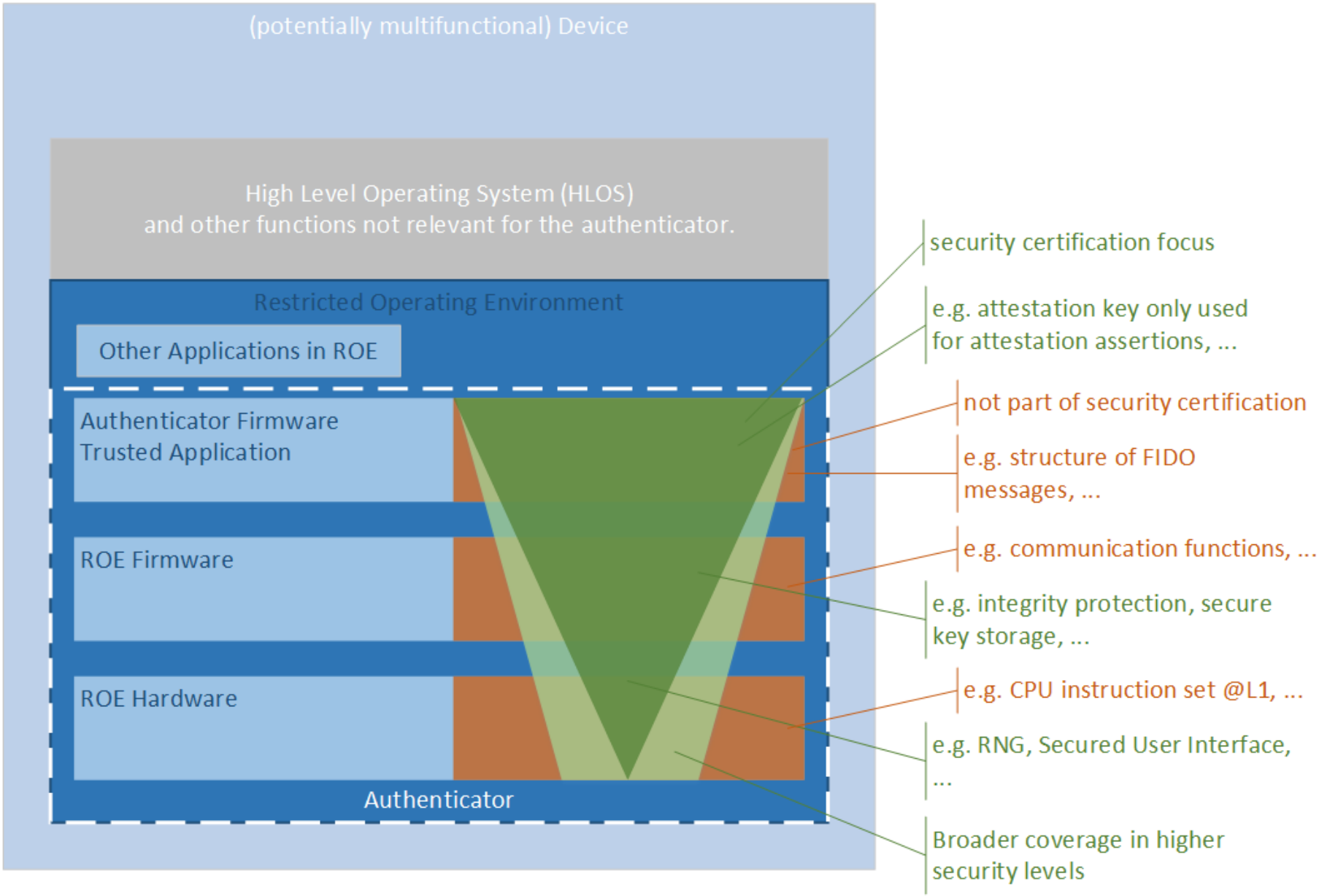

Fig. 2 Restricted Operating Environments Security Certification Focus

The following aspects of the AROE are relevant for the FIDO Security Certification:

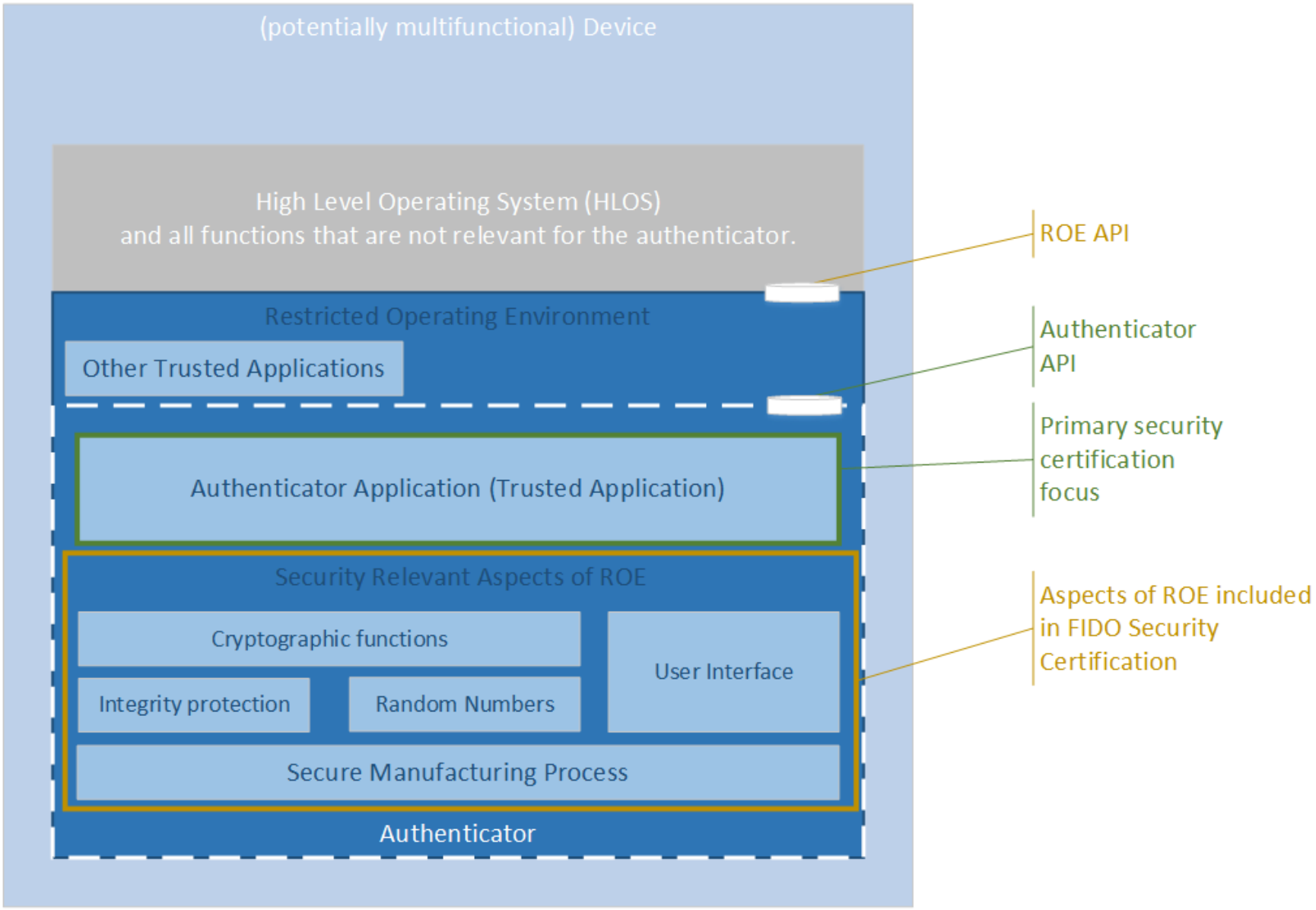

Fig. 3 AROE Aspects Relevant for FIDO Security Certification

3. Requirements for Restricted Operating Environment to be Allowed

- The AROE security configuration MUST be controlled by the vendor of the commercial device or its delegates or its suppliers.
- The AROE MUST protect itself from modifications degrading its security. This includes modifications when powered-off. It hence requires a secure boot process of the AROE.
- The AROE MUST provide full isolation from any rich OS or external devices or operating environments it connects with except for conveyance of protocol messages intended for communication with the rich OS and external devices or operating environments. As a consequence, it MUST NOT be

possible for SW or HW on the same device but outside the AROE to modify any state, registers, memory or storage inside the operating environment.

- The AROE SHOULD be security-oriented with the bulk of the functionality it hosts and provides being focused primarily on security (e.g., not large graphics engines, signal processors, general purpose app hosting, network stacks and such).
- If multiple apps or processes are allowed within the AROE and they are not within the authenticator boundary, there must be strong and complete isolation between the authenticator and those apps.
-
- The apps hosted by the AROE SHOULD be primarily security-oriented (e.g., does not host thousands of downloadable games, complex productivity apps like word processors, or large scale network apps like web browsers).
- A security oriented SW engineering practice SHOULD be followed
  - Code is reviewed by security experts
  - A security patch system is in place
  - Security incidents are tracked
  - Security coding practice is followed
  - System documentation is produced

4. Allowed Restricted Operating Environments

The following is the official lists of Approved Restricted Operating Environments (***AROE***s) FIDO Certification.

All entries in this list implement the requirements listed in Section 3.

Additions to this list must meet the requirements listed in Section 3 and must be voted on to the list by the FIDO SPWG. The vote approval is simply a vote on a new version of this document.

Operating Environment	Notes	Key Protection Type
TEEs based on ARM TrustZone HW	All operating systems (ROE firmware) running on ARM TrustZone HW are accepted as AROE as required for Level 2 FIDO Authenticator Certification. See ARM TrustZone Security Whitepaper and ARM Architecture Reference Manual.	TEE
TEE Based on Intel VT HW	All operating systems (ROE firmware) running on Intel VT HW are accepted as AROE as required for Level 2 FIDO Authenticator Certification. See Intel Vanderpool Technology for IA-32 Processors (VT-x) Preliminary Specification.	TEE
TEE Based on Intel SGX HW	All operating systems (ROE firmware) running on Intel SGX HW are accepted as AROE as required for Level 2 FIDO Authenticator Certification. See Innovative Instructions and Software Model for Isolated Execution and Innovative Technology for CPU based Attestation and Sealing.	TEE
TEE Based on Intel ME/TXE HW	All operating systems (ROE firmware) running on Intel ME/TXE HW are accepted as AROE as required for Level 2 FIDO Authenticator Certification. See Intel's Embedded Solutions: from Management to Security	TEE

TEE with GlobalPlatform TEE Protection Profile Certification	GlobalPlatform TEE Protection Profile Certification is NOT required for Level 2 FIDO Authenticator Certification, but it is sufficient for any TEE to be qualified as an Allowed Restricted Operating Environment. See TEE Protection Profile v1.2.1	TEE
Windows 10 Virtualization-based Security.	Security apps and services that are running at Virtual Trust Level 1 are accepted as AROE as required for Level 2 FIDO Authenticator Certification See Moore Defeating - Pass the Hash Separation of Powers.	SW
Secure World of AMD PSP (Platform Security coProcessor).	All operating environments running on the secure world side of the TrustZone in the AMD PSP. See AMD Secure Technology.	TEE
Trusted Platform Modules (TPMs) Complying to Trusted Computing Group specifications.	For example, TPM Main Specification Version 1.2 [TPM] or TPM Library Specification Version 2.0 [TPMv2] are accepted as AROE as required for Level 2 FIDO Authenticator Certification.	SW (HW stored or wrapped but may be exported to user device, i.e. SW due to the Note)
Secure Element (SE)	Secure Operating Systems (ROE firmware) running on a secure tamper-resistant microcontroller are accepted as AROE as required for Level 2 FIDO Authenticator Certification.	SE

Embedded CPU with in-package RAM	A system, running on a normal microcontroller:
	• with cpu, all flash and memory in a single package (tamper resistance is not required)
	• without access to flash and memory from outside the package
	• with security features including
	  ◦ Secure Boot to protect the integrity of the system
	• that does not allow installing applications
	• that restricts applications inside the Authenticator Boundary to:
	  ◦ Small and security-oriented
	  ◦ Fully under control of the Authenticator Vendor
	• that limits communication with external systems as follows:
	  ◦ FIDO protocols over FIDO approved transports (at the time of writing USB, NFC or BLE) are allowed.
	  ◦ Non-FIDO transports are allowed if necessary for chip programming
	  ◦ Network protocol stacks are explicitly disallowed (e.g., Ethernet, TCP/IP...)
	  ◦ Communication other than FIDO protocols must:
	  ▪ be small, simple and security-oriented in implementation
	  ▪ not result in compromise of FIDO security goals and certification requirements	

The above list is for specific technologies that can be given blanket AROE status.They can be approved before use in any particular authenticator. Once approved the approval is for any authenticator they are used in.

Sometimes authenticators are built using technologies that can't be given blanket approval because the security of their application is too variable. Another case is where the technology employed for the authenticator is entirely bespoke, and no technology can be named. Nonetheless, many authenticators do possess the characteristics of an AROE and must be allowed by certification.

In these cases, the authenticator vendor can provide a detailed description of the software and the hardware used to build the authenticator that answers all of the criteria listed in section 4 below. The FIDO security secretariat will take extra time on the certification to evaluate this detailed description and make a determination whether it is considered and AROE or not.

A. References

A.1 Normative references

[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

A.2 Informative references

[TPM]
. *TPM Main Specification*. URL: http://www.trustedcomputinggroup.org/resources/tpm_main_specification

[TPMv2]
. *TPM 2.0 Library Specification*. September 2016. URL: https://trustedcomputinggroup.org/tpm-library-specification/