FIDO Authenticator Allowed Restricted Operating Environments List

FIDO Alliance 24 May 2017

This version:
https://fidoalliance.org/specs/fido-uaf-v1.0-fd-20170524/fido-allowed-AROE-v1.0-fd-20170524.html
Editors:
Laurence Lundblade, Qualcomm
Meagan Karlsson, FIDO Alliance

Abstract

This document helps support the FIDO Authenticator Security Certification program. The FIDO Security Certification program has chosen only to certify authenticators running in Allowed Restricted Operating Environments (AROE). Authenticators *not* running in an allowed restricted operating environment are not eligible for FIDO Security Certification.

> NOTE
>
> As of February 2017, work on a ceritifcation program that does not require an AROE was started by the FIDO Alliance. This work will also result in a renaming or renumber of the security levels. The security level naming and numbering used here is the one in common use during 2015 and 2016 where the lowest security certification is Level 1 and Level 1 requires an AROE.

Status of This Document

This section describes the status of this document at the time of its publication. Other documents may supersede this document. A list of current FIDO Alliance publications and the latest revision of this technical report can be found in the FIDO Alliance specifications index at https://www.fidoalliance.org/specifications/.

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

Implementation of certain elements of this Document may require licenses under third party intellectual property rights, including without limitation, patent rights. The FIDO Alliance, Inc. and its Members and any other contributors to this Document are not, and shall not be held, responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.

THIS FIDO ALLIANCE DOCUMENT IS PROVIDED “AS IS” AND WITHOUT ANY WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTY OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

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

Implementation of certain elements of this Specification may require licenses under third party intellectual property rights, including without limitation, patent rights. The FIDO Alliance, Inc. and its Members and any other contributors to the Specification are not, and shall not be held, responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.

THIS FIDO ALLIANCE SPECIFICATION IS PROVIDED “AS IS” AND WITHOUT ANY WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTY OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

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].

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.

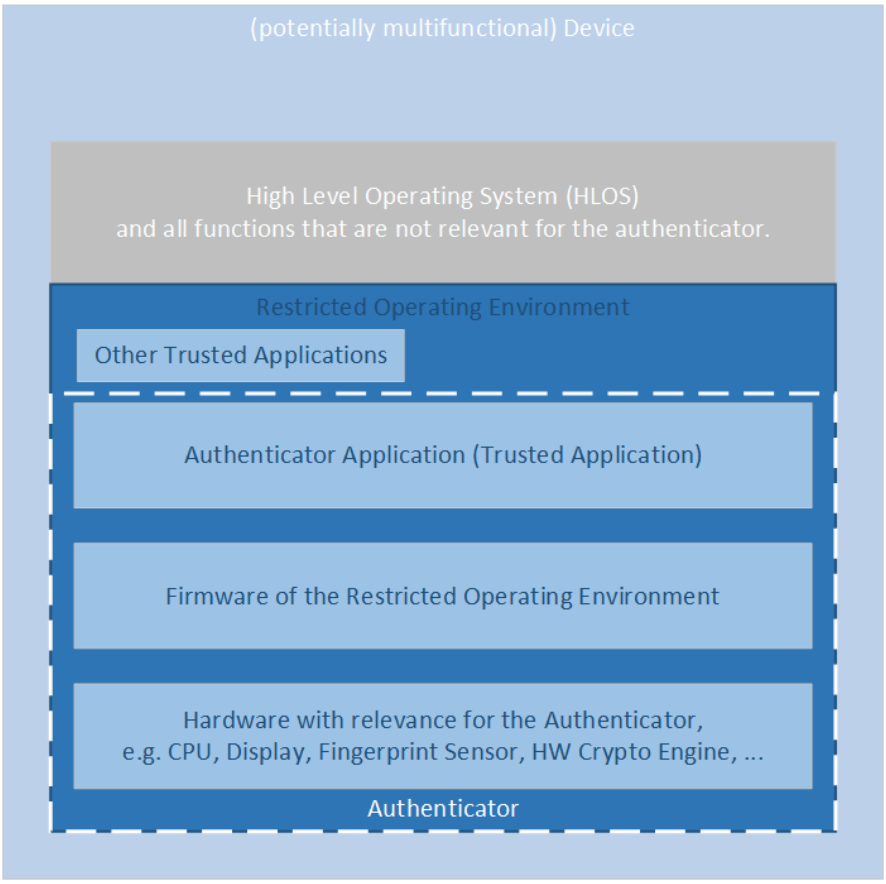

Fig. 1 Restricted Operating Environments Architectural Overview

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 Levels 1 and 2, we are mostly concerned about the protection against scalable attacks (e.g. malware). At FIDO Security Levels 3 and 4 we also require protection against physical attacks.

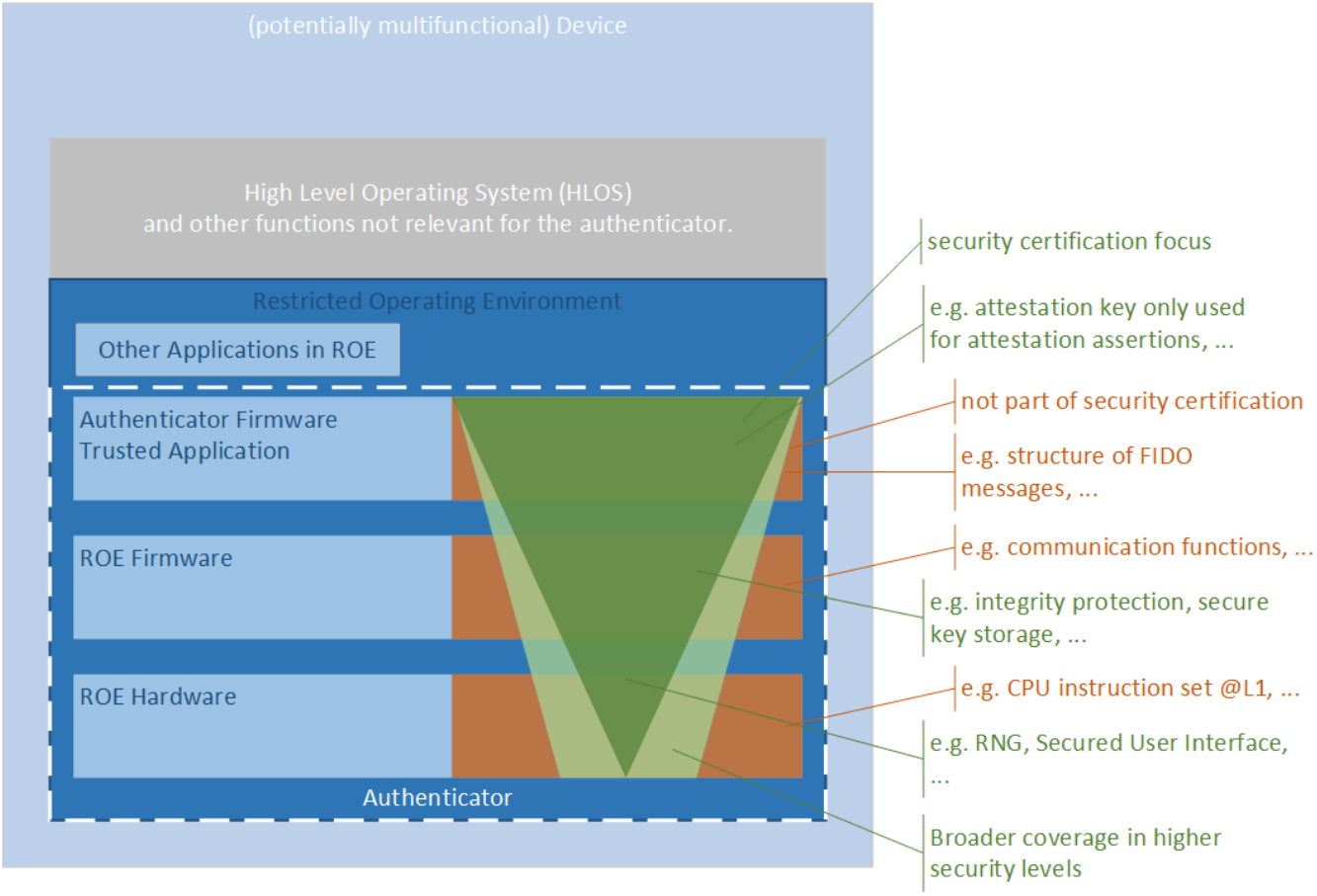

Fig. 2 Restricted Operating Environments Security Certification Focus

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

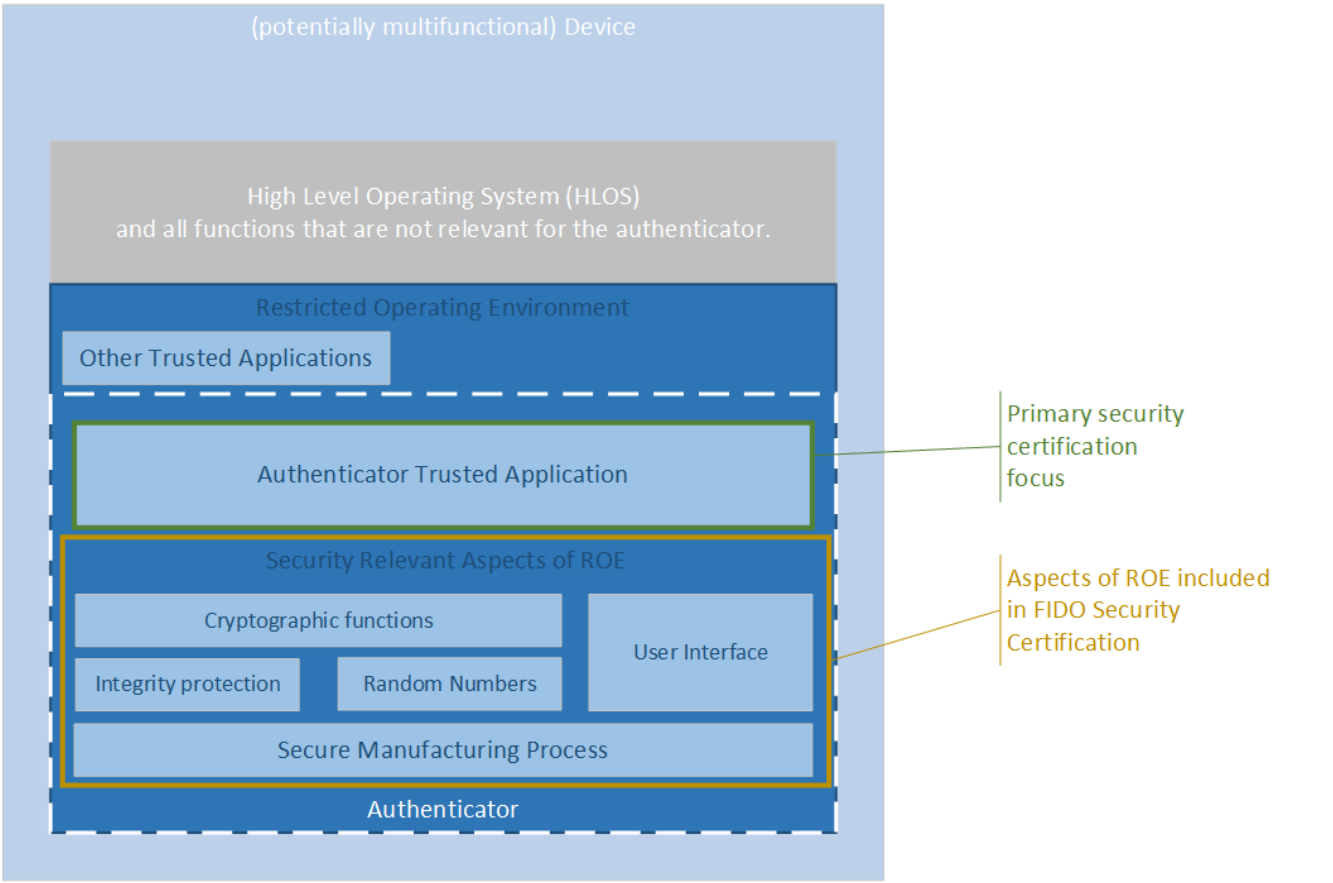

Fig. 3 AROE Aspects Relevant for FIDO Security Certification

3. Allowed Restricted Operating Environments

The following table outlines the Allowed Restricted Operating Environments (**AROE**s) for FIDO Security Certification.

Operating Environment	Notes

Operating Environment	Notes
TEEs based on ARM TrustZone HW	All operating systems (ROE firmware) running on ARM TrustZone HW are accepted for Level 1 FIDO Security Certification. See ARM TrustZone Security Whitepaper and ARM Architecture Reference Manual.
TEE Based on Intel VT HW	All operating systems (ROE firmware) running on Intel VT HW are accepted for Level 1 FIDO Security Certification. See Intel Vanderpool Technology for IA-32 Processors (VT-x) Preliminary Specification.
TEE Based on Intel SGX HW	All operating systems (ROE firmware) running on Intel SGX HW are accepted for Level 1 FIDO Security Certification. See Innovative Instructions and Software Model for Isolated Execution and Innovative Technology for CPU based Attestation and Sealing.
TEE Based on Intel ME/TXE HW	All operating systems (ROE firmware) running on Intel ME/TXE HW are accepted for Level 1 FIDO Security Certification
TEE with GlobalPlatform TEE Protection Profile Certification	GlobalPlatform TEE Protection Profile Certification is NOT required for Level 1 FIDO Security Certification, but it is sufficient for any TEE to be qualified as an Allowed Restricted Operating Environment. See TEE Protection Profile v1.2.1
Windows 10 Virtualization-based Security.	Security apps and services that are running at Virtual Trust Level 1. See Moore Defeating - Pass the Hash Separation of Powers.
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.
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].
Secure Element (SE)	Secure Operating Systems (ROE firmware) running on a secure tamper-resistant microcontroller.

4. 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).
- 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

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 Trusted Computing Group. Accessed March 2014. URL: http://www.trustedcomputinggroup.org/resources/tpm_main_specification

[TPMv2]
TPM Library Specification Trusted Computing Group. Accessed February 2017. URL: https://trustedcomputinggroup.org/tpm-library-specification/