FIDO Authenticator Security Requirements

FIDO Alliance 29 June 2018

This version:
https://fidoalliance.org/specs/fido-v1.0--20180629/fido-authnr-sec-reqs-v1.0--20180629.html
Previous version:
fido-authenticator-security-requirements-v1.0-fd-20170524.html
Editor:
Rolf Lindemann, Nok Nok Labs, Inc.
Contributors:
Dr. Joshua E. Hill, InfoGard Laboratories
Douglas Biggs, InfoGard Laboratories

Abstract

This documents defines the security requirements for FIDO Authenticators.

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://www.fidoalliance.org.

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 Requirements 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 the Requirements 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 REQUIREMENTS 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.

Table of Contents

1. Notation

1.1 Version

This document version (DV) is DV 1.2.0.

	L1	L1+	L2	L2+	L3	L3+
Security Requirements version (RV)	RV 1.2.0	-	RV 1.2.0	-	RV 1.1.0	RV 1.1.0
Allowed Cryptography List version (CV)	CV 1.2.0	-	CV 1.2.0	-	CV 1.2.0	CV 1.2.0
Vendor Questionnaire version (QV)	QV 1.1.1	-	QV 1.1.1	-	QV 1.0.1	QV 1.0.1
Test Procedures version (PV)	PV 1.1.0	-	PV 1.1.0	-	PV 1.0.0	PV 1.0.0

Table 1: Versions represented by this document

1.2 Key Words

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].

In summary:

1. "MUST", "REQUIRED", or "SHALL", mean that the definition is an absolute requirement of this document.
2. "MUST NOT", or "SHALL NOT", mean that the definition is an absolute prohibition of this document.
3. "SHOULD", or "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications MUST be understood are carefully weighed before choosing a different course.
4. "SHOULD NOT", or "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications SHOULD be understood and the case carefully weighed before implementing any behavior described with this label.
5. "MAY", or "OPTIONAL", mean that an item is truly optional.

The terms "vendor" and "implementer" are used interchangeably in FIDO security certification documents. The term "implementer" is is preferred.

1.3 How to Read this Document

This section is non-normative.

This document is a combination of FIDO Alliance Security Requirements, Test Procedures, and Vendor Questionnaires. Each Requirement has the following elements:

- **Requirement Number**: Unique identifier for each Requirement
- **Specification**: The FIDO Specification for which this Requirement is applicable. For example, UAF, U2F, FIDO2, or UAF + U2F + FIDO2 (meaning it is applicable to UAF, U2F, and FIDO2)
- **Testing Style**: The testing style of the Security Requirement, explained in theTesting Style section below.
- **Requirement Level**: The Level to which the Requirement applies, explained in theSecurity Levels section below.

- **Security Measures**: The Security Measures from the FIDO Security References [FIDOSecRef]. These are mechanisms to implement in order to satisfy a Security Requirement .
- **Requirement**: The text of the Security Requirement - a description of necessary conditions to enforce security. It provides an exact description of what is to be evaluated and could be applied on all the life-cycle stages of the Authenticator.
- **Note**: An optional section that contains informative text to support the Requirement.
- **Relation to Partner Program**: This describes how the Requirement can be met by a particular Partner Program. Whether a requirement can be met through a Partner Program or not varies by Requirement, Security Level and the Partner Program. Partner Programs are explained in the Partner Programs section below.
- **Calibration**: The Calibration box reflects the required strength of the protection measures to meet the Requirement. The higher security levels generally require greater strength and more thorough evaluation. For example, for Common Criteria based programs higher security levels calibrate by require a higher attack potential be achieved.
- **Vendor Questionnaire**: The Vendor Questionnaire boxes are divided by Level, and reflect the information the Vendor must provide to prove the Requirement is met prior to the Security Evaluation. The Vendor shall complete the Vendor Questionnaire that corresponds to the Level of Authenticator Certification they are seeking.
- **Test Procedure**: The Test Procedure boxes are divided by Level, and describes how the Authenticator is to be evaluated. More specifically, it describes the actions the Test Proctor (e.g., for L1), or the Accredited Security Laboratory (e.g., for L2 and higher) must complete during the Security Evaluation to verify the Requirement is met. The Test Procedure will be followed that corresponds to the Level of Authenticator Certification indicated by the Vendor.
    - **Test Assurance Mode**: Each Test Procedure includes a Test Assurance Mode to provide additional clarification on how the Test Procedure will be performed. The Assurance Modes are explained in the Test Assurance Modes section below.

The following table is an example of the Requirement structure within this document:

No.	Requirement	Security Measures
[Requirement Number]	[Specification]; [Testing Style]; [Level] Requirement text. NOTE Note text. Relation to Partner Program **[Level] [Partner Program]**: Relation to Partner Program text. Calibration Calibration text. [Level] Vendor Questionnaire Vendor Questionnaire text. [Level] Test Procedure {Test Assurance Mode} Test Procedure text.	[Security Measures]

Example Requirement

1.4 Security Levels

All requirements apply to all **Security Levels** unless otherwise noted. If a requirement is marked "L<n> and higher" then it applies to level L<n> and all levels above L<n> and not to levels below L<n>.

Phrases starting with 'At L<n> ...' *refine* the requirement(s) stated above that apply in the scope of an L<n> certification.

1.5 Partner Programs

Partner Programs are the independent FIDO Certification Programs with which FIDO relies on to offer joint FIDO

Certification Programs to reduce the certification burden on Vendors. In this version, Partner Programs are relevant to certification levels 4 and 5. All vendors targetting L3 or L3+ certification MUST provide a mapping to Partner Program requirements. This MUST be based on the following table [FIDO-SR-Mapping-Table] provided by FIDO.

> NOTE
>
> This table is provided only as a guidance document for both vendors and labs to simplify evidence writing and evaluation tasks. Therefore, it is not intended to add or replace any of FIDO security requirements. This version of the table translates FIDO security requirements into Common Criteria (CC) Security Functional Requirements (SFR) and Security Assurance Requirements (SAR) and map these to the Java Card Open Configuration Protection Profile (PP) [JCPP], Security IC Platform PP [PP0084], FIPS 140-2 CM Validation [FIPS140-2] and FIDO U2F Authenticator PP [U2FPP]. Moreover, future work will cover additional Partner Programs endorsed by the security industry such as EMVCo and DSC PP and more.

> NOTE
>
> This version of the FIDO Security Requirements only accepts CC Partner Programs. Vendors having a FIPS 140-2 Cryptographic Module Validation could refer to this mapping table for re-using their evidence documentation as inputs for CC Partner Program evaluation when applicable.

1.6 Examples of Underlying Platforms

This section is non-normative.

DISCLAMER: The following examples are hypothetical realizations with various assumptions and the attack scenario is limited to physical probing of manipulative attacks.
Note that there might be other ways to attack the realization more easy (e.g. observing/side-channel-attack or semi-invasive/fault-injection-attack).

Therefore a systematic evaluation of the real realization is needed in order to determine the real and correct rating.

Example Cases	Rating-Result in Points	Rating-Result according CC V3	FIDO Level
Case 1: Basic CPU connected to RAM via simple PCB	8	No Rating	L1 - L2+
Case 2: Basic CPU connected to RAM via multilayer PCB with potting	11	No Rating	L1 - L2+
Case 3: CPU and RAM on the same die with absolutely no counter measures, internal integrity checks	24	Enhanced-Basic = up to AVA_VAN.3	L3
Case 4: TrustZone or SGX or hypervisor with RAM encryption & integrity check connected to RAM via simple PCB	23	Enhanced-Basic = up to AVA_VAN.3	L3
Case 5: Basic CPU connected to RAM via simple PCB self-destruct enclosure (not sure this is possible, but is fun to think about…)	21	Enhanced-Basic = up to AVA_VAN.3	L3
Case 6: CPU with RAM encryption & integrity check connected to RAM via simple PCB	23	Enhanced-Basic = up to AVA_VAN.3	L3
Case 7: Non-certified secure element	24	Enhanced-Basic = up to AVA_VAN.3	L3
Case 8: CPU and RAM in a stacked die package	24	Enhanced-Basic = up to AVA_VAN.3	L3
Case 9: CPU with PoP (package on package) connection to RAM	22	Enhanced-Basic = up to AVA_VAN.3	L3
Case 10: Standard TPM (CC EAL4+ moderate certified)	27	Moderate = up to AVA_VAN.4	L3+
Case 11: CC certified secure element	33	High = up to AVA_VAN.5	L3+

Table 2: Examples of underlying platforms and physical attacks

Reference for Rating in Points see [AttackPotentialSmartcards].

> NOTE
>
> With RAM we mean *memory* in general (including FLASH, EEPROM,…) in case information is stored there.

1.7 FIDO Specifications

Some requirements are prefaced by “(UAF)”, “(U2F)”, or “(FIDO2)”. These are applicability statements indicating that the requirement applies only to the UAF, U2F, or FIDO2 protocol families.

For requirements that relate to normative requirements of the UAF, U2F, or FIDO2 specifications, a reference is included citing the relevant section of the specifications. These references are included in square brackets, for example “[U2FRawMsgs], [Section 5.1]” refers to the U2F Authenticator specification, section 5.1.

1.8 Security Measures

All of the requirements end with a reference to the **security measures** that are supported by the requirement in question. These references are included within parentheses, for example “(SM-2)”. The security measure references are described in the the FIDO Security Reference document [FIDOSecRef].

1.9 Testing Style

Each requirement is also tagged with the testing style.

The following testing styles are included in this document:

- Documentation and Definition Requirements (**DaD**): These requirements are associated with the existence of documentation, thus are easy to confirm through simple checks.
- Generate and Verify Rationale Requirements (**GaVR**): These requirements are divided into three subtypes:
  - **GaVR-1**: Requirement that is nearly transparently verifiable, but which are expected to have the possibility of significant per-Authenticator variation.
  - **GaVR-2**: Requirement that pertains to disallowed functionality or functionality that can only occur in proscribed situations.
  - **GaVR-3**: Requirement where tester knowledge, skill and experience are significant factors in test efficacy.
- Transparently Verifiable Functional requirements (**TVFR**): These requirements are expected to be easy to confirm in almost all Authenticator designs, but there is some functional requirement to be verified.

1.9.1 Test Assurance Modes

Because GaVR and TVFR relate to functional requirements, there are different **test assurance mode**s that we can seek depending on the importance of the requirement in question. These are as follows:

- **A0**: The vendor asserts compliance to the requirement.
  - Guidance: An **assertion of compliance** is done through demonstration of the requirement during the Conformance Self-Validation or Interoperability Testing phases of FIDO Functional Certification. No Additional documentation is required.
- **A1**: The FIDO Security Secretariat confirms that there is a sufficient rationale that describes how the requirement is fulfilled.
  - Guidance: This **rationale** can be a detailed written description, architectural diagrams, a specially constructed document that addresses this particular requirement, or can be one or more existing design documents which, together, convince the tester that the requirement is fulfilled.
- **A2**: In addition to the testing for A0, the tester (FIDO Accredited Security Laboratory) additionally confirms that there is design documentation that describes how the requirement is fulfilled.
- **A3**: In addition to the testing for A2, the tester confirms that the Authenticator satisfies the requirement by targeted review of the implementation (by source / HDL / schematic code review).
  - Guidance: If this requirement has been verified as part of a separate FIPS 140-2 or Common Criteria validation effort for the Authenticator or one of its subcomponents, this verification can be used to fulfill the A3 assurance mode tests.
- **A4**: In addition to the testing for A3, the tester confirms that the Authenticator satisfies the requirement by exercising the Authenticator (through operational testing).

1.9.2 Test Procedures - Key Words

- **Review**: This is a high-level check to confirm that desired data or rationale is present. It is often followed by a verification task (see verify) to ensure the evidence meets the requirement. The reporting for this style of procedural verb is simple assertion and a reference to the document/section that satisfied the review.
- **Verify**: This is a more in-depth verification and/or analysis performed by the tester. The reporting for this style of procedural verb is more extensive, and requires that the tester outlines the steps and rationale used in the task.
- **Conduct**: The tester performs either some review procedure that was supplied by the vendor or a vulnerability assessment and a penetration testing. Note that vulnerability assessment and penetration testing SHALL follow the style of the relevant Partner Program. The tester MUST retain evidence that these procedures were followed, and SHOULD provide a high-level summary of the procedure and its results within the report.
- **Execute**: The tester runs a procedure which could be either a defined action or a sample test documented by the vendor. The tester MUST retain evidence of this procedure and SHOULD provide a high-level summary of the action and its results within the report.

2. Requirements

This section is normative.

2.1 Authenticator Definition and Derived Authenticator Requirements

The **FIDO Authenticator** (**Authenticator**, for short) is a set of hardware and software that implements the Authenticator portion of the FIDO UAF, FIDO U2F, or FIDO2 protocols. For the purpose of this requirements, the Authenticator is the set of hardware and software within the Authenticator boundary, as defined in the response to requirement 1.1.

We use the term **Authenticator Application** to refer to the entity that (a) is provided by the Authenticator vendor and (b) combines with the underlying **operating environment** (hardware and firmware) in a way that results in a FIDO Authenticator. This operating environment might be clearly separated from a high-level operating system (HLOS). In this case we call it "**Restricted Operating Environment**" (**ROE**). If such separation meets the requirements defined in [FIDORestrictedOperatingEnv], we call it **Allowed Restricted Operating Environment** (**AROE**).

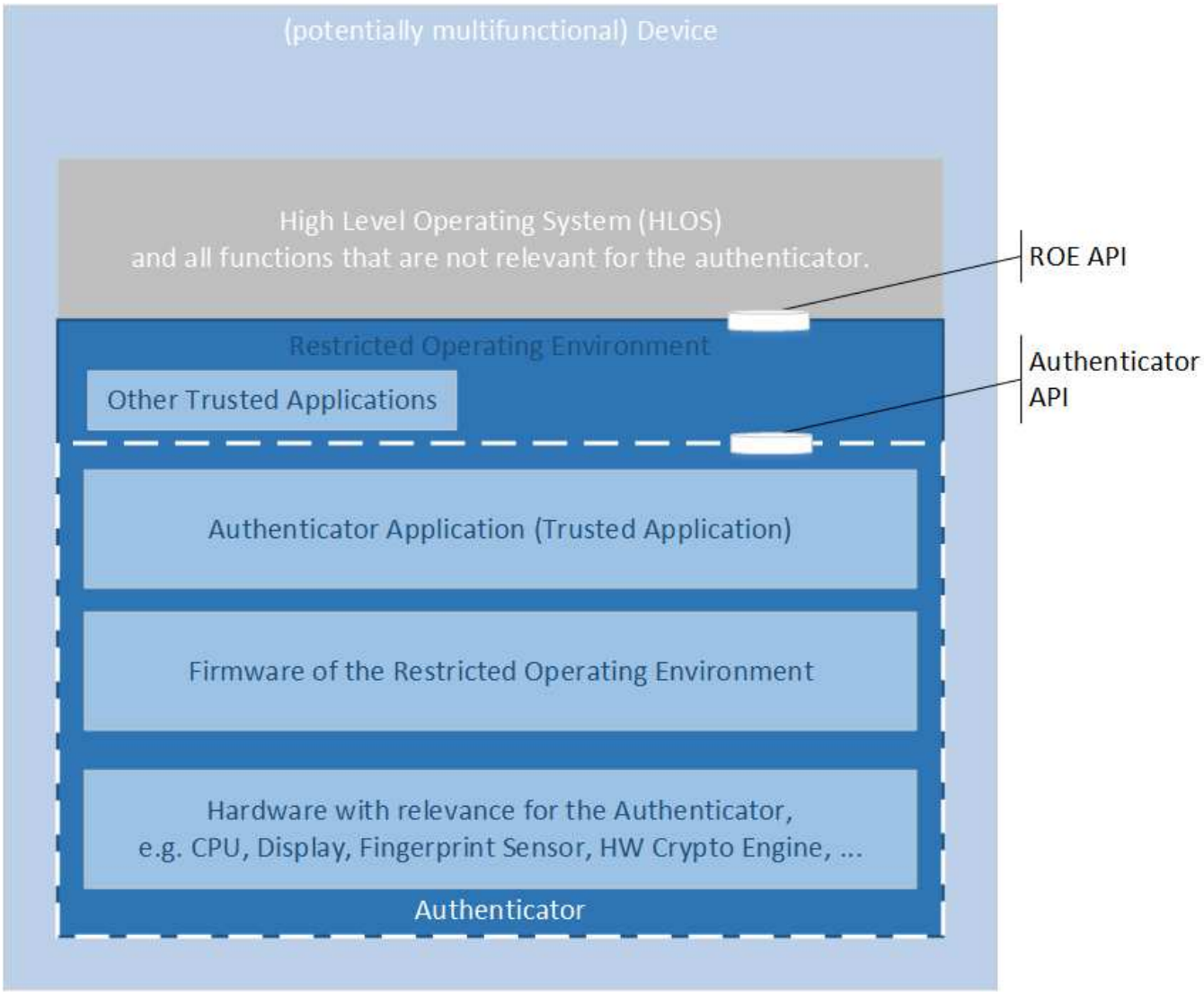

Fig. 1 Restricted Operating Environments Architectural Overview

At L1, the Restricted Operating Environment as used in the figure above might be identical with the HLOS plus underlying HW and doesn't need to be an Allowed Restricted Operating Environment (AROE).

At L2 and above the Restricted Operating Environment MUST be an Allowed Restricted Operating Environment according to [FIDORestrictedOperatingEnv], e.g. a Trusted Execution Environment or a Secure Element.

In these requirements, the term “FIDO Relevant” means “used to fulfill or support FIDO Security Goals or FIDO Authenticator Security Requirements”.

> NOTE
>
> For the certification levels L1 and L2 the Authenticator doesn't need to restrict the private authentication key (Uauth.priv) to signing valid FIDO messages only (see requirement 2.1.15 which is label L2+ and higher and higher). As a consequence, the generation of the to-be-signed object could be performed outside of the Authenticator.

No.	Requirement	Security Measures
	UAF + U2F + FIDO2; DaD; L1 and higher The vendor SHALL document an explicit **Authenticator boundary**. The Authenticator’s boundary SHALL include any hardware that performs or software that implements functionality used to fulfill FIDO Authenticator Security Requirements, or FIDO Relevant user verification, key generation, secure transaction confirmation display, or signature generation. If the Authenticator includes a software component, the boundary SHALL contain the processor that executes this software. If Transaction Confirmation Display is supported and the Metadata Statement related to this Authenticator claims Transaction Confirmation Display support with tcDisplay including the flag TRANSACTION_CONFIRMATION_DISPLAY_PRIVILEGED_SOFTWARE (0x0002), then the Transaction Confirmation Display MAY be implemented outside of an AROE - even when the Authenticator aims for a certification at L2 and higher. However, in such case the vendor SHALL document where and how Transaction Confirmation Display is implemented. The Authenticator boundary as defined by FIDO is comprised of the hardware and software where the Authenticator runs. The Authenticator Application by definition, is always inside the authenticator boundary. The vendor MUST describe the operational environment for the Authenticator Application, including any specific hardware or operating system requirements to completely define this boundary. The Authenticator always comprises hardware and software and the vendor SHALL describe the boundary. An Authenticator typically belongs to one of the 4 categories: 1. Authenticator Application running on some HLOS *without* an effective protection of the Authenticator Security Parameters against most other applications running in the same environment. 2. Authenticator Application running on some HLOS *with* an effective protection of the Authenticator Security Parameters against most other applications running in the same environment - without breaking the HLOS. 3. as #2, but having the Secret Authenticator Security Parameters protected by an AROE. 4. entire Authenticator is implemented in an AROE (i.e. typically qualifying for L2 and higher). For Authenticators falling under #1-3 above, the Authenticator is qualified for L1 Authenticator Certification only, and SHOULD refer to the L1 portions of this Requirements document. For Authenticators meeting #4, the Authenticator is qualified for L1 or above. It is up to the vendor to review the requirements in this document to determine the Level of Authenticator Certification they wish to complete. > NOTE > > The Vendor should provide a clear description of the HW, supported OS versions that the evaluation is covering. See below: > > - Name of the authenticator:	

No.		Security Measures
	• Hardware Type & Version: • Underlying Software Platform/OS: In addition, the vendor must provide a high-level physical and logical representation of the Authenticator security boundary. The documentation provided by the vendor should cover software attack protection and, if required, hardware attack protection.	
1.1	**Relation to Partner Program** **L3 Common Criteria**: A Security Target document MUST be provided (see [CC1V3-1R5]). This requirement is addressed by ASE_INT and ASE_SPD (see [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target document MUST be provided (see [CC1V3-1R5]). This requirement is addressed by ASE_INT and ASE_SPD (see [CC3V3-1R5]). **Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. At L1, the Authenticator vendor SHALL declare and describe to which of the above mentioned categories the Authenticator Application belongs. At L1, the vendor SHALL also describe what portions of functionality the Authenticator uses from any underlying operating environment that belongs to the Authenticator but that is not included in the Authenticator Application. **L2 Vendor Questionnaire** *Provide* the tester with documentation that specifies how the requirement above is met. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Mapping to Partner Program Requirements • Source Code **L1 Test Procedure** {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. **L2 Test Procedure** {A2} The tester SHALL *verify* that the documentation meets the requirement.	(SM-1, SM-9, SM-26)

No.	Requirement	Security Measures
1.2	**L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. UAF + U2F + FIDO2; DaD; L1 and higher The vendor SHALL document all FIDO Relevant security and cryptographic functions implemented within the Authenticator, both those on the “Allowed Cryptography List” [FIDOAllowedCrypto] and those not on this list. NOTE Some algorithms may only be allowed for certain Security Certification Levels. For example, not all cryptographic algorithms that are acceptable for L1 may be acceptable for L3. **Relation to Partner Program** **L3 Common Criteria**: A Security Target and a Development document MUST be provided (see [CC1V3-1R5]). This requirement is addressed by Class FCS and ADV (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target and a Development document MUST be provided (see [CC1V3-1R5]). This requirement is addressed by Class FCS and ADV (see [CC2V3-1R5] and [CC3V3-1R5]). **Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. At L1, the vendor SHALL mark the FIDO Relevant security and cryptographic functions implemented in the Authenticator but implemented *outside the Authenticator Application* (i.e. in the underlying OS or HW). **L2 Vendor Questionnaire** *Provide* the tester with documentation that specifies how the requirement above is met. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Mapping to Partner Program Requirements • Source Code	(SM-1, SM-9, SM-16, SM-26)

No.	Requirement	Security Measures
1.3	**L1 Test Procedure** {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. **L2 Test Procedure** {A2} The tester SHALL *verify* that the documentation meets the requirement. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. UAF + U2F + FIDO2; DaD; L1 and higher The vendor SHALL document where Authenticator User Private Keys (Uauth.priv) are stored, the structure of all KeyIDs/CredentialIDs and Key Handles used by the Authenticator, and explain how these private keys are related to the KeyIDs/CredentialIDs and Key Handles used by the Authenticator. **Relation to Partner Program** **L3 Common Criteria**: Development documentation MUST be provided This requirement is addressed by Class ADV (see [CC3V3-1R5]). **L3+ Common Criteria**: Development documentation MUST be provided This requirement is addressed by Class ADV (see [CC3V3-1R5]). **Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. At L1, the private keys, KeyIDs/CredentialIDs etc. that are generated outside the Authenticator Application SHALL be documented, but their internal structure does not need to be explained in detail. **L2 Vendor Questionnaire** *Provide* the tester with documentation that specifies how the requirement above is met. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Mapping to Partner Program Requirements • Source Code	(SM-1, SM-6, SM-26)

No.	Requirement	Security Measures
1.4	**L1 Test Procedure** {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. **L2 Test Procedure** {A2} The tester SHALL *verify* that the documentation meets the requirement. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. UAF + FIDO2; DaD; L1 and higher The vendor SHALL document an Authenticator as a first-factor Authenticator or a second-factor Authenticator. [UAFAuthnrCommands], [Section 6.3.4] and [FIDOGlossary] entries "Authenticator, 1stF / First Factor" and "Authenticator, 2ndF / Second Factor". **Relation to Partner Program** **L3 Common Criteria**: a Security Target MUST be provided (see [CC1V3-1R5]). This requirements is addressed by ASE_INT (see [CC3V3-1R5]). **L3+ Common Criteria**: a Security Target MUST be provided (see [CC1V3-1R5]). This requirements is addressed by ASE_INT (see [CC3V3-1R5]). **Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. At L1, in addition to the rationale provided by the vendor, this requirement MUST be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required. **L2 Vendor Questionnaire** *Provide* the tester with documentation that specifies how the requirement above is met. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Mapping to Partner Program Requirements • Source Code **L1 Test Procedure**	(SM-26)

No.	Requirement	Security Measures
	{A0} The Security Secretariat SHALL *verify* the requirement during Interoperability Testing.	

L2 Test Procedure

{A2} The tester SHALL *verify* that the documentation meets the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

UAF + FIDO2; TVFR; L1 and higher

If the Authenticator is a second-factor Authenticator, then the Authenticator SHALL NOT store user names (UAF) / PublicKeyCredentialUserEntity (FIDO2) inside a Raw Key Handle [UAFAuthnrCommands], [Section 5.1]. A cryptographically wrapped Raw Key Handle is called Key Handle.

Relation to Partner Program

L3 Common Criteria: A Security Target and a Tests document MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FPR_ANO.2 and Class ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target and a Tests document MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FPR_ANO.2 and Class ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

L1 Vendor Questionnaire

Is this requirement applicable to the Authenticator? If **No**, then *describe* why.

If Yes, *Provide* the Security Secretariat with a description of how the requirement above is met.

L2 Vendor Questionnaire

Is this requirement applicable to the Authenticator? If **No**, then *describe* why.

If Yes, *Describe* how this requirement can be verified through documentation review. Please provide explicit design document references.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

1.5 (SM-23)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

No.	Requirement	Security Measures
1.6	**L1 Test Procedure** {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. **L2 Test Procedure** {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. UAF + FIDO2; TVFR; L1 and higher Supporting Transaction Confirmation is OPTIONAL for Authenticators. If the Authenticator supports Transaction Confirmation Display, then it SHALL hash the Transaction Content using an Allowed Hashing Cryptographic Function ([UAFAuthnrCommands] Section 6.3.4, [WebAuthn] Section 10.2 and 10.3). **Relation to Partner Program** **L3 Common Criteria**: A Security Target, a Development and a Tests document MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_COP.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target, a Development and a Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_COP.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. **L2 Vendor Questionnaire** *Describe* how this requirement can be verified through documentation review. Please provide explicit design document references. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation	(SM-16)

No.	Requirement	Security Measures

- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF+FIDO2; TVFR; L1 and higher

If the Authenticator uses the KHAccessToken method of binding keys to apps, then when responding to a “Register”, “Sign”, or “Deregister” command which includes the AppID/RP ID, the Authenticator SHALL use an Allowed Hashing or Data Authentication Cryptographic Function to mix the ASM-provided KHAccessToken and AppID/RP ID.

If the Authenticator uses an alternative method of binding keys to apps, the vendor SHALL describe why this method provides equivalent security. Equivalent security means, (1) it prevents other apps (not originating from the same RP) from using the key and (2) in the case of bound Authenticators, it prevents other FIDO Clients of triggering the use of that key, and (3) it may rely on the underlying HLOS platform to work as expected.

Relation to Partner Program

L3 Common Criteria: A Security Target, a Development and a Tests document MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_IFC.1, FDP_IFF.1, FCS_COP.1 Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, a Development and a Tests document MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_IFC.1, FDP_IFF.1, FCS_COP.1 Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

No.	Requirement	Security Measures
1.7	**Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. **L2 Vendor Questionnaire** *Describe* how this requirement can be verified through documentation review. Please provide explicit design document references. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L1 Test Procedure** {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. **L2 Test Procedure** {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. UAF; TVFR; L1 and higher If the Authenticator uses the KHAccessToken method of binding keys to apps, then the Authenticator SHALL NOT process a “Deregister” command prior to validating the KHAccessToken. [UAFAuthnrCommands], [Section 6.4.4] **Relation to Partner Program** **L3 Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see	(SM-16)

No.	Requirement	Security Measures
	[CC1V3-1R5]). This requirement is addressed by FDP_IFC.1, FDP_IFF.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	
	L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FDP_IFC.1, FDP_IFF.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	
	Calibration No calibration required.	
	L1 Vendor Questionnaire *Provide* the Security Secretariat with a rationale of how the requirement above is met.	
	L2 Vendor Questionnaire *Describe* how this requirement can be verified through documentation review. Please provide explicit design document references.	
1.8	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	(SM-13)
	L3+ Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	
	L1 Test Procedure {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.	
	L2 Test Procedure {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.	
	L3 Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	
	L3+ Test Procedure	

No.	Requirement	Security Measures
1.9	The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. UAF + FIDO2; TVFR; L1 and higher Supporting Transaction Confirmation is OPTIONAL for Authenticators. If the Authenticator supports Transaction Confirmation Display, then it SHALL display the transaction content supplied in the “Sign” command. [UAFAuthnrCommands], Section 6.3.4, [FIDOGlossary], and [WebAuthn] Sections 10.2 and 10.3. If the Metadata Statement related to this Authenticator claims Transaction Confirmation Display support with tcDisplay including the flag TRANSACTION_CONFIRMATION_DISPLAY_PRIVILEGED_SOFTWARE (0x0002), the Transaction Confirmation Display MAY be implemented outside of an AROE. If tcDisplay includes the flag TRANSACTION_CONFIRMATION_DISPLAY_TEE, or TRANSACTION_CONFIRMATION_DISPLAY_HARDWARE, then the Transaction Confirmation Display SHALL be implemented inside the AROE as part of the Authenticator. **Relation to Partner Program** **L3 Common Criteria**: A Security Target, Development and Tests document MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FDP_IFC.1, FDP.IFF.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target, Development and Tests document MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FDP_IFC.1, FDP.IFF.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. At L1, in addition to the rationale provided by the vendor, this requirement MUST be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required. **L2 Vendor Questionnaire** Is this requirement applicable to the Authenticator? If **No**, then *describe* why. If **Yes**, *describe* how this requirement can be verified through documentation review. Please provide explicit design document references. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: - High Level Design Documentation - Tests Documents - Mapping to Partner Program Requirements - Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the	(SM-10)

No.	Requirement	Security Measures

following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A0} The Security Secretariat SHALL *verify* the requirement during Interoperability Testing.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; GaVR-3; L1 and higher

Authenticators SHALL validate data input to the Authenticator to defend against buffer overruns, stack overflows, integer under/overflow or other such invalid input-based attack vectors.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FAU_ARP.1, FDP_ITC.1, FDP_IFC.1, FDP_MSA.3, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FAU_ARP.1, FDP_ITC.1, FDP_IFC.1, FDP_MSA.3, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

L1: At L1, the Authenticator Application needs to verify only the inputs to the Authenticator Application before they are processed further by the underlying operating environment.

L2: At L2, this requirement SHALL be applied to all inputs that can impact FIDO Security Goals or fulfillment of the FIDO Authenticator Security Requirements, including all those inputs into the FIDO implementation. All inputs to the Authenticator, including those not directly related to the FIDO implementation such as general inputs to the AROE, SHOULD meet this requirement.

L3: At L3, this requirement SHALL be met for all inputs to the Authenticator. At L3, the protection SHALL be strong enough to be protected against *enhanced-basic* effort software and hardware attacks

No.	Requirement	Security Measures
	[AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.3 or higher vulnerability analysis (see [CEMV3-1R5]).	
	L3+: At L3+, this requirement SHALL be met for all inputs to the Authenticator. At L3+, the protection SHALL be strong enough to be protected against *moderate* or *high* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.4 or higher vulnerability analysis (see [CEMV3-1R5]).	
1.10	NOTE At L2, L3 and L3+ the entire AROE is likely to be within the authenticator boundary and thus part of the Authenticator. Examples of inputs directly related to the FIDO authenticator are FIDO protocol messages and FIDO authenticator configuration inputs. Examples of inputs to the AROE that are not directly related to FIDO are calls to configure the AROE itself or get status from the AROE itself. if the AROE can load and run an application like a signed ELF file, that signed ELF file is an input to the authenticator and the code for verifying and loading the ELF file are subject to this requirement. This is because a malicious ELF file could allow an attacker to compromise the AROE kernel and thus compromise FIDO code running on the AROE. At L2, L3 and L3+ the inputs to the Authenticator are primarily inputs that come from the less-secure or non-secure world outside the AROE. These are typically calls that come from the High-Level or Rich OS. Inputs between modules and subsystems within the AROE are not considered inputs for this requirement. Data read by the AROE from unsecured storage is also considered an input to the AROE.	(SM-28)

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

L2 Vendor Questionnaire

Provide a rationale that the Authenticator validates all data input to the Authenticator.

Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

No.	Requirement	Security Measures
	L2 Test Procedure {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements. ~~UAF + FIDO2; DaD; L2+ and higher~~ If the Authenticator has a Transaction Confirmation Display, the AppID/RP ID SHALL be displayed to the user when a “Register”, “Sign”, or “Deregister” (UAF) command is received. Displaying the AppID/RP ID SHALL meet the same security characteristics that apply to the Transaction Confirmation Display (see requirement 1.9). **Relation to Partner Program** **L3 Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FDP_IFC.1, FDP_IFF.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FDP_IFC.1, FDP_IFF.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **Calibration** No calibration required.	
1.11	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:	(SM-10)

No.	Requirement	Security Measures
	• High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements	

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

2.2 Key Management and Authenticator Security Parameters

2.2.1 Documentation

No.	Requirement	Security Measures
2.1.1	UAF + U2F + FIDO2; DaD; L1 and higher The vendor SHALL document all **Authenticator Security Parameters** (ASPs). Data parameters used by or stored within the Authenticator which are FIDO Relevant are called **Authenticator Security Parameter**. These SHALL, at minimum, include all FIDO user verification reference data, FIDO biometric data, Key Handle Access Tokens, **User Verification Token**s (see [UAFAuthnrCommands], Section 5.3 and [FIDOGlossary]), signature or registration operation counters, FIDO Relevant cryptographic keys, and FIDO relevant Allowed Random Number Generator state data. Biometric data is defined as raw captures off the sensor, stored templates, candidate match templates, and any intermediate forms of biometric data. Biometric data not used with FIDO is excluded.	(SM-1, SM-2, SM-6, SM-13, SM-15, SM-16, SM-26)

Relation to Partner Program

L3 Common Criteria: A Security Target document MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ASE_SPD (see[CC3V3-1R5]).

L3 Common Criteria: A Security Target document MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ASE_SPD (see[CC3V3-1R5]).

Calibration

No calibration required.

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

L2 Vendor Questionnaire

Provide the tester with documentation that specifies how the requirement above is met.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

No.	Requirement	Security Measures
	• High Level Design Documentation • Mapping to Partner Program Requirements **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Mapping to Partner Program Requirements **L1 Test Procedure** {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. **L2 Test Procedure** {A2} The tester SHALL *verify* that the documentation meets the requirement. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement.	
2.1.2	UAF + U2F + FIDO2; DaD; L1 and higher For each Authenticator Security Parameter, the vendor SHALL document the protections that are implemented for this parameter in order to support the FIDO Authenticator Security Goals or FIDO Authenticator Security Requirements, the location where this parameter is stored, how the parameter is protected in each storage location, how and when the parameter is input or output from the Authenticator, in what form the parameter is input or output, and when (if ever) the parameter is destroyed. Those Authenticator Security Parameters whose confidentiality MUST be protected in order to support the FIDO Security Goals or FIDO Authenticator Security Requirements SHALL be documented as "**Secret Authenticator Security Parameters**"; these SHALL, at minimum, include any of the following that are FIDO Relevant: secret and private keys, Allowed Random Number Generators' state data, FIDO user verification reference data, and FIDO biometric data. **Relation to Partner Program** **L3 Common Criteria**: A Security Target and Development documents MUST be provided (see[CC1V3-1R5]). This requirement is addressed by FDP_IFF.1 and Class ADV (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target and Development documents MUST be provided (see[CC1V3-1R5]). This requirement is addressed by FDP_IFF.1 and Class ADV (see [CC2V3-1R5] and [CC3V3-1R5]). **Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. At L1, the vendor SHALL describe the reliance of the Authenticator Application on the underlying operating environmentfor those Authenticator Security Parameters which are not fully maintained in the Authenticator Application. **L2 Vendor Questionnaire**	(SM-1, SM-2, SM-6, SM-13, SM-15, SM-16, SM-26)

No.	Requirement	Security Measures

Provide the tester with documentation that specifies how the requirement above is met.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Mapping to Partner Program Requirements

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Mapping to Partner Program Requirements

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *verify* that the documentation meets the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

UAF + U2F + FIDO2; DaD; L1 and higher

For each Authenticator Security Parameter that is a cryptographic key that is generated, used, or stored within the Authenticator, the vendor SHALL document how this key is generated, whether the key is unique to a particular Authenticator or shared between multiple Authenticators, and the key's claimed cryptographic strength. This claimed cryptographic strength SHALL NOT be larger than the maximal allowed claimed cryptographic strength for the underlying algorithm, as specified in the "Allowed Cryptography List" [FIDOAllowedCrypto]. If the key is used with an algorithm not listed on the "Allowed Cryptography List" [FIDOAllowedCrypto], then the claimed cryptographic strength for this key SHALL be zero.

> NOTE
>
> This requirement interacts with requirement 5.4 as the cryptographic strength of a key might get degraded - depending on potential side channel attacks - slightly each time the key is used.

Relation to Partner Program

L3 Common Criteria: A Security Target and Development documents MUST be provided (see[CC1V3-1R5]).

This requirement is addressed by FCS_CKM and Class ADV (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target and Development documents MUST be provided (see[CC1V3-1R5]).

This requirement is addressed by FCS_CKM and Class ADV (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

No.	Requirement	Security Measures
2.1.3	L1 Vendor Questionnaire *Provide* the Security Secretariat with a rationale of how the requirement above is met. At L1, the vendor SHALL describe the reliance of the Authenticator Application on the underlying operating environment for those Authenticator Security Parameters (where stored, how protected, ...) which are not fully maintained in the Authenticator Application. If a cryptographic key is generated using an RNG with an unknown cryptographic strength, the cryptographic strength of that key is unknown. L2 Vendor Questionnaire *Provide* the tester with documentation that specifies how the requirement above is met. L3 Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Mapping to Partner Program Requirements L3+ Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Mapping to Partner Program Requirements L1 Test Procedure {A2} The tester SHALL *verify* that the documentation meets the requirement. L2 Test Procedure {A2} The tester SHALL *verify* that the documentation meets the requirement. L3 Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement. L3+ Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement. ~~UAF + U2F + FIDO2; DaD; L1 and higher~~ The vendor SHALL document the Authenticator's **Overall Claimed Cryptographic Strength**; the Overall Authenticator Claimed Cryptographic Strength SHALL be less than or equal to the claimed cryptographic strength of all the Authenticator Security Parameters that are cryptographic keys. NOTE The security strength is a number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system. It is specified in bits and it is often a value like 80, 112, 128, 192, 256. Relation to Partner Program **L3 Common Criteria**: A Security Target and Operation User Guidance MUST be provided (see [CC1V3-1R5]). This requirement is addressed by ASE_SPD, FCS_COP.1 and AGD_OPE.1 (see [CC2V3-1R5] and [CC3V3-1R5]).	(SM-1, SM-2, SM-6, SM-13, SM-16, SM-26)

No.	Requirement	Security Measures
2.1.4	**L3+ Common Criteria**: A Security Target and Operation User Guidance MUST be provided (see [CC1V3-1R5]). This requirement is addressed by ASE_SPD, FCS_COP.1 and AGD_OPE.1 (see [CC2V3-1R5] and [CC3V3-1R5]).	(SM-1, SM-16, SM-26)

Calibration

L1: At L1, if the security strength for the RNG is not known, an unknown Overall Claimed Cryptographic Strength SHALL be assumed - which is allowed at L1.

L2: At L2, the Authenticator's Overall Claimed Cryptographic Strength SHALL at least be greater than or equal to 100 bits and it SHOULD be greater than or equal to 112 bits.

L3: At L3, the Authenticator's Overall Claimed Cryptographic Strength SHALL at least be greater than or equal to 100 bits and it SHOULD be greater than or equal to 112 bits.

L3+: At L3+, the Authenticator's Overall Claimed Cryptographic Strength SHALL at least be greater than or equal to 100 bits and it SHOULD be greater than or equal to 112 bits.

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

L2 Vendor Questionnaire

Provide the tester with documentation that specifies how the requirement above is met.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Operation User Guidance
- Mapping to Partner Program Requirements

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Operation User Guidance
- Mapping to Partner Program Requirements

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *verify* that the documentation meets the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

All Authenticator Security Parameters within the Authenticator SHALL be protected against modification and

No.	Requirement	Security Measures
	substitution.	
2.1.5	**Relation to Partner Program** **L3 Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FPT_PHP.3, FMT_MTD.1, FPT_TST.1, FDP_SDI.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FPT_PHP.3, FMT_MTD.1, FPT_TST.1, FDP_SDI.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **Calibration** **L1**: At L1, the Authenticator Application SHALL follow best security practices specific to the underlying operating environment for protecting the Authenticator Security Parameters against being modified or substituted by (1) the user and (2) other applications. Due to the nature of L1 it is acceptable for the Authenticator Application to rely on the underlying operating environment for protecting the Authenticator Security Parameters against other applications running in the same operating environment. **L2**: At L2, the requirement SHALL be fulfilled by mechanisms functioning entirely inside the AROE. **L3**: At L3, the protection SHALL be strong enough to be protected against *enhanced-basic* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.3 or higher vulnerability analysis (see [CEMV3-1R5]). **L3+**: At L3+, the protection SHALL be strong enough to be protected against *moderate* or *high* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.4 or higher vulnerability analysis (see [CEMV3-1R5]). **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. **L2 Vendor Questionnaire** *Provide* a rationale that all Authenticator Security Parameters within the Authenticator are protected against modification and substitution. *Provide* a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire**	(SM-1, SM-6, SM-13, SM-15, SM-16)

No.	Requirement	Security Measures

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

UAF; U2F; FIDO2; GaVR-3; L1 and higher

All Secret Authenticator Security Parameters within the Authenticator SHALL be protected against unauthorized disclosure.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_ITT.1, FTP_ITT.1, FDP_IFC.1, FPT_PHP.3, FPR_UNO.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_ITT.1, FTP_ITT.1, FDP_IFC.1, FPT_PHP.3, FPR_UNO.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

L1: At L1, the Authenticator Application SHALL follow best security practices specific to the underlying operating environment for protecting the Authenticator Security Parameters against being modified or substituted by (1) the user and (2) other applications.

At L1, the Authenticator Application (either by implementing appropriate protection mechanisms directly in the Authenticator Application or by leveraging the underlying operating environment for implementing those) SHALL protect the Secret Authenticator Security Parameters from being disclosed to other application running in the same operating environment. If the Authenticator Application cannot leverage mechanisms of the underlying operating environment for that, it SHALL at least store such parameters in

No.	Requirement	Security Measures
	encrypted form such that the decryption key is not available to the other applications running in the same operating environment. For example, by using a user provided secret to be entered or a key derived from some biometric at startup of the Authenticator Application using a best practice key derivation function (for converting a low entropy password into a cryptographic key, e.g. according to [SP800-132]).	
	L2: At L2, the requirement SHALL be fulfilled by mechanisms functioning entirely inside the AROE.	
	L3: At L3, the protection SHALL be strong enough to be protected against *enhanced-basic* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.3 or higher vulnerability analysis (see [CEMV3-1R5]).	
	L3+: At L3+, the protection SHALL be strong enough to be protected against *moderate* or *high* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.4 or higher vulnerability analysis (see [CEMV3-1R5]).	
	L1 Vendor Questionnaire *Provide* the Security Secretariat with a rationale of how the requirement above is met.	
2.1.6	L2 Vendor Questionnaire *Provide* a rationale that all Secret Authenticator Security Parameters within the Authenticator are protected against unauthorized disclosure. *Provide* a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.	(SM-1, SM-13, SM-16)
	L3 Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	
	L3+ Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	
	L1 Test Procedure {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.	
	L2 Test Procedure {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.	
	L3 Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	

No.	Requirement	Security Measures
	The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.	

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

UAF + U2F + FIDO2; TVFR; L1 and higher

The Authenticator SHALL use an Allowed Data Authentication, Signature, or Key Protection Cryptographic Function to protect any externally-stored Authenticator Security Parameters against modification or the replay of stale (but possibly previously authenticated) data.

> NOTE
>
> In this requirement, externally-stored refers to parameters stored outside of the Authenticator boundary. For example, cloud storage services.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, FDP_ACC.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5])

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, FDP_ACC.1 Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5])

Calibration

No calibration required.

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

L2 Vendor Questionnaire

Describe how this requirement can be verified through documentation review. Please provide explicit design document references.

2.1.7 **L3 Vendor Questionnaire** (SM-1, SM-6, SM-13, SM-15, SM-16, SM-25)

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

No.	Requirement	Security Measures

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; TVFR; L1 and higher

The Authenticator SHALL protect any externally-stored Secret Authenticator Security Parameters using an Allowed Key Protection Cryptographic Function. [UAFAuthnrCommands], [Sections 5.1, 6.3.4] for RawKeyHandles.

Relation to Partner Program

L3 Common Criteria: A Security Taget, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, FDP_ACC.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Taget, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, FDP_ACC.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

L2 Vendor Questionnaire

No.	Requirement	Security Measures
	Describe how this requirement can be verified through documentation review. Please provide explicit design document references.	
2.1.8	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L1 Test Procedure** {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. **L2 Test Procedure** {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. ~~UAF + U2F + FIDO2; TVFR; L1 and higher~~ Any key used with an Allowed Key Protection Cryptographic Function to protect an externally-stored secret or private key which is an Authenticator Security Parameter SHALL have a claimed cryptographic strength greater than or equal to the claimed cryptographic strength of the key being wrapped. **Relation to Partner Program** **L3 Common Criteria**: Security Target, Development, Tests and Preparative Procedures Guidance documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_COP.1, AGD_PRE.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: Security Target, Development, Tests and Preparative Procedures Guidance documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_COP.1, AGD_PRE.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	(SM-1, SM-6, SM-13, SM-15, SM-16, SM-25)

No.	Requirement	Security Measures
2.1.9	**Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. At L1, externally-stored means stored outside the Authenticator boundary. In the case of L1 this Authenticator boundary includes the underlying operating environment. **L2 Vendor Questionnaire** *Describe* how this requirement can be verified through documentation review. Please provide explicit design document references. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Guidance Documents • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Guidance Documents • Mapping to Partner Program Requirements • Source Code **L1 Test Procedure** {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. **L2 Test Procedure** {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. UAF + U2F + FIDO2; TVFR; L1 and higher	(SM-1, SM-6, SM-16, SM-25)

No.	Requirement	Security Measures
2.1.10	Authenticators might offload the persistent storage of key material to components outside the Authenticator boundary if they cryptographically wrap it appropriately. Such structure containing cryptographically wrapped key material or information related to keys is called **Key Handle containing a key** (in [WebAuthn] the term Credential ID is used instead of Key Handle). If the Authenticator uses such **Key Handle** approach, the Authenticator SHALL verify that any Key Handle containing a key provided to the Authenticator was generated by that Authenticator using an Allowed Data Authentication or Signature Cryptographic Function; if not, then no signature using this key SHALL be generated. [U2FRawMsgs], [Section 5.1] and [UAFAuthnrCommands], [Annex A Security Guidelines, entry Wrap.sym]. **Relation to Partner Program** **L3 Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_COP.1, FMT_MTD.3, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_COP.1, FMT_MTD.3, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **Calibration** **L1**: At L1, this Authenticator boundary includes the underlying operating environment. **L2**: No calibration required. **L3**: No calibration required. **L3+**: No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. **L2 Vendor Questionnaire** *Describe* how this requirement can be verified through documentation review. Please provide explicit design document references. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation	(SM-1, SM-2, SM-16, SM-25, SM-27)

No.	Requirement	Security Measures

- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF; TVFR; L1 and higher

If the Authenticator supports the KHAccessToken [UAFAuthnrCommands] method of binding keys to apps, then the Authenticator SHALL verify that the supplied KHAccessToken is associated with the referenced Key Handle prior to using that Key Handle to generate a signature; if not, then no signature associated with this Key Handle SHALL be generated. [UAFAuthnrCommands], [Section 6.3.4].

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, FDP_IFF, FDP_IFC, FIA_USB.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, FDP_IFF, FDP_IFC, FIA_USB.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

L2 Vendor Questionnaire

Describe how this requirement can be verified through documentation review. Please provide explicit design document references.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the

No.	Requirement	Security Measures
2.1.11	following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	(SM-13)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; TVFR; L1 and higher

If the Authenticator supports the Key Handle approach, then the Authenticator SHALL verify that any Key Handle containing a key provided to the Authenticator is associated with the application parameter (U2F) or AppID (UAF) or RP ID (FIDO2) by using an Allowed Data Authentication or Signature Cryptographic Function; if not, then no signature using this key SHALL be generated. [U2FRawMsgs], [Section 5.1] and [UAFAuthnrCommands], [Section 6.3.4].

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, FDP_IFF, FDP_IFC, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, FDP_IFF, FDP_IFC, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No.	Requirement	Security Measures
	No calibration required.	

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

L2 Vendor Questionnaire

Describe how this requirement can be verified through documentation review. Please provide explicit design document references.

No.	Requirement	Security Measures
2.1.12	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	(SM-1, SM-2, SM-16, SM-25, SM-27)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; GaVR-1; L1 and higher

The Authenticator SHALL generate an independent User Authentication Key for each registration [UAFAuthnrCommands], [Section 6.2.4].

> NOTE
>
> Any User Authentication Key (Uauth) SHALL only be used for authenticating one user account to one particular Relying Party.

No.	Requirement	Security Measures
	Relation to Partner Program **L3 Common Criteria**: A Security Target, Development and Tests document MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_COP.1, FCS_RNG, FCS_CKM, FDP_IFF, FDP_IFC, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target, Development and Tests document MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_COP.1, FCS_RNG, FCS_CKM, FDP_IFF, FDP_IFC, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	
	Calibration No calibration required.	
	L1 Vendor Questionnaire *Provide* the Security Secretariat with a rationale of how the requirement above is met.	
	L2 Vendor Questionnaire *Provide* the tester with documentation that specifies how the requirement above is met.	
2.1.13	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	(SM-1, SM-2, SM-27)
	L3+ Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	
	L1 Test Procedure {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.	
	L2 Test Procedure {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.	
	L3 Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	
	L3+ Test Procedure	

No.	Requirement	Security Measures
	The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	

UAF + U2F + FIDO2; TVFR; L2 and higher

The Authenticator SHALL support Full Basic attestation (or an attestation method with equal or better security), or Attestation CA [WebAuthn] section 6.3.3, or ECDAA attestation [FIDOEcdaaAlgorithm].

The Attestation Private Key SHALL only be used to sign well-formed FIDO attestation objects.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, FDP_IFF, FDP_IFC, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, FDP_IFF, FDP_IFC, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

L2 Vendor Questionnaire

Describe how this requirement can be verified through documentation review. Please provide explicit design document references.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

2.1.14 (SM-3)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

No.	Requirement	Security Measures
	The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; TVFR; L2+ and higher

All Authenticator User Private Keys (Uauth.priv) SHALL only be usable for generating well-formed FIDO signature assertions. [U2FImplCons], [Section 2.7] and [UAFAuthnrCommands], [Section 5.2].

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests document MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_IFF, FDP_IFC, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests document MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_IFF, FDP_IFC, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

2.1.15 (SM-1)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

No.	Requirement	Security Measures
2.1.16	**L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. UAF + U2F + FIDO2; TVFR; L1 and higher In the event that an Authenticator Security Parameter is “destroyed” it is SHALL be made permanently unavailable so it can never be read or used again. NOTE The means by which this is accomplished is implementation and level dependent. It may by simply deleting it, overwriting it, destroying the key material used to encrypt it or other. NOTE The purpose of this requirement is primarily so that a factory reset carried out by an end user before they sell or dispose of their device giving assurance that the new owner cannot re instate authentication keys. **Relation to Partner Program** **L3 Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_CKM.4, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_CKM.4, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **Calibration** **L1**: At L1, the Authenticator Application SHALL follow best security practices specific to the underlying operating environment for protecting the Authenticator Security Parameters against being recovered and used. **L2**: At L2, the requirement SHALL be fulfilled by mechanisms functioning entirely inside the AROE. **L3**: At L3, the means for making the Authenticator Security Parameter permanently unavailable SHALL be strong enough to be protected against enhanced-basic effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.3 or higher vulnerability analysis (see [CEMV3-1R5]). **L3+**: At L3+, the means for making the Authenticator Security Parameter permanently unavailable SHALL be strong enough to be protected against moderate or high effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.4 or higher vulnerability analysis (see [CEMV3-1R5]). **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met.	(SM-1, SM-24)

No.	Requirement	Security Measures

L2 Vendor Questionnaire

Describe how this requirement can be verified through documentation review. Please provide explicit design document references.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; TVFR; L2 and higher

Authenticators might support a function allowing the user resetting the Authenticator to the original (factory) state, i.e. deleting all user specific information. This process is called **factory reset** in this document.

In the event of a factory reset, the Authenticator SHALL destroy all User-specific Secret Authenticator Security Parameters other than any Allowed Random Number Generator's state.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests document MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_IFF.1, FMT_MSA.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

No.	Requirement	Security Measures
	L3+ Common Criteria: A Security Target, Development and Tests document MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FDP_IFF.1, FMT_MSA.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	

Calibration

No calibration required.

L2 Vendor Questionnaire

Describe how this requirement can be verified through documentation review. Please provide explicit design document references.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

2.1.17		(SM-1, SM-18, SM-19)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; TVFR; L1 and higher

Any time the Authenticator generates an Authenticator Security Parameter which is a key for use with an algorithm specified in the “Allowed Cryptography List” [FIDOAllowedCrypto], the Authenticator SHALL generate keys as required by the standard referenced in the “Allowed Cryptography List” [FIDOAllowedCrypto] for that algorithm.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests MUST be provided (see [CC1V3-

No.	Requirement	Security Measures
	1R5])..	
	This requirement is addressed by FCS_CKM.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	
	L3+ Common Criteria: A Security Target, Development and Tests MUST be provided (see [CC1V3-1R5])..	
	This requirement is addressed by FCS_CKM.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	
	Calibration No calibration required.	
	L1 Vendor Questionnaire *Provide* the Security Secretariat with a rationale of how the requirement above is met.	
	L2 Vendor Questionnaire *Describe* how this requirement can be verified through documentation review. Please provide explicit design document references.	
2.1.18	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	(SM-1, SM-16, SM-21)
	L3+ Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	
	L1 Test Procedure {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.	
	L2 Test Procedure {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.	
	L3 Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	
	L3+ Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement.	

No.	Requirement	Security Measures
	The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	

UAF + U2F + FIDO2; GaVR-1; L1 and higher

Any wrapped FIDO biometric data and FIDO user verification reference data that is output from the Authenticator SHALL only be able to be unwrapped by the Authenticator that produced this data.

> NOTE
>
> Cryptographic Collision would be an exception.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests document MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_ACC.1, FDP_ACF.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests document MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_ACC.1, FDP_ACF.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

L2 Vendor Questionnaire

Provide a rationale for how the requirement above is met.

Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.

2.1.19

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

(SM-27)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

No.	Requirement	Security Measures
2.1.20	**L1 Test Procedure** {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. **L2 Test Procedure** {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. UAF + U2F + FIDO2; GaVR-1; L1 and higher Any wrapped Authenticator User Private Key (UAuth.priv) that is output from the Authenticator SHALL only be able to be unwrapped by the Authenticator that produced this data. **Relation to Partner Program** **L3 Common Criteria**: A Security Target, Development and Tests document MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FDP_ACC.1, FDP_ACF.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target, Development and Tests document MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FDP_ACC.1, FDP_ACF.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. **L2 Vendor Questionnaire** *Provide* a rationale for how the requirement above is met. *Provide* a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents	(SM-1, SM-6, SM-26)

No.	Requirement	Security Measures

- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

2.2.2 Random Number Generation

No.	Requirement	Security Measures

UAF + U2F + FIDO2; TVFR; L1 and higher

An Allowed Random Number Generator or Allowed Key Derivation Function SHALL be used for all key generation resulting in an Authenticator Security Parameter and for any random input for FIDO Relevant signature generation.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_CKM.1, FCS_RNG.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_CKM.1, FCS_RNG.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No.	Requirement	Security Measures
2.2.1	**L1**: At L1, the Authenticator Application SHOULD use the OSes RNG if it is an Allowed RNG according to [FIDOAllowedCrypto] and add entropy as described in [FIDOAllowedCrypto], section "Random Number Generator". Otherwise the Authenticator Application SHALL implement its own Allowed RNG using the OSes RNG and potentially other sources for seeding entropy. **L2**: At L2, the requirement SHALL be fulfilled by mechanisms functioning entirely inside the AROE. **L3**: No calibration required. **L3+**: No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. **L2 Vendor Questionnaire** *Describe* how this requirement can be verified through documentation review. Please provide explicit design document references. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L1 Test Procedure** {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. **L2 Test Procedure** {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the	(SM-16)

No.	developer test results. **Requirement**	**Security Measures**

UAF + U2F + FIDO2; DaD; L1 and higher

The security strength (see the relevant Allowed Deterministic Random Number Generator specification document cited in the “Allowed Cryptography List” [FIDOAllowedCrypto]) of any Authenticator’s Allowed Deterministic Random Number Generator SHALL be at least as large as the largest claimed cryptographic strength of any key generated or used. If the Authenticator generates a key with an Allowed Key Derivation Function, or uses a key with parameters generated by an Allowed Key Derivation Function (see the “Allowed Cryptography List” [FIDOAllowedCrypto]), then the security level of the Allowed Key Derivation Function SHALL be at least as large as the claimed cryptographic level of they key generated or used.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_RNG.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_RNG.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

L2 Vendor Questionnaire

Provide the tester with documentation that specifies how the requirement above is met.

2.2.2

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

(SM-1, SM-26)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

No.	Requirement	Security Measures
	{A2} The tester SHALL *verify* that the documentation meets the requirement.	

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; TVFR; L1 and higher

If the Authenticator adds Authenticator generated nonces and the nonces are produced randomly, then an Allowed Random Number Generator SHALL be used for nonce generation.

Authenticators with unrestricted keys (i.e. Metadata Statement isKeyRestricted: false) don't exclusively control the to-be-signed message and hence have no need to generate a nonce.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_CKM.1, FCS_RNG.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_CKM.1, FCS_RNG.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

L2 Vendor Questionnaire

Describe how this requirement can be verified through documentation review. Please provide explicit design document references.

L3 Vendor Questionnaire

2.2.3	Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	(SM-16)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the

No.	Requirement	Security Measures

following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF; TVFR; L2+ and higher

The Authenticator generated nonce SHALL be of sufficient length to guarantee that the probability of collision between produced Authenticator nonces for a particular User Authentication Key is less than 2^-32 after the maximum number of signatures allowed to be generated using that key.

If the Authenticator generated nonce value added is 16 bytes or longer, then this requirement can be considered to have been fulfilled without a separate argument.

> NOTE
>
> This interacts with requirement 5.4, describing the maximum possible number of signatures.

Bytes in Nonce	Log Base 2 of Allowed Operations
8	16
9	20
10	24
11	28
12	32

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_RNG.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_RNG.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-

No.	Requirement	Security Measures
	1R5]).	
2.2.4	**Calibration** No calibration required.	(SM-8, SM-22)

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; L3 and higher

If the Authenticator implements a Deterministic Random Number Generator, then an Allowed Physical True Random Number Generator SHALL always be used for seeding (seed, re-seed, seed update).

> NOTE
>
> Random Numbers means non-reproducible random numbers. In the instance that reproducible values are desired, using a Key Derivation Function (KDF) is dealt with elsewhere in this requirement set.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_RNG.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see

No.	Requirement	Security Measures
	[CC1V3-1R5]). This requirement is addressed by FCS_RNG.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	

Calibration

No calibration required.

2.2.5	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	(SM-16)

2.2.3 Signature Counters

Support of Signature counters is OPTIONAL.

> NOTE
>
> Authenticators with unrestricted keys (i.e. Metadata Statement field isKeyRestricted: false) cannot support these counters.

Authenticators with restricted keys (i.e. Metadata Statement field isKeyRestricted: true), SHALL set the signature counter value in the assertions to "0" to indicate that they are not supported.

An Authenticator using (1) restricted keys (i.e. Metadata Statement field isKeyRestricted: true) and (2) including values other than "0" for the counter "claims" to support the counter.

NOTE

If the Authenticator claims supporting signature counter(s), it MAY implement a single signature counter for all keys or one signature counter per key.

No.	Requirement	Security Measures
2.3.1	UAF + U2F + FIDO2; DaD; L1 and higher The vendor SHALL document whether the Authenticator supports Signature Counters and if they are supported, the vendor SHALL document whether one Signature Counter *per authentication key* is implemented or one (global) Signature Counter for all authentication keys (i.e. at least one counter covering multiple keys). **Relation to Partner Program** **L3 Common Criteria**: A Security Target document MUST be provided (see [CC1V3-1R5]). This requirement is addressed by ASE_INT and ASE_SPD (see [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target document MUST be provided (see [CC1V3-1R5]). This requirement is addressed by ASE_INT and ASE_SPD (see [CC3V3-1R5]). **Calibration** **L1**: At L1, Authenticators not running in anAllowed Restricted Operating Environment (AROE) [FIDORestrictedOperatingEnv], SHALL support signature counter(s). **L2**: No calibration required. **L3**: No calibration required. **L3+**: No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. **L2 Vendor Questionnaire** *Provide* the tester with documentation that specifies how the requirement above is met. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Mapping to Partner Program Requirements	(SM-15)

No.	Requirement	Security Measures
	• Source Code	

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *verify* that the documentation meets the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

UAF + U2F + FIDO2; GaVR-2; L1 and higher

If the Authenticator claims supporting signature counter(s), then the Authenticator SHALL ensure that the signature counter value *contained in FIDO signature assertions* related to one specific authentication key either

1. is (a) greater than "0" and always has been greater than "0" for any previously generated FIDO signature assertion related to the same authentication key *and* is (b) greater than the signature counter value contained in any previously generated FIDO signature assertion related to the same authentication key, or
2. is set to "0" indicating that the signature counter is not supported any longer (e.g. in the case of a counter error).

> NOTE
>
> Once a signature counter value *contained in a FIDO signature assertion* for one specific authentication key has been set to "0" in MUST stay at such value for that specific authentication key (due to the requirement 1).

[U2FImplCons], [Section 2.6] and [UAFAuthnrCommands] [Section 6.3.4].

If one signature counter per authentication key is implemented (recommended option), it SHALL be incremented by 1 per signature operation. If a global signature counter is implemented, it SHOULD be incremented by a positive random number per signature operation (see [UAFAuthnrCommands] [Section A Security Guidelines, entry SignCounter]).

Relation to Partner Program

L3 Common Criteria: A Security Target, Devlopment and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_IFF, FDP_IFC, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Devlopment and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_IFF, FDP_IFC, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

No.	Requirement	Security Measures
2.3.2	L1 Vendor Questionnaire Is this requirement applicable to the Authenticator? If **No**, then *describe* why. If Yes, *provide* the Security Secretariat with a rationale of how the requirement above is met. L2 Vendor Questionnaire Is this requirement applicable to the Authenticator? If **No**, then *describe* why. If Yes, *provide* a rationale for how the requirement above is met. *Provide* a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references. L3 Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code L3+ Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code L1 Test Procedure {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. L2 Test Procedure {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale. L3 Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. L3+ Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	(SM-15)

2.3 Authenticator's Test for User Presence and User Verification

No.	Requirement	Security Measures
	UAF + U2F + FIDO2; TVFR; L1 and higher If the Authenticator is not marked as a Silent Authenticator [FIDOGlossary], the Authenticator SHALL provide a mechanism to establish if the user authorizes a given action. (For a U2F, this is the "Test for User Presence".	

No.	Requirement	Security Measures
	Generically, the term “**User Verification**” may also refer to this “Test for User Presence”.) NOTE This requirement prevents remote attacks. The user has to confirm an action by pressing a button or providing some other (physical) gesture. **Relation to Partner Program** **L3 Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FIA_UID.2, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FIA_UID.2, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. At L1, in addition to the rationale provided by the vendor, this requirement MUST be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required. **L2 Vendor Questionnaire** *Describe* how this requirement can be verified through documentation review. Please provide explicit design document references.	
3.1	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L1 Test Procedure** {A0} The Security Secretariat SHALL *verify* the requirement during Interoperability Testing. **L2 Test Procedure** {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the	(SM-1, SM-5)

No.	Requirement	Security Measures
	results of this review meet the requirement. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	
3.2	UAF + U2F + FIDO2; GaVR-2; L1 and higher If the Authenticator is not marked as a Silent Authenticator [FIDOGlossary], the Authenticator SHALL NOT perform any authentication relevant operation without first establishing a user has requested the operation by verifying the user ([UAFAuthnrCommands], [section 6.2.4, 6.3.4]). An Authenticator without any keys for the specific user MAY allow the enrollment of new biometric reference data for that user without any additional user verification (bootstrapping user binding). **Authentication relevant operation**s are: 1. Generating User Authentication Keys. 2. Producing signatures using such keys. 3. Adding any additional user verification methods. 4. Adding or changing user verification reference data sets (e.g. passwords or biometric templates). All such operations, with the exception of "Producing signatures using such keys" SHALL always require a fresh user verification (see requirement 3.4). With **fresh user verification** we mean a user verification that is performed at the time the respective operation to be approved by the user is triggered (and not before it). >>>>>>> master **Relation to Partner Program** **L3 Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FIA_UAU.2, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FIA_UAU.2, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. **L2 Vendor Questionnaire** *Provide* a rationale for how the requirement above is met.	(SM-1,

No.	Requirement	Security Measures
	Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.	SM-5

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

I *verify* the provided rationale and documentation meets the requirement.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

3.3 was removed as a U2F Security Requirement for L1 and higher as part of DV 1.1.0. See Requirement 3.4. Requirement text within DV 1.0.2 read as follows:

3.3 ~~Once the Authenticator's test for user presence is successful (and user presence is detected), the user SHALL be deemed "present" for no more than 10 seconds, or until the next operation which requires user presence is performed, whichever comes first.~~

UAF + U2F + FIDO2; GaVR-1; L1 and higher

This requirement relates to "UserVerificationCaching" as specified in [UAFRegistry] for more details.

If not declared otherwise in the Metadata Statement Once the Authenticator's user verification / user presence check is successful, the user SHALL be deemed "verified" for no more than 10 seconds, or until the next operation which requires user verification, whichever comes first. Any provided User Verification Token SHALL NOT be valid after this time period. [UAFAuthnrCommands], [Appendix A Security Guidelines]

If declared otherwise in the Metadata Statement

1. The authenticator SHALL truthfully declare support of this user verification caching in the related

No.	Requirement	Security Measures
	Metadata Statement [FIDOMetadataStatement] (entry isFreshUserVerificationRequired=false). 2. Once the Authenticator's user verification / user presence check is successful, the user SHALL be deemed "verified" for no longer than the "maximum user verification caching time" as provided by the caller. If the caller has not specified a "maximum user verification caching time", then the Authenticator SHALL NOT cache the user verification event. Any provided User Verification Token SHALL NOT be valid after this time period. Multiple authentication operations might be performed in this time. The authenticator MAY limit the number of acceptable authentications in this time. 3. The authenticator SHALL add the "maximum user verification caching time" related to the specific Uauth key to the attestation statement. 4. When performing a TransactionConfirmation operation, the authenticator SHALL perform fresh user verification.	

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests document MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FIA_UAU.2, FIA_UAU.6, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests document MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FIA_UAU.2, FIA_UAU.6, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

3.4

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

At L1, in addition to the rationale provided by the vendor, this requirement MUST be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.

(SM-5)

L2 Vendor Questionnaire

Provide a rationale for how the requirement above is met.

Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

No.	Requirement	Security Measures
	• Low Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	

L1 Test Procedure

{A0} The Security Secretariat SHALL *verify* the requirement during Interoperability Testing.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + FIDO2; GaVR-1; L1 and higher

The Authenticator SHALL NOT reveal the stored username(s) (UAF) / PublicKeyCredentialUserEntity (FIDO2) prior to verifying the user. [UAFAuthnrCommands], Section 6.3.4.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_ITT.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_ITT.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

At L1, in addition to the rationale provided by the vendor, this requirement MUST be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.

L2 Vendor Questionnaire

Provide a rationale for how the requirement above is met.

Provide a documentation review procedure to confirm that the Authenticator's design is consistent with

No.	Requirement	Security Measures
	the provided rationale. Please provide explicit design document references.	
3.5	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	(SM-5, SM-10)
	L3+ Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	
	L1 Test Procedure {A0} The Security Secretariat SHALL *verify* the requirement during Interoperability Testing.	
	L2 Test Procedure {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.	
	L3 Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	
	L3+ Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	
	UAF + FIDO2; GaVR-1; L1 and higher The Authenticator SHALL NOT output unencrypted AppIDs/RP IDs or KeyIDs/CredentialIDs that are associated with a Key Handle prior to verifying the user.	
	Relation to Partner Program **L3 Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FPT_ITC.1, FIA_UAU.2, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FPT_ITC.1, FIA_UAU.2, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	

No.	Requirement	Security Measures
	Calibration No calibration required.	
	L1 Vendor Questionnaire *Provide* the Security Secretariat with a rationale of how the requirement above is met.	
	L2 Vendor Questionnaire *Provide* a rationale for how the requirement above is met. *Provide* a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.	
3.6	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	(SM-5, SM-23)
	L3+ Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	
	L1 Test Procedure {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.	
	L2 Test Procedure {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.	
	L3 Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	
	L3+ Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	

~~UAF + U2F + FIDO2; L2+ and higher~~

If the Authenticator accepts input directly from the user or provides outputs directly to the user, then this communication SHALL be protected from data injection, disclosure, modification or substitution through use of a Trusted Path. This Trusted Path SHALL allow a user to communicate directly with the Authenticator, SHALL only be able to be activated by the Authenticator or the user, and cannot be imitated by untrusted software.

NOTE

No.		Security Measures
	Only silent authenticators [FIDOGlossary] do not have a need for accepting any input directly from the user or providing output directly to the user. A Trusted Path is the means by which a user and a security functionality of the Authenticator can communicate with the necessary confidence. In other words, a Trusted Path allows users to perform functions through an assured direct interaction with the security functionality of the Authenticator. For instance, plaintext ASPs may be entered into or output from the Authenticator in an encrypted form (e.g. display text digitally signed). This means that if the Authenticator has a Transaction Confirmation Display, it SHALL be protected from a display overlay attack.	

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FTP_TRP.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FTP_TRP.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

L3: At L3, the protection SHALL be strong enough to be protected against *enhanced-basic* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.3 or higher vulnerability analysis (see [CEMV3-1R5]).

3.7	**L3+**: At L3+, the protection SHALL be strong enough to be protected against *moderate* or *high* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.4 or higher vulnerability analysis (see [CEMV3-1R5]).	(SM-5, SM-10, SM-29)

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

No.	Requirement	Security Measures
	The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

UAF + U2F + FIDO2; GaVR-3; L1 and higher

The Authenticator SHALL protect against injection or replay of FIDO user verification data (e.g. user presence status, PIN, or biometric data).

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FPT_RPL.1, FAU_ARP.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FPT_RPL.1, FAU_ARP.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

L1: At L1, the Authenticator Application SHALL follow best security practices specific to the underlying operating environment for protecting against injection or replay of FIDO user verification data. This especially means that the Authenticator Application SHALL NOT provide any API for injecting FIDO user verification data.

L2: At L2, the requirement SHALL be fulfilled by mechanisms functioning entirely inside the AROE.

L3: At L3, the protection SHALL be strong enough to be protected against *enhanced-basic* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.3 or higher vulnerability analysis (see [CEMV3-1R5]).

L3+: At L3+, the protection SHALL be strong enough to be protected against *moderate* or *high* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.4 or higher vulnerability analysis (see [CEMV3-1R5]).

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

L2 Vendor Questionnaire

Provide a rationale for how the requirement above is met.

No.	Requirement	Security Measures
3.8	*Provide* a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.	(SM-3, SM-5, SM-7)

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

UAF + U2F + FIDO2; GaVR-3; L1 and higher

Authenticators implementing user verification methods other than user presence check [FIDOGlossary], SHALL rate-limit user verification attempts in order to prevent brute-force attacks. [FIDOMetadataStatement], sections 3.1, 3.2, 3.3 and [UAFAuthnrCommands], Appendix A Security Guidelines, entry "Matcher".

The overarching requirement is based on an upper limit for the probability of a successful brute-force attack. The upper limits specified in "calibration" below.

For the purposes of this requirement, a **brute-force attack** is defined as follows: The attacker tries all possible input combinations (e.g. passwords, PINs, patterns, biometrics...) in order to pass the user verification. In the case of biometric user verification, the attacker brings a potentially unlimited number of "friends" that can try whether their biometric characteristic is accepted (as false accept). In all cases the number of trials per time is limited by the verification speed of the authenticator and the integrity of the authenticator is not violated (e.g. no decapping of chips, no malware, ...) - since there are other requirements

No.	Requirement	Security Measures
	dealing with such attacks. NOTE • The rate limiting requirement applies to all user verification methods (other than user presence check). • Implementing a more strict rate limiting method is allowed. • We *recommend* 1. Allowing up to 3 failed user verification attempts without any penalty and then imposing a delay of at least 30 seconds before the 4th one, increasing exponentially with each successive attempt (e.g., 1 minute before the 5th one, 2 minutes before the 6th one), or 2. Disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available after the 5th failed user verification attempt. Disabling the first user verification method and falling back to an alternative user verification method MAY take place at any time without imposing additional delays. **Relation to Partner Program** **L3 Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FAU_ARP.1, FAU_SAA.1, FAU_GEN.1, FPT_STM.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FAU_ARP.1, FAU_SAA.1, FAU_GEN.1, FPT_STM.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **Calibration** **L1**: At L1, the time dependent probability of a successful brute-force attack on the authenticator SHALL be P(*t*) ≤ maximum(170/10000, (24**t*+16) / 10000), with *t* being the time in days. For a 4 digit PIN it means up to 170 non-biometric user verification attempts in the first 6.4 days and then at least one hour delay per one of them. **L2**: At L2, the time dependent probability of a successful brute-force attack on the authenticator SHALL be P(*t*) ≤ maximum(170/10000, (12**t*+16) / 10000), with *t* being the time in days. For a 4 digit PIN it means up to 170 non-biometric user verification attempts in the first 12.8 days and then at least a two hour delay per one of them. At L2, the requirement SHALL be fulfilled by mechanisms functioning entirely inside the Authenticator Boundary, i.e. inside the AROE. **L3**: At L3, in addition to meeting the calibration for L2, the protection SHALL be strong enough to be protected against *enhanced-basic* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.3 or higher vulnerability analysis (see [CEMV3-1R5]). NOTE This implies that an attack potential calculation should be undertaken to determine what the actual	
3.9		(SM-1,

No.		Security Measures
	rate limit should be to meet the requirement at the level. It is likely to be more restrictive for the end user than the rate described in the requirement text.	SM-5 (SM-37)
	L3+: At L3+, in addition to meeting the calibration for L2, the protection SHALL be strong enough to be protected against *moderate* or *high* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.4 or higher vulnerability analysis (see [CEMV3-1R5]). NOTE This implies that an attack potential calculation should be undertaken to determine what the actual rate limit should be to meet the requirement at the level. It is likely to be more restrictive for the end user than the rate described in the requirement text.	

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

At L1, in addition to the rationale provided by the vendor, this requirement MUST be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.

L2 Vendor Questionnaire

Provide a rationale for how the requirement above is met.

Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A0} The Security Secretariat SHALL *verify* the requirement during Interoperability Testing.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer

No.	Requirement	Security Measures
	test results. The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.	

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

UAF1+ U2F1+ FIDO2; GaVR-3; L2+ and higher

If the authenticator supports biometric user verification (e.g. fingerprint, face recognition, etc.), then the authenticator biometric component SHALL be certified according to [FIDOBiometricsRequirements]. The Level Calibration, correspondence to Partner Programs, Vendor Questionnaires, and Test Procedures for this requirement are all specified in [FIDOBiometricsRequirements].

Relation to Partner Program

L3 Common Criteria: A Security Target, a Preparative Guidance document a Biometric Certification Report MUST be provided. (see [CC1V3-1R5]) This requirement is addressed by ASE_INT, ASE_SPD and AGD_PRE (see [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, a Preparative Guidance document and a Biometric Certification Report MUST be provided. (see [CC1V3-1R5]) This requirement is addressed by ASE_INT, ASE_SPD and AGD_PRE (see [CC3V3-1R5]).

Calibration

L3: Refer to [CAFVM], [FSDPP] and [BEAT].

L3+: Refer to [CAFVM], [FSDPP] and [BEAT].

3.10 (SM-1, SM-5, SM-27)

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Guidance Documents
- Mapping to Partner Program Requirements
- FIDO Biometric Certification Report

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Guidance Documents
- Mapping to Partner Program Requirements
- FIDO Biometric Certification Report

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

L3+ Test Procedure

No.	Requirement	Security Measures
	The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.	

2.4 Privacy

No.	Requirement	Security Measures
	UAF + U2F + FIDO2; GaVR-1; L1 and higher An Authenticator SHALL NOT have any **Correlation Handle** that is visible across multiple Relying Parties. If the authenticator uses a shared attestation key (e.g. Full Basic Attestation), the minimum number of Authenticators sharing this key MUST be at least 100000.	

> NOTE
>
> The goal of this requirement is that, for privacy reasons, the Authenticator MUST NOT leak information about the user across multiple Relying Parties by sharing a Correlation Handle.
>
> This requirement specifically applies to KeyIDs/CredentialIDs, KeyHandles etc.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FPR_ANO.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FPR_ANO.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

L2 Vendor Questionnaire

Provide a rationale for how the requirement above is met.

Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.

4.1		(SM-23)

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

No.	Requirement	Security Measures

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; GaVR-1; L1 and higher

An Authenticator SHALL NOT provide information to one Relying Party that can be used to uniquely identify that Authenticator instance to a different Relying Party.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FMT_MTD.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FMT_MTD.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

L2 Vendor Questionnaire

Provide a rationale for how the requirement above is met.

Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the

No.	Requirement	Security Measures
	provided rationale. Please provide explicit design document references.	
4.2	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L1 Test Procedure** {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. **L2 Test Procedure** {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. UAF + FIDO2; GaVR-1; L1 and higher An external party with two (AAID, KeyID) / (AAGUID, CredentialID) tuples produced using the Authenticator SHALL NOT be able to establish that they were produced using the same Authenticator. **Relation to Partner Program** **L3 Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FPR_UNL.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FPR_UNL.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	(SM-23)

No.	Requirement	Security Measures
4.3	**Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. **L2 Vendor Questionnaire** *Provide* a rationale for how the requirement above is met. *Provide* a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code **L1 Test Procedure** {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. **L2 Test Procedure** {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. UAF; GaVR-1; L1 and higher The Authenticator's response to a "Deregister" command SHALL NOT reveal whether the provided KeyID was registered. **Relation to Partner Program**	(SM-23)

No.	Requirement	Security Measures
	L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FDP_IFC, FDP_IFF, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	
	L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FDP_IFC, FDP_IFF, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	

Calibration

No calibration required.

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

At L1, in addition to the rationale provided by the vendor, this requirement MUST be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.

L2 Vendor Questionnaire

Provide a rationale for how the requirement above is met.

Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.

4.4

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

(SM-23)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A0} The Security Secretariat SHALL *verify* the requirement during Interoperability Testing.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

No.	Requirement	Security Measures
4.5	The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. At L1, this requirement MUST be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required. **L2 Vendor Questionnaire** *Provide* a rationale for how the requirement above is met. *Provide* a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references. **L3 Vendor Questionnaire**	SM-5

Uauth test FIDO2; GaVR-1; L1 and higher

The Authenticator's response to any command (e.g. an "Authenticate") SHALL NOT reveal whether a key was registered for the given AppID / RP ID without the Authenticator either (1) requiring a KeyID / Credential ID as input or (2) verifying the user (using a method other than user presence check) - unless the authenticator registered a key to that entity.

> NOTE
>
> This requirement is intended to avoid third parties having physical access to an Authenticator to determine the AppIDs/RP IDs the Authenticator has been registered to - without having user consent.
>
> This means that Authenticators that (a) persistently store the Uauth key pair inside the Authenticator boundary and (b) that implement *no* user verification or *only* implement user presence check need to provide a response that cannot be distinguished from a valid authentication response.
>
> Such Authenticators could maintain a dedicated Uauth key pair for generating responses for unknown AppIDs / RP IDs. The corresponding public key shall never leave the Authenticator (since with knowledge of the corresponding public key the response could be distinguished from a response for a registered AppID / RP ID).

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_IFC, FDP_IFF, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FDP_IFC, FDP_IFF, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

No.	Requirement	Security Measures

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A0} The Security Secretariat SHALL *verify* the requirement during Interoperability Testing.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

2.5 Physical Security, Side Channel Attack Resistance and Fault Injection Resistance

No.	Requirement	Security Measures

UAF + U2F + FIDO2; DaD; L2 and higher

The vendor SHALL document the physical security and side channel attack protections used by the Authenticator.

Relation to Partner Program

L3 Common Criteria: Development documentation MUST be provided.

This requirement is addressed by Class ADV (see [CC3V3-1R5]).

L3+ Common Criteria: Development documentation MUST be provided.

This requirement is addressed by Class ADV (see [CC3V3-1R5]).

Calibration

No.	Requirement	Security Measures
	No calibration required.	

L2 Vendor Questionnaire

Provide the tester with documentation that specifies how the requirement above is met.

5.1

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Mapping to Partner Program Requirements
- Source Code

(SM-1, SM-20, SM-24, SM-26, SM-29)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Mapping to Partner Program Requirements
- Source Code

L2 Test Procedure

{A2} The tester SHALL *verify* that the documentation meets the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

N/A

5.2 was removed as a UAF + U2F L2+ and higher Security Requirement as part of DV 1.1.0. See Requirement 5.3. Requirement text within DV 1.0.2 read as follows:

~~The Authenticator SHALL provide evidence of physical tampering that allows the attacker to violate FIDO Security Goals or FIDO Authenticator Security Requirements.~~

5.2

~~NOTE~~

~~At L3, such evidence SHALL be visible to the user (and not necessarily to the RP). As a consequence, a level of cooperation from the user is expected to protect the RP.~~

N/A

UAF + U2F + FIDO2; L2+ and higher

The Authenticator shall resist physical tampering that allows the attacker to violate FIDO Security Goals or FIDO Authenticator Security Requirements.

NOTE

The keys can be zeroed in response to an attack so the Authenticator is no longer usable. This is the way the relying party can be informed of the attack. If the Authenticator includes a biometric user verification feature, the calibration as defined below must address that feature to the same level of vulnerability assessment.

No.		Security Measures
	NOTE Resistance to physical tampering obviates the need for physical tamper evidence.	
	Relation to Partner Program **L3 Common Criteria**: A Security Target and Development documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FPT_PHP.3 and Class ADV (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target and Development documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FPT_PHP.3 and Class ADV (see [CC2V3-1R5] and [CC3V3-1R5]).	
5.3	**Calibration** **L3**: At L3, the protection SHALL be strong enough to be protected against *enhanced-basic* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.3 or higher vulnerability analysis (see [CEMV3-1R5]). **L3+**: At L3+, the protection SHALL be strong enough to be protected against *moderate* or *high* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.4 or higher vulnerability analysis (see [CEMV3-1R5]).	(SM-20, SM-24, SM-26)
	L3 Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Mapping to Partner Program Requirements • Source Code	
	L3 Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.	

UAF + U2F + FIDO2; TVFR; L2 and higher

No.	Requirement	Security Measures
5.4	Each secret or private key that is an Authenticator Security Parameter SHALL have a key use limit establishing the maximal number of times that particular key can be used within a particular Authenticator.	(SM-24, SM-26)

NOTE

Key refresh needs to be initiated by the RP for ideal user experience. In the current protocol, there is no provision for the Authenticator to initiate key refresh.

This requirement interacts with requirements 2.3, 2.25, 5.5, 5.6.

This is a requirement that provides flexibility in satisfying other requirements. The idea is that key use limit SHOULD be established such that the other requirements cited here are fulfilled (providing the vendor the ability to restrict the number of possible key uses rather than using longer nonces or better side-channel countermeasures), and additionally provides the option for the vendor to defend the Authenticator against attacks that are not yet known.

Both cryptographic and side-channel attacks on the Authenticator can be enabled by having access to information associated with distinct cryptographic operations under the same key, so the vendor MAY elect to impose a conservative key use limit in order to defend against such attacks, especially for attacks that are not yet known and thus cannot easily be otherwise defended against.

Any limit that allows the Authenticator to fulfill the other related requirements is sufficient for compliance to the requirement set. Some examples follow:

If a vendor doesn't require any particular key use limit to satisfy additional requirements, and they are not concerned with the possibility of unknown cryptographic attack, then this limit can be simply the maximal possible uses of this key, given the hardware constraints of the Authenticator (i.e., the rate of key use that the hardware can support multiplied by the total expected lifetime of the Authenticator). In this instance, the Authenticator need not retain the number of uses of each key. For example, if a device can perform one key use per second and has an expected lifetime of 5 years, then a reported key use limit of roughly (5*365+1)*86400 (less than 2^28) would be sufficient.

If the vendor does wish to limit the number of possible key uses, but does not wish to store state associated with this data, then the vendor can limit the average key use rate such that the total number of uses of a given key throughout the expected lifetime of the Authenticator is sufficiently low. For an example, if an Authenticator vendor wishes to limit the total number of key uses of a user key to 10,000,000 (less than 2^24) and the Authenticator has a expected lifetime of 5 years, then the Authenticator MUST enforce a long term average key use rate of roughly 1 key use every 158 seconds.

If a vendor does not wish to arbitrarily limit the rate at which keys can be used, but does wish to restrict the number of possible key uses, then they can store a count of the number of times a particular key has been used, and then disable use of the key at the limit.

Some keys (e.g., the User Private Key, or the Attestation key) cannot be painlessly replaced within the FIDO protocol (this requires re-enrolling, or replacing the Authenticator, respectively), so a suitably large limit SHOULD be chosen to prevent usability problems.

FIDO Authenticators typically require a user verification before using a private key. Such manual interaction requires a minimum amount of time.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FMT_MTD.2, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FMT_MTD.2, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

No.	Requirement	Security Measures

Calibration

No calibration required.

L2 Vendor Questionnaire

Describe how this requirement can be verified through documentation review. Please provide explicit design document references.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; L3 and higher

The Authenticator SHALL NOT leak Secret Authenticator Security Parameter data (e.g. due to power, near field, or radio leakage) at a rate that would allow an attacker to weaken the key below the claimed cryptographic strength of the key, even after an attacker has observed all allowed key uses.

> NOTE
>
> This interacts with requirement 5.4.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development documents MUST be provided (see [CC1V3-1R5]).

No.	Requirement	Security Measures
	This requirement is addressed by FPT_PHP.2, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	
	L3+ Common Criteria: A Security Target, Development documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FPT_PHP.3, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	
5.5	**Calibration** **L3**: At L3, the protection SHALL be strong enough to be protected against *enhanced-basic* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.3 or higher vulnerability analysis (see [CEMV3-1R5]). **L3+**: At L3+, the protection SHALL be strong enough to be protected against *moderate* or *high* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.4 or higher vulnerability analysis (see [CEMV3-1R5]). **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Mapping to Partner Program Requirements • Source Code **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.	(SM-20)

UAF + U2F + FIDO2; GaVR-3; L2+ and higher

The variations in the amount of time required to perform a cryptographic algorithm SHALL NOT allow remote attackers to reduce the security of Authenticator Security Parameters which are secret or private keys below their claimed cryptographic strength.

> NOTE
>
> This requirement is mandatory for L2+-and-higher but it remains relevant for L2 as a developer guideline. It refers to all Secret Authenticator Security Parameters, and not just the authentication and attestation keys. This means it includes keys used to wrap these parameters, including keys that might

No.		Security Measures
	be used to wrap biometric reference data. The defense against remote timing attacks requires securing the cryptographic operation implementations and/or hardening the Allowed Restricted Operating Environment (AROE, see [FIDORestrictedOperatingEnv]) cache implementation: **Securing cryptographic operations:** Concerning symmetric-key algorithms, It is recommended to use Hardware-based cryptographic algorithms replacing the software-based implementation and thus eliminating the side-channel information leaked from the execution of cryptographic operations. Otherwise, the software implementation MUST consider randomization of the control flow so that there is no fixed relation between the execution path and the cache set. Or, MUST enable using the same amount of cache independently from the keys used. **AROE cache enhanced implementations:** It is recommended to secure the cache memory implementation in order to restrict the impact from the Rich OS on the AROE cache memory. This could be done by programming memory allocations so that the Rich OS memory will never be mapped to the AROE cache memory. The implementation can also consider flushing sensitive secure cache to memory to eliminate the information on the table access. For more details on how to implement adequate counter-measures please review the following research papers: • for **ECC, remote timing attack (protocol timing)** refer to https://eprint.iacr.org/2011/232 • for **ECC, local cache timing attack (local cache timing)** refer to http://eprint.iacr.org/2014/161 • for **RSA cache timing** refer to https://eprint.iacr.org/2015/898 • for **AES cache timing** refer to https://eprint.iacr.org/2014/435	
	NOTE This interacts with requirement 5.4.	
5.6	**Relation to Partner Program** **L3 Common Criteria**: A Security Target and Devlopment documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FPT_PHP.2 and Class ADV (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target and Devlopment documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FPT_PHP.3 and Class ADV (see [CC2V3-1R5] and [CC3V3-1R5]). **Calibration** **L3**: At L3, the protection SHALL be strong enough to be protected against *enhanced-basic* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.3 or higher vulnerability analysis (see [CEMV3-1R5]). **L3+**: At L3+, the protection SHALL be strong enough to be protected against *moderate* or *high* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.4 or higher vulnerability analysis (see [CEMV3-1R5]). **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation	(SM-20, SM-29)

No.	Requirement	Security Measures
	• Mapping to Partner Program Requirements • Source Code	

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Mapping to Partner Program Requirements
- Source Code

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

UAF + U2F + FIDO2; L3 and higher

The length of time required to perform a cryptographic algorithm using a Secret Authenticator Security Parameter SHALL NOT be dependent on the value of that secret or private key.

> NOTE
>
> No time variations are allowed in this requirement, in comparison to requirement 5.6, in which some time variations are allowed.

Relation to Partner Program

L3 Common Criteria: A Security Target and Development documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FPT_PHP.2, Class ADV (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target and Development documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FPT_PHP.3, Class ADV (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

5.7	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Mapping to Partner Program Requirements • Source Code	(SM-20, SM-29)

No.	Requirement	Security Measures
	L3+ Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Mapping to Partner Program Requirements • Source Code **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. UAF + U2F + FIDO2; GaVR-2; L2 and higher All physical and logical debug interfaces to the Authenticator which enable violation of FIDO Authenticator Security Goals or FIDO Authenticator Security Requirements SHALL be disabled and unusable in fielded Authenticators. **Relation to Partner Program** **L3 Common Criteria**: A Security Target, Development, Tests and Preparative Procedure Guidance documentation MUST be provided. This requirement is addressed by FPT_TST.1, AGD_PRE, Class ADV and ATE. **L3+ Common Criteria**: A Security Target, Development, Tests and Preparative Procedure Guidance documentation MUST be provided. This requirement is addressed by FPT_TST.1, AGD_PRE, Class ADV and ATE. **Calibration** No calibration required. **L2 Vendor Questionnaire** *Provide* a rationale for how the requirement above is met. *Provide* a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Guidance Documents • Mapping to Partner Program Requirements • Source Code	
5.8		(SM-23, SM-26)

No.	Requirement	Security Measures

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Guidance Documents
- Mapping to Partner Program Requirements
- Source Code

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; L3 and higher

The Authenticator SHALL be resistant to induced fault attacks.

> NOTE
>
> This requirement is mandatory for L3 and higher but it is still relevant for L2 and higher as a developer guideline. The developer SHALL take into account SW-based fault induction side channel attack and implement relevant countermeasures such as enabling memory error detection.

Relation to Partner Program

L3 Common Criteria: A Security Target and Development documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FPT_PHP.2 and Class ADV (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target and Development documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FPT_PHP.3 and Class ADV (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

L3: At L3, the protection SHALL be strong enough to be protected against *enhanced-basic* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.3 or higher vulnerability analysis (see [CEMV3-1R5]).

L3+: At L3+, the protection SHALL be strong enough to be protected against *moderate* or *high* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is

No.	Requirement	Security Measures
3.9	defined by AVA_VAN.4 or higher vulnerability analysis (see [CEMV3-1R5]).	(SM-28, SM-21)

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Mapping to Partner Program Requirements
- Source Code

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

2.6 Attestation

For compliance with L1, Surrogate Basic Attestation [UAFProtocol] in the case of UAF / self-signed attestation certificates in the case of U2F is acceptable.

No.	Requirement	Security Measures
	UAF + U2F + FIDO2; TVFR; L2 and higher The vendor SHALL use attestation certificates / ECDAA Issuer public keys [FIDOEcdaaAlgorithm] dedicated to a single Authenticator model.	

Relation to Partner Program

L3 Common Criteria: A Security Target, Development, Tests and Preparative Guidance documentation MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, AGD_PRE, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development, Tests and Preparative Guidance documentation MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, AGD_PRE, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

No.	Requirement	Security Measures
6.1	**Calibration** No calibration required. **L2 Vendor Questionnaire** *Describe* how this requirement can be verified through documentation review. Please provide explicit design document references. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Guidance Documents • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Tests Documents • Guidance Documents • Mapping to Partner Program Requirements • Source Code **L2 Test Procedure** {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results. UAF + U2F + FIDO2; TVFR; L1 and higher Each Authenticator being declared as the same model (i.e. having the same AAID, AAGUID or having at least one common attestationCertificateKeyIdentifier in the MetadataStatement), SHALL fulfill at least the security characteristics stated for that Authenticator model. **Relation to Partner Program** **L3 Common Criteria**: A Security Target, Preparative and User Guidance documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_COP.1, AGD_PRE and AGD_OPE (see [CC2V3-1R5] and [CC3V3-1R5]).	(SM-3)

No.	Requirement	Security Measures
6.2	**L3+ Common Criteria**: A Security Target, Preparative and User Guidance documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_COP.1, AGD_PRE and AGD_OPE (see [CC2V3-1R5] and [CC3V3-1R5]) **Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. At L1, in addition to the rationale provided by the vendor, this requirement MUST be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required. **L2 Vendor Questionnaire** *Describe* how this requirement can be verified through documentation review. Please provide explicit design document references. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Guidance Documents • Mapping to Partner Program Requirements • Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Guidance Documents • Mapping to Partner Program Requirements • Source Code **L1 Test Procedure** {A0} The Security Secretariat SHALL *verify* the requirement during Interoperability Testing. **L2 Test Procedure** {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. **L3+ Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. UAF + U2F + FIDO2; GaVR-1; L1 and higher The Authenticator SHALL accurately describe itself in its provided metadata, or alternately describe an Authenticator of lesser security. The vendor SHALL provide all mandatory Metadata Statement fields see [FIDOMetadataRequirements].	(SM-3)

No.	Requirement	Security Measures
6.3	**Relation to Partner Program** **L3 Common Criteria**: A Security Target, Preparative and User Guidance documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_COP.1, AGD_PRE and AGD_OPE (see [CC2V3-1R5] and [CC3V3-1R5]) **L3+ Common Criteria**: A Security Target, Preparative and User Guidance documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_COP.1, AGD_PRE and AGD_OPE (see [CC2V3-1R5] and [CC3V3-1R5]) **Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met. At L1, in addition to the rationale provided by the vendor, this requirement MUST be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required. **L2 Vendor Questionnaire** *Provide* a rationale for how the requirement above is met. *Provide* a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: - High Level Design Documentation - Guidance Documents - Mapping to Partner Program Requirements - Source Code **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: - Low Level Design Documentation - Guidance Documents - Mapping to Partner Program Requirements - Source Code **L1 Test Procedure** {A0} The Security Secretariat SHALL *verify* the requirement during Interoperability Testing. **L2 Test Procedure** {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement.	(SM-3)

No.	Requirement	Security Measures

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

~~UAF + U2F + FIDO2; DaD; L2 and higher~~

The vendor SHALL document whether the attestation root certificate is shared across multiple Authenticator models.

In such case, the attestation certificate MUST contain an extension indicating the Authenticator model (e.g. AAID or AAGUID).

Relation to Partner Program

L3 Common Criteria: A Security Target, Preparative and User Guidance documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, AGD_PRE and AGD_OPE (see [CC2V3-1R5] and [CC3V3-1R5])

L3+ Common Criteria: A Security Target, Preparative and User Guidance documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, AGD_PRE and AGD_OPE (see [CC2V3-1R5] and [CC3V3-1R5])

Calibration

No calibration required.

L2 Vendor Questionnaire

Describe how this requirement can be verified through documentation review. Please provide explicit design document references.

6.4

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Guidance Documents
- Mapping to Partner Program Requirements
- Source Code

(SM-3)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Guidance Documents
- Mapping to Partner Program Requirements
- Source Code

L2 Test Procedure

{A2} The tester SHALL *verify* that the documentation meets the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

No.	Requirement	Security Measures
	L3+ Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement.	
6.5	UAF + FIDO2; DaD; L2 and higher The vendor SHALL document whether the attestation certificate includes the Authenticator model (e.g. AAID or AAGUID). L2 Vendor Questionnaire *Provide* the tester with documentation that specifies how the requirement above is met. Relation to Partner Program **L3 Common Criteria**: A Security Target, Preparative and User Guidance documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_COP.1, AGD_PRE and AGD_OPE (see [CC2V3-1R5] and [CC3V3-1R5]) **L3+ Common Criteria**: A Security Target, Preparative and User Guidance documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FCS_COP.1, AGD_PRE and AGD_OPE (see [CC2V3-1R5] and [CC3V3-1R5]) L3 Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Guidance Documents • Mapping to Partner Program Requirements • Source Code L3+ Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Guidance Documents • Mapping to Partner Program Requirements • Source Code L2 Test Procedure {A2} The tester SHALL *verify* that the documentation meets the requirement. L3 Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement. L3+ Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement.	(SM-3)

2.7 Operating Environment

NOTE

At L1 we allow the Authenticator Application to run in any operating environment. For the levels L2 through L3+, the Authenticator Application needs to run in an Allowed Restricted Operating Environment [FIDORestrictedOperatingEnv].

No.	Requirement	Security Measures

UAF + U2F + FIDO2; GaVR-1; L2 and higher

The Authenticator Application SHALL run in an Allowed Restricted Operating Environment (AROE) [FIDORestrictedOperatingEnv].

Relation to Partner Program

L3 Common Criteria: A Security Target, a Preparative and Operational User Guidance documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ASE_SPD, AGD_OPE and AGD_PRE (see [CC3V3-1R5])

L3+ Common Criteria: A Security Target, a Preparative and Operational User Guidance documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ASE_SPD, AGD_OPE and AGD_PRE (see [CC3V3-1R5])

Calibration

No calibration required.

L2 Vendor Questionnaire

Provide a rationale for how the requirement above is met.

Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.

7.1

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Guidance Documents
- Mapping to Partner Program Requirements
- Source Code

(SM-1)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Guidance Documents
- Mapping to Partner Program Requirements
- Source Code

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

No.	Requirement	Security Measures
7.2	L3+ Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement. UAF + U2F + FIDO2; GaVR-3; L2 and higher The operating environment SHALL be configured so that all operating environment security functions used by the Authenticator are active and available for use to support the FIDO Authenticator Security Goals or FIDO Authenticator Security Requirements. Relation to Partner Program **L3 Common Criteria**: A Security Target, a Preparative and Operational User Guidance and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by ASE_SPD, AGD_OPE, AGD_PRE and Class ATE (see [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target, a Preparative and Operational User Guidance and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by ASE_SPD, AGD_OPE, AGD_PRE and Class ATE (see [CC3V3-1R5]). Calibration No calibration required. L2 Vendor Questionnaire *Provide* a rationale for how the requirement above is met. *Provide* a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references. L3 Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Guidance Documents • Tests Documents • Mapping to Partner Program Requirements • Source Code L3+ Vendor Questionnaire Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Low Level Design Documentation • Guidance Documents • Tests Documents • Mapping to Partner Program Requirements • Source Code L2 Test Procedure {A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale. L3 Test Procedure The Tester SHALL *verify* the provided rationale and documentation meets the requirement.	(SM-1)

No.	Requirement	Security Measures
	The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.	

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; GaVR-3; L2 and higher

The operating environment SHALL prevent non-Authenticator processes from reading, writing and modifying running or stored Authenticator Application and its associated memory.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development, a Preparative and Operational User Guidance documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ASE_SPD, AGD_OPE, AGD_PRE and Class ADV (see [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development, a Preparative and Operational User Guidance documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ASE_SPD, AGD_OPE, AGD_PRE and Class ADV (see [CC3V3-1R5]).

Calibration

L2: At L2, the requirement SHALL be fulfilled by mechanisms functioning entirely inside the AROE.

L3: At L3, the protection SHALL be strong enough to be protected against *enhanced-basic* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.3 or higher vulnerability analysis (see [CEMV3-1R5]).

L3+: At L3+, the protection SHALL be strong enough to be protected against *moderate* or *high* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.4 or higher vulnerability analysis (see [CEMV3-1R5]).

L2 Vendor Questionnaire

Provide a rationale for how the requirement above is met.

Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.

7.3 (SM-1)

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Guidance Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the

No.	Requirement	Security Measures

following supporting documents:

- Low Level Design Documentation
- Guidance Documents
- Mapping to Partner Program Requirements
- Source Code

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

~~UAF + U2F + FIDO2; GaVR-3; L2 and higher~~

The operating environment SHALL NOT be able to be modified in a way that undermines the security of the Authenticator.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development, a Preparative and Operational User Guidance documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ASE_SPD, AGD_OPE, AGD_PRE and Class ADV (see [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development, a Preparative and Operational User Guidance documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ASE_SPD, AGD_OPE, AGD_PRE and Class ADV (see [CC3V3-1R5]).

Calibration

L2: At L2, the requirement SHALL be fulfilled by mechanisms functioning entirely inside the AROE.

L3: At L3, the protection SHALL be strong enough to be protected against *enhanced-basic* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.3 or higher vulnerability analysis (see [CEMV3-1R5]).

L3+: At L3+, the protection SHALL be strong enough to be protected against *moderate* or *high* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.4 or higher vulnerability analysis (see [CEMV3-1R5]).

L2 Vendor Questionnaire

Provide a rationale for how the requirement above is met.

Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.

7.4 No.	Requirement	Security Measures (SM-1)

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Guidance Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Guidance Documents
- Mapping to Partner Program Requirements
- Source Code

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

UAF + U2F + FIDO2; GaVR-1; L2 and higher

The security configuration of the operating environment SHALL be fully under control of the Authenticator vendor or its delegates such that the security configuration present at commercial shipment cannot be changed except for in-the-field updates that are also fully under control of the Authenticator device vendor or its delegates.

> NOTE
>
> In some environments (e.g. PC), the user (i.e. anyone other than the Authenticator vendor or its delegates) might change the security configuration of the Authenticator. However, it is the responsibility of the Authenticator to detect potential changes in the Authenticator security configuration and provide the appropriate RP response through a FIDO assertion if the changed configuration still meets the expected security characteristics according to the Metadata Statement (or stop working and either protect the security parameters at the prior level or securely destroy them if it doesn't). The Authenticator certification MUST include all security configuration items available to the user.

Relation to Partner Program

L3 Common Criteria: A Security Target, a Preparative and Operational User Guidance documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ASE_SPD, AGD_OPE and AGD_PRE (see [CC3V3-1R5]).

No.	Requirement	Security Measures
	L3+ Common Criteria: A Security Target, a Preparative and Operational User Guidance documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by ASE_SPD, AGD_OPE and AGD_PRE (see [CC3V3-1R5]).	

Calibration

No calibration required.

7.5	**L2 Vendor Questionnaire** *Provide* a rationale for how the requirement above is met. *Provide* a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.	(SM-1, SM-28)

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Guidance Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Guidance Documents
- Mapping to Partner Program Requirements
- Source Code

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

~~UAF + U2F + FIDO2; GaVR-1; L2 and higher~~

The security characteristics of the Authenticator SHALL NOT be modifiable by anyone other than the Authenticator device vendor or its delegates.

Relation to Partner Program

L3 Common Criteria: A Security Target, a Preparative and Operational User Guidance documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ASE_SPD, AGD_OPE and AGD_PRE (see [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, a Preparative and Operational User Guidance documents MUST be provided (see [CC1V3-1R5]).

No.	Requirement	Security Measures
	This requirement is addressed by ASE_SPD, AGD_OPE and AGD_PRE (see [CC3V3-1R5]).	

Calibration

No calibration required.

L2 Vendor Questionnaire

Provide a rationale for how the requirement above is met.

Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.

No.	Requirement	Security Measures
7.6	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Guidance Documents • Mapping to Partner Program Requirements • Source Code	(SM-1, SM-28)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Guidance Documents
- Mapping to Partner Program Requirements
- Source Code

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

2.8 Self-Tests and Firmware Updates

No.	Requirement	Security Measures
	UAF + U2F + FIDO2; GaVR-2; L2 and higher An Authenticator SHALL either (a) be resistant to induced fault analysis (requirement 5.9) or (b) after powering up, an Authenticator SHALL run a known answer self-test for any deterministic cryptographic function prior to using that function, or (c) the Authenticator SHALL verify the validity of its software and Firmware using an Allowed Signature Algorithm. If the most recent known answer self-test did not pass, the corresponding cryptographic function SHALL NOT be used.	

Relation to Partner Program

No.	Requirement	Security Measures
	L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FPT_PHP.2 and/or FPT_TST.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	
	L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]). This requirement is addressed by FPT_PHP.3 and/or FPT_TST.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).	

Calibration

No calibration required.

L2 Vendor Questionnaire

Is this requirement applicable to the Authenticator? If **No**, then *describe* why.

Provide a rationale for how the requirement above is met.

Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.

L3 Vendor Questionnaire

8.1	Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	(SM-21, SM-24)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer

No.	test results. **Requirement**	**Security Measures**

UAF + U2F + FIDO2; TVFR; L1 and higher

If the Authenticator mediates the update of its software, then the Authenticator SHALL use an Allowed Data Authentication or Signature Cryptographic Function, as required by the standard referenced in the “Allowed Cryptography List” [FIDOAllowedCrypto], to verify that the software being loaded has not been tampered with. If the loaded software does not pass, then the Authenticator SHALL NOT update the software.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, FPT_TST.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FCS_COP.1, FPT_TST.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

L1 Vendor Questionnaire

Is this requirement applicable to the Authenticator? If **No**, then *describe* why.

If Yes, *provide* the Security Secretariat with a rationale of how the requirement above is met.

L2 Vendor Questionnaire

Is this requirement applicable to the Authenticator? If **No**, then *describe* why.

If Yes, *provide* a rationale for how the requirement above is met.

Provide a documentation review procedure to confirm that the Authenticator’s design is consistent with the provided rationale. Please provide explicit design document references.

8.2 (SM-16, SM-26, SM-24)

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- High Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

No.	Requirement	Security Measures

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; TVFR; L2 and higher

An Authenticator SHALL either (a) be resistant to induced fault analysis (requirement 5.9) or (b) the Authenticator SHALL verify that any generated Authenticator Security Parameters which are public / private keys have the correct mathematical relationships prior to outputting the public key or using the private key for signature generation, or (c) the Authenticator SHALL verify the validity of its software and Firmware using an Allowed Signature Algorithm.

Relation to Partner Program

L3 Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FPT_PHP.2 and/or FPT_TST.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FPT_PHP.3 and/or FPT_TST.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

No calibration required.

L2 Vendor Questionnaire

Is this requirement applicable to the Authenticator? If **No**, then *describe* why.

Provide a rationale for how the requirement above is met.

Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.

8.3	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	(SM-21)

No.	Requirement	Security Measures

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

UAF + U2F + FIDO2; L2+ and higher

An Authenticator SHALL either be resistant to induced fault analysis (requirement 5.9) or the Authenticator SHALL verify that any produced signature is valid prior to outputting the signature.

Relation to Partner Program

L3 Common Criteria:A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FPT_PHP.2 and/or FPT_TST.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

L3+ Common Criteria: A Security Target, Development and Tests documents MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by FPT_PHP.3 and/or FPT_TST.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

L3: At L3, the protection SHALL be strong enough to be protected against *enhanced-basic* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.3 or higher vulnerability analysis (see [CEMV3-1R5]).

L3+: At L3+, the protection SHALL be strong enough to be protected against *moderate* or *high* effort software and hardware attacks [AttackPotentialSmartcards]. The vulnerability assessment methodology is defined by AVA_VAN.4 or higher vulnerability analysis (see [CEMV3-1R5]).

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

No.	Requirement	Security Measures
2d	• High Level Design Documentation • Tests Documents • Mapping to Partner Program Requirements • Source Code	(SM-2.1)

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Low Level Design Documentation
- Tests Documents
- Mapping to Partner Program Requirements
- Source Code

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.

2.9 Manufacturing and Development

NOTE

At L1, the creation of the final Authenticator Application is considered the Authenticator manufacturing.

No.	Requirement	Security Measures
	UAF + U2F + FIDO2; TVFR; L1 and higher If Authenticator Security Parameters which are cryptographic keys are generated during manufacturing, then these keys SHALL be generated as required by the standard referenced in the “Allowed Cryptography List” [FIDOAllowedCrypto] for that algorithm using an Allowed Random Number Generator.	

Relation to Partner Program

L3 Common Criteria: A Security Target, Preparative Guidance and Development Security Life-cycle support documentation MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ASE_SPD, AGD_PRE and ALC_DVS.1 (see [CC3V3-1R5])

L3+ Common Criteria: A Security Target, Preparative Guidance and Development Security Life-cycle support documentation MUST be provided (see [CC1V3-1R5]).

No.	Requirement	Security Measures
	This requirement is addressed by ASE_SPD, AGD_PRE and ALC_DVS.2 (see [CC3V3-1R5])	

Calibration

L1: At L1, the creation of the finalAuthenticator Application is considered the Authenticator manufacturing.

L2: No calibration required.

L3: No calibration required.

L3+: No calibration required.

L1 Vendor Questionnaire

Is this requirement applicable to the Authenticator? If **No**, then *describe* why.

If Yes, *provide* the Security Secretariat with arationale of how the requirement above is met.

L2 Vendor Questionnaire

Is this requirement applicable to the Authenticator? If **No**, then *describe* why.

9.1	If Yes, *describe* how this requirement can be verified through documentation review. Please provide explicit design documentation references.	(SM-28)

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Guidance Documents
- Life-Cycle Support Documents
- Mapping to Partner Program Requirements

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Guidance Documents
- Life-Cycle Support Documents
- Mapping to Partner Program Requirements

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *conduct* a development site audit to validate the security measures defined in the life-

No.	cycle support documents Requirement	Security Measures

UAF + U2F + FIDO2; TVFR; L2 and higher

Access to the private component of any Authenticator's attestation key SHALL be restricted to security-qualified authorized factory personnel.

Relation to Partner Program

L3 Common Criteria: A Security Target, Preparative Guidance and Development Security Life-cycle support documentation MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ASE_SPD, AGD_PRE and ALC_DVS.1 (see [CC1V3-1R5]).

L3+ Common Criteria: A Security Target, Preparative Guidance and Development Security Life-cycle support documentation MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ASE_SPD, AGD_PRE and ALC_DVS.2 (see [CC3V3-1R5]).

Calibration

L2: At L2, security protection controls (physical, procedural, personnel, and other security measures) on the production environment MUST be adequate to provide the confidentiality and integrity of the design and implementation of the Authenticator that is **necessary** to ensure that secure operation of the Authenticator is not compromised.

> NOTE
>
> For example, production machines SHALL NOT be directly connected to unprotected networks (e.g. the Internet).

Only security-qualified authorized factory personnel SHALL have access to all means of processing the handling of attestation key life cycle (generation, provisioning, and verification).

Security measures for protecting the life cycle management of the key generation and key provisioning SHALL be provided in the Vendor Questionnaire.

> NOTE
>
> Security-qualified authorized factory personnel should be limited to a small number of people. It should not be every worker in the factory and it should not be all the development engineers.

9.2	**L3**: At L3, ALC_DVS.1 MUST be applied.	(SM-28)
	L3+: At L3+, ALC_DVS.2 MUST be applied.	

L2 Vendor Questionnaire

Describe how this requirement can be verified through documentation review. Please provide explicit design documentation references.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Life-Cycle Support Documents
- Mapping to Partner Program Requirements

No.	Requirement	Security Measures

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Life-Cycle Support Documents
- Mapping to Partner Program Requirements

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *conduct* a development site audit to validate the security measures defined in the life-cycle support documents

UAF + U2F + FIDO2; TVFR; L2 and higher

The equipment used to generate, store and provision Authenticator Security Parameters SHALL be secured to prevent modification of all provisioned Authenticator Security Parameters and secured to prevent capture of provisioned Secret Authenticator Security Parameters. The equipment used by the authenticator vendor to generate, store and provision other keys whose compromise would affect the security of the Authenticator and the ability to identify it based on certificates in the FIDO Metadata Service [FIDOMetadataService] SHALL also be secured.

Relation to Partner Program

L3 Common Criteria: A Development Security Life-cycle support documentation MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ALC_DVS.1 (see [CC3V3-1R5]).

L3+ Common Criteria: A Development Security Life-cycle support documentation MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ALC_DVS.2 (see [CC3V3-1R5]).

Calibration

L2: At L2, all Authenticator Security Parameters must be protected by some form of integrity protection and all Secret Authenticate Security Parameters must never be exposed in the clear. Use of Allowed Cryptographic Algorithms [FIDOAllowedCrypto] is preferred, but not required for these protections (if the lack of security is compensated by physical controls).

> NOTE
>
> For example, attestation secret keys provisioned over a serial cable between the Authenticator device and the equipment used to store and inject keys should be encrypted and integrity protected to prevent factory personnel from snooping the cable or carrying out a man-in-the-middle attack on the cable.

No.	Requirement	Security Measures
	L3: At L3, ALC_DVS.1 (see [CC3V3-1R5]) MUST be applied.	
9.3	**L3+**: At L3+, ALC_DVS.2 (see [CC3V3-1R5]) MUST be applied.	(SM-28)

L2 Vendor Questionnaire

Describe how this requirement can be verified through documentation review. Please provide explicit design documentation references.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Life-Cycle Support Documents
- Mapping to Partner Program Requirements

L3+ Vendor Questionnaire

TProvide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Life-Cycle Support Documents
- Mapping to Partner Program Requirements

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

The Tester SHALL *conduct* a development site audit to validate the security measures defined in the life-cycle support documents

UAF + U2F + FIDO2; TVFR; L1 and higher

A revision control system SHALL be implemented for the Authenticator and all of its components, and for all associated Authenticator documentation. This revision control system SHALL, at minimum, track changes to all software or hardware specifications, implementation files, and all tool chains used in the production of the final Authenticator.

Relation to Partner Program

L3 Common Criteria: A Configuration Management Scope and Capabilities documentation MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ALC_CMC.4 and ALC_CMS.1 (see [CC3V3-1R5]).

L3+ Common Criteria: A Configuration Management Scope and Capabilities documentation MUST be provided (see [CC1V3-1R5]).

No.	Requirement	Security Measures
	This requirement is addressed by ALC_CMC.4 and ALC_CMS.1 (see [CC3V3-1R5]).	

Calibration

L1: At L1, the use of a revision control system SHALL only be proven for the Authenticator Application.

L2: No calibration required.

L3: No calibration required.

L3+: No calibration required.

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

9.4	**L2 Vendor Questionnaire** *Describe* how this requirement can be verified through documentation review. Please provide explicit design documentation references.	(SM-28)

L3 Vendor Questionnaire

TProvide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Life-Cycle Support Documents
- Mapping to Partner Program Requirements

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Life-Cycle Support Documents
- Mapping to Partner Program Requirements

L1 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *conduct* a development site audit to validate the security measures defined in the life-cycle support documents

~~UAF + U2F + FIDO2; TVFR; L1 and higher~~

Each version of each configuration item that comprises the Authenticator and associated documentation SHALL be assigned a unique identification.

No.		Security Measures

NOTE

"Configuration item" stands for all the objects managed by the configuration management system during the product development. These may be either parts of the product (e.g. source code) or objects related to the development of the product like guidance documents, development tools, tests results, etc.)

Relation to Partner Program

L3 Common Criteria: A Configuration Management Scope and Capabilities documentation MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ALC_CMC.4 and ALC_CMS.1 (see [CC3V3-1R5]).

L3+ Common Criteria: A Configuration Management Scope and Capabilities documentation MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ALC_CMC.4 and ALC_CMS.1 (see [CC3V3-1R5]).

Calibration

L1: At L1, the configuration items comprising the Authenticator Application are relevant.

L2: No calibration required.

L3: No calibration required.

L3+: No calibration required.

L1 Vendor Questionnaire

Provide the Security Secretariat with a rationale of how the requirement above is met.

9.5 (SM-28)

L2 Vendor Questionnaire

Describe how this requirement can be verified through documentation review. Please provide explicit design documentation references.

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Life-Cycle Support Documents
- Mapping to Partner Program Requirements

L3+ Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Life-Cycle Support Documents
- Mapping to Partner Program Requirements

L1 Test Procedure

{A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

No.	Requirement	Security Measures

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *conduct* a development site audit to validate the security measures defined in the life-cycle support documents

UAF + U2F + FIDO2; TVFR; L2 and higher

There SHALL be management and control over all personnel that can enter the physical part of the factory where attestation key material is configured into the authenticators.

> NOTE
>
> This refers to all factory workers possibly including those that have little or nothing to do with the manufacturing line itself, such as cleaning and repair staff. The point of this requirement is to defend against counterfeit devices being run through the manufacturing line to receive real attestation keys. For example, loading dock staff working at 2 AM might conspire to manufacture counterfeit devices.

Relation to Partner Program

L3 Common Criteria: A Development Security Life-cycle support documentation MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ALC_DVS.1 (see [CC3V3-1R5]).

L3+ Common Criteria: A Development Security Life-cycle support documentation MUST be provided (see [CC1V3-1R5]).

This requirement is addressed by ALC_DVS.2 (see [CC3V3-1R5]).

Calibration

L2: At L2, standard per-person badge access systems or standard brass keys and door locks are acceptable. Any personnel without a key or badge MUST be escorted by one with a key or badge.

L3: At L3, ALC_DVS.1 (see [CC3V3-1R5]) must be applied.

L3+: At L3+, ALC_DVS.2 (see [CC3V3-1R5]) must be applied.

9.6	**L2 Vendor Questionnaire** *Describe* how this requirement can be verified through documentation review. Please provide explicit design documentation references.	(SM-28)

L3 Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Life-Cycle Support Documents

No.	Requirement	Security Measures
	• Mapping to Partner Program Requirements	

L3+ Vendor Questionnaire

TProvide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents:

- Life-Cycle Support Documents
- Mapping to Partner Program Requirements

L2 Test Procedure

{A2} The tester SHALL *conduct* the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.

L3 Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

L3+ Test Procedure

The Tester SHALL *verify* the provided rationale and documentation meets the requirement.

The Tester SHALL *execute* a sample of tests from the tests documentation provided to verify the developer test results.

The Tester SHALL *conduct* a development site audit to validate the security measures defined in the life-cycle support documents

A. References

A.1 Normative references

[AttackPotentialSmartcards]
Application of Attack Potential to Smartcards January 2013. URL: https://www.sogis.org/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v2-9.pdf

[BEAT]
N. Tekampe; A. Merle; J. Bringer; M. Gomez-Barrero; J. Fierrez; J. Galbally (UAM). *BEAT: Towards the Common Criteria evaluations of biometric systems*. URL: https://www.beat-eu.org/project/deliverables-public/d6-5-toward-common-criteria-evaluations-of-biometric-systems

[CAFVM]
. *CCDB-2008-09-002 Characterizing Attacks to Fingerprint Verification Mechanisms* 2011. published. URL: https://www.commoncriteriaportal.org/files/supdocs/CCDB-2008-09-002.pdf

[CC1V3-1R5]
CCMB-2017-04-001 Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. April 2017. URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[CC2V3-1R5]
CCMB-2017-04-001 Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. April 2017. URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

[CC3V3-1R5]
CCMB-2017-04-001 Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. April 2017. URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[CEMV3-1R5]
CCMB-2017-04-004 Common Methodology for Information Technology Security Evaluation - Evaluation Methodology. April 2017. URL: https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf

[FIDO-SR-Mapping-Table]
R. Atoui; J. Hill. *FIDO Security Requirements Partner Program Mapping Table* Working Draft. URL:

[FIDOAllowedCrypto]
Dr. Joshua E. Hill; Douglas Biggs. *FIDO Authenticator Allowed Cryptography List*. August 2017. Draft. URL: https:./fido-authenticator-allowed-cryptography-list-v1.0-wd-20180629.html

[FIDOBiometricsRequirements]
Meagan Karlsson. *FIDO Biometrics Requirements*. June 2017. Draft. URL: https://drafts.fidoalliance.org/biometrics/requirements/latest/

[FIDOEcdaaAlgorithm]
R. Lindemann; J. Camenisch; M. Drijvers; A. Edgington; A. Lehmann; R. Urian. *FIDO ECDAA Algorithm*. Review Draft. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-ecdaa-algorithm-v1.2-rd-20171128.html

[FIDOGlossary]
R. Lindemann; D. Baghdasaryan; B. Hill; J. Hodges. *FIDO Technical Glossary*. Implementation Draft. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-glossary-v1.2-rd-20171128.html

[FIDOMetadataRequirements]
Meagan Karlsson. *FIDO Authenticator Metadata Requirements*. June 2017. Draft. URL: https:./fido-authenticator-metadata-requirements-v1.0-wd-20180629.html

[FIDOMetadataStatement]
B. Hill; D. Baghdasaryan; J. Kemp. *FIDO Metadata Statements v1.0*. Implementation Draft. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-metadata-statement-v1.2-rd-20171128.html

[FIDORestrictedOperatingEnv]
Laurence Lundblade; Meagan Karlsson. *FIDO Authenticator Allowed Restricted Operating Environments List*. August 2017. Draft. URL: https:./fido-authenticator-allowed-restricted-operating-environments-list-v1.0-wd-20180629.html

[FIDOSecRef]
R. Lindemann; D. Baghdasaryan; B. Hill. *FIDO Security Reference*. Implementation Draft. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-security-ref-v1.2-rd-20171128.html

[FIPS140-2]
FIPS PUB 140-2: Security Requirements for Cryptographic Modules. May 2001. URL: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[FSDPP]
. *BSI-CC-PP-0063 Fingerprint Spoof Detection Protection Profile (FSDPP)*. 2009. URL: http://biometrics.nist.gov/cs_links/ibpc2010/pdfs/Henniger2_Olaf_IBPC_Paper.pdf

[JCPP]
. *Java Card Protection Profile - Open Configuration*. May 2012. URL: https://www.commoncriteriaportal.org/files/ppfiles/ANSSI-CC-profil_PP-2010-03en.pdf

[PP0084]
. *BSI-CC-PP-0084-2014 Security IC Platform Protection Profile with Augmentation Packages*. URL: https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf

[U2FImplCons]
D. Balfanz. *FIDO U2F Implementation Considerations v1.0*. Draft. URL: https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-implementation-considerations-v1.2-ps-20170411.html

[U2FPP]
. *BSI-PP-CC-0096-2017 FIDO Universal Second Faction (U2F) Authenticator Common Criteria Protection Profile*. 26 June 2017. In Development. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0096b_pdf.pdf?__blob=publicationFile&v=2

[U2FRawMsgs]
D. Balfanz. *FIDO U2F Raw Message Formats v1.0*. Proposed Standard. URL: https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-raw-message-formats-v1.2-ps-20170411.html

[UAFAuthnrCommands]
D. Baghdasaryan; J. Kemp; R. Lindemann; R. Sasson; B. Hill. *FIDO UAF Authenticator Commands v1.0*. Implementation Draft. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-uaf-authnr-cmds-v1.2-rd-20171128.html

[UAFProtocol]
R. Lindemann; D. Baghdasaryan; E. Tiffany; D. Balfanz; B. Hill; J. Hodges. *FIDO UAF Protocol Specification v1.0*. Proposed Standard. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-uaf-protocol-v1.2-rd-20171128.html

[WebAuthn]
Vijay Bharadwaj; Hubert Le Van Gong; Dirk Balfanz; Alexis Czeskis; Arnar Birgisson; Jeff Hodges; Michael B. Jones; Rolf Lindemann; J. C. Jones. *Web Authentication: An API for accessing Scoped Credentials*. September 2016. Draft. URL: https://www.w3.org/TR/webauthn/

A.2 Informative references

[FIDOMetadataService]

R. Lindemann; B. Hill; D. Baghdasaryan. *FIDO Metadata Service v1.0*. Implementation Draft. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-metadata-service-v1.2-rd-20171128.html

[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

[SP800-132]
Meltem Sönmez Turan; Elaine Barker; William Burr; Lily Chen. *NIST Special Publication 800-132: Transitions: Recommendation for Password-Based Key Derivation*. December 2010. URL: http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf

[UAFRegistry]
R. Lindemann; D. Baghdasaryan; B. Hill. *FIDO UAF Registry of Predefined Values*. Proposed Standard. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-uaf-reg-v1.2-rd-20171128.html

FIDO Authenticator Allowed Cryptography List

FIDO Alliance 29 June 2018

This version:
https://fidoalliance.org/specs/fido-v1.0--20180629/fido-allowed-crypto-v1.0--20180629.html
Previous version:
fido-authenticator-allowed-cryptography-list-v1.0-fd-20170524.html
Editors:
Dr. Joshua E. Hill, InfoGard Laboratories
Douglas Biggs, InfoGard Laboratories

Abstract

This document helps support the FIDO Authenticator Security Certification program. This list does not in any way alter the protocol specifications provided in other FIDO Authenticator documents, so the presence or absence of an algorithm in this list does not suggest that this algorithm is or is not allowed within any FIDO protocol. For certified FIDO Authenticators, there are various requirements that limit “internal” algorithms, those that are not explicitly specified within the FIDO Authenticator protocol. Additionally, the procedure for determining the “Overall Authenticator Claimed Cryptographic Strength” involves locating the security level for each algorithm used by the FIDO Authenticator within this document; this procedure applies to all cryptographic algorithms used by the FIDO Authenticator.

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://www.fidoalliance.org.

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 Requirements 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 the Requirements 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 REQUIREMENTS 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.

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].

1.1 Version

This document specifies version 1.2.0 of the allowed cryptography (CV).

2. Requirements for Additional Candidates

If a vendor wants to use a cryptographic security function for an internal use that requires an Allowed algorithm, or to claim a non-zero security strength, then the vendor / lab shall provide a written argument that it:

- Additional candidates for algorithms shall at least support a cryptographic strength of 112 bits.
- Is not a proprietary solution,
- Fulfills the required security attributes (e.g., if the use requires confidentiality and data authentication, the primitive provides this),
- Has a security strength that can be readily characterized,
- Is accepted by at least one major standards group (e.g., NIST, ANSI, ISO, IETF), and
- Has undergone extensive public review.

3. Allowed Cryptographic Functions

The stated security level identifies the expected number of computations that a storage-constrained attacker (who has access to no more than 2^80 bytes of storage) shall expend in order to compromise the security of the cryptographic security function, under the currently best known attack that can be conducted under this storage constraint. This has been extracted from the currently best known relevant attacks against each cryptographic primitive, and is expected to shift over time as attacks improve.

If the security level stated is n, then the expected number of computations is less than the expected number of computations required to guess an (n+1)-bit random binary string, and not less than the number of computations required to guess an n bit random binary string (i.e., on average, the number of computations required is less than 2^n computations and greater than or equal to 2^(n-1) computations).

3.1 Confidentiality Algorithms

> NOTE
>
> Provide confidentiality, up to the stated security level.

Algorithm	Specified in	Security Level (bits)
Three-Key Triple-DES	[ANSI-X9-52]	112[1]
AES-128	[FIPS197]	128
AES-192	[FIPS197]	192
AES-256	[FIPS197]	256

Three-key triple-DES is not allowed for any certification issued after January 1, 2020. This is due to the increased applicability of a weaknesses shared by all block ciphers with a 64-bit block size, and similar deprecation plans by other certification programs.

> NOTE
>
> Since it can take many months to complete a certification it is suggested that no authenticators using three-key triple-DES start the certification process after July 1, 2019 so they likely have enough time to complete the certification process before January 1, 2020.

[1] Based on the standard meet-in-the-middle attack.

3.2 Hashing Algorithms

> NOTE
>
> Provide pre-image resistance, 2nd pre-image resistance, and collision resistance.

Algorithm	Specified in	Security Level (bits)
SHA-256	[FIPS180-4]	128
SHA-384	[FIPS180-4]	192
SHA-512	[FIPS180-4]	256
SHA-512/t, 256 ≤ t < 512	[FIPS180-4]	t/2
SHA3-256	[FIPS202]	128
SHA3-384	[FIPS202]	192
SHA3-512	[FIPS202]	256

3.3 Data Authentication Algorithms

> NOTE
>
> Provide data authentication.

Algorithm	Specified in	Security Level (bits)
HMAC	[FIPS198-1]	Minimum of the length of the output of the hash used[2], one-half of the number of bits in the hash state[3], or the number of bits in the HMAC key.
CMAC	[SP800-38B]	Equal to the minimum of the strength of the underlying cipher and the length of the output MAC.
GMAC	[SP800-38D]	Equal to the minimum of the strength of the underlying cipher and the length of the output MAC.

[2]Both due to the obvious guessing attack, and covers the case where the supplied key is hashed for the HMAC.

[3]Based on a birthday attack; a collision of the final state can lead to an existential forgery of longer messages with the same prefix.

3.4 Key Protection Algorithms

> NOTE
>
> Provide confidentiality and data authentication.

Algorithm	Specified in	Security Level (bits)
Key Wrapping	[SP800-38F]	Equal to the strength of the underlying cipher.
GCM Mode, with length 96 bit or larger IVs. For any given key, the IV length must be fixed.	[SP800-38D]	Equal to the strength of the underlying cipher.
RSA OAEP	[RFC3447]. Key generation must be according to [FIPS186-4].	112
CCM Mode	[SP800-38C]	Equal to the strength of the underlying cipher.
Encrypt-then-HMAC[4]	Encryption specification depends on the cipher selected. HMAC specification [FIPS198-1]	The minimum of the strength of the cipher and the HMAC.
Encrypt-then-CMAC[5]	Encryption specification depends on the cipher selected. CMAC specification [SP800-38B]	The minimum of the strength of the cipher and the CMAC.

[4]The cipher and HMAC shall use independent keys, and the information HMACed shall include any IV / Nonce / Counter (if sent/stored), and, if the message size varies, the length of the message; when present, this message length shall reside prior to any variable length message components.

[5]The cipher and CMAC shall use independent keys, and the information CMACed shall include any IV / Nonce / Counter (if sent/stored).

3.5 Random Number Generator

In FIDO an allowed random number generator shall meet the requirements of one of the following sub sections.

Evidence that the requirements are met could be given by providing a proof that the implementation uses the underlying platform certified RNG/RBG through Common Criteria, FIPS 140-2 (issued on August 7th 2015 or after) or an equivalent evaluation scheme against the listed standards, or by having a FIDO approved lab conducting an evaluation of the RNG/RBG implementation against the standards listed below. In other words, the following standards define the metrics required to assess the quality of the RNG implementation.

> NOTE
>
> If the designer is interested in retaining the security of an (EC)DSA private key in the event of an entropy source failure or Deterministic Random Number Generator state compromise, then RFC6979-like properties can be obtained by providing the hash of the message being signed and the private key in use to the Deterministic Random Number Generator in a secure fashion (e.g., via the SP800-90A additional input parameter). Additional parameters (e.g., the KeyID / Key Handle, if it was randomly generated) may also be used to increase resistance to attack in certain scenarios.

> NOTE
>
> The August 7th 2015 date for FIPS 140-2 reflects the date that FIPS 140-2 IG7.15 came into effect, which provided an explict set of requiremnets for the evaluation of the security of seeding sources for allowed DRBGs.

3.5.1 Physical/True (TRNG)/Non-Deterministic Random Number/Bit Generator(NRBG) Requirements

The (physical) random number generator shall meet the requirements specified in:

1. AIS 20/31 PTG.2 or PTG.3 or in

> NOTE
>
> If PTG.2 is used, an application-specific post processing may additionally be required to prevent any bias in the output function.

> For instance, these requirements are met if a certified hardware platform is used (e.g. according to Global Platform TEE Protection Profile or Eurosmart Security IC Platform Protection Profile) and the Security Target contains Extended Component FCS_RNG.1 including at least one of the allowed classes PTG.2, or PTG.3.

2. NIST SP800-90C NRBG [SP800-90C] or in

Algorithm	Specified in	Security Level (bits)
Source RBG is DRBG with access to Live Entropy Source or it is an NRBG.	[SP800-90C], section 6	Any security strength.

3. NIST FIPS 140-2 [FIPS140-2] validation (issued on August 7th 2015 or after), with Entropy Source Health Tests. The related security level is as defined in the module's security policy.

   We consider this a physical RNG if at least as much entropy is added into the RNG as is retrieved per request.

> NOTE
>
> It is uncommon for the DRBGs in FIPS modules to meet these requirements, unless their design anticipates one of the SP800-90C NRBG designs.

The security strength (in bits) of an allowed physical/true random number generator is equivalent to the size (in bits) of the random bytes retrieved from it.

3.5.2 Deterministic Random Number (DRNG)/Bit Generator (DRBG) Requirements

> NOTE
>
> Provide computational indistinguishability from an ideal random sequence, cycle resistance, non-destructive reseeding, insensitivity of a seeded generator to seed source failure or compromise, backtracking resistance. Ideally, the ability to provide additional input, and ability to recover from a compromised internal state.

The (deterministic) random number generator shall meet the requirements specified in:

1. AIS 20/31 DRG.3 or DRG.4 (having an entropy of the seed of at least N bits, where N is the targeted security level) or in
2. NIST SP800-90A DRBG [SP800-90ar1],

Algorithm	Specified in	Security Level (bits)
HMAC_DRBG	[SP800-90ar1], Revision 1, section 10.1.2	The instantiated security level, as defined in [SP800-90ar1].
CTR_DRBG	[SP800-90ar1], Revision 1, section 10.2.1	The instantiated security level, as defined in [SP800-90ar1].
HASH_DRBG	[SP800-90ar1], Revision 1, section 10.1.1	The instantiated security level, as defined in [SP800-90ar1].

3. or in NIST FIPS 140-2 [FIPS140-2] validation (issued on August 7th 2015 or after).

> NOTE
>
> We consider this a deterministic RNG if less entropy is added into the RNG than is retrieved.

> NOTE
>
> The [SP800-90ar1] standard requires that the DRBG must be seeded using either another [SP800-90ar1] Approved DRBG, or an Approved [SP800-90b] entropy source. [FIPS140-2] further allows for testing as described in IG7.15.

3.6 Key Derivation Functions (KDFs)

Deriving keys.

Algorithm	Specified in	Security Level (bits)
KDF in counter mode	[SP800-108]	min(Bit length of key derivation key Ki used as input, Security level of PRF)
KDF in feedback mode	[SP800-108]	min(Bit length of key derivation key Ki used as input, Security level of PRF)
KDF in double pipeline iteration mode	[SP800-108]	min(Bit length of key derivation key Ki used as input, Security level of PRF)
HKDF	[SP800-56cr1], [RFC5869]	min(Bit length of key derivation key Ki used as input, Security level of HMAC)

Where PRF denotes an acceptable pseudorandom function as defined in [SP800-108].

3.7 Signature Algorithms

> NOTE
>
> Provide data authentication, and non-repudiation.

Algorithm	Specified in	Security Level (bits)
ECDSA on P-256	[ECDSA-ANSI], [FIPS186-4]	128
2048-bit RSA PSS	[FIPS186-4]	112
1024*n-bit RSA PKCS v1.5 (n=2,3,4)	[FIPS186-4]	112
ECDSA on secp256k1	[ECDSA-ANSI], [FIPS186-4], Certicom SEC 2	126[7]
SM2 digital signatures (SM2 part 2) using the SM3 hash on the SM2 curve specified by OSCCA.	SM2 1 , SM3	128
Ed25519	EDDSA [RFC8032]	128[8]

[7] Based on an attack using Pollard rho on the equivalence classes defined by the curve's easily computable endomorphism.

[8] Based on the difficulty of performing discrete logs on the group defined by the recommended curve parameters.

3.8 Anonymous Attestation Algorithms

> NOTE
>
> Provide anonymous attestation.

The strength in this section is the minimum of three values:

1. The strength of the underlying hash.
2. The difficulty of conducting a discrete log within the Elliptic Curve.
3. The difficulty of conducting a discrete log within a finite field in which the Elliptic Curve can be embedded (we'll refer to this field as the embedding field).

In most cases, the limiting factor was the difficulty of performing the discrete log calculation within the embedding field.

The security level values here were taken from NIST guidance. This NIST guidance is based on conducting the discrete log calculation within prime ordered fields; the structure of the fields here is richer, and this structure could possibly allow for a more advanced discrete log approach that could be considerably faster. Currently, the best known algorithms in both cases have the same asymptotic complexity (Lq [1⁄3]), but without extensive testing, it isn't clear how the number of computations compares.

In addition, the NIST guidance does not allow for security levels other than a few specific proscribed values: if the number of bits required to represent the order of the embedding field is between 3072 and 7679, the security level is reported as 128

bits. Similarly, if the number of bits required to represent the order of the embedding field is between 2048 and 3071, the security strength is reported as 112 bits.

Algorithm	Specified in	Security Level (bits)
ED256	[FIDOEcdaaAlgorithm], section Object Formats and Algorithm Details, [TPMv2-Part4]	128
ED256-2	[FIDOEcdaaAlgorithm], section Object Formats and Algorithm Details, [DevScoDah2007]	112
ED512	[FIDOEcdaaAlgorithm], section Object Formats and Algorithm Details, [ISO15946-5]	128
ED638	[FIDOEcdaaAlgorithm], section Object Formats and Algorithm Details, [TPMv2-Part4]	128

A. References

A.1 Normative references

[ANSI-X9-52]
Triple Data Encryption Algorithm Modes of Operation. July 29, 1998. Current. URL:

[DevScoDah2007]
Augusto Jun Devegili; Michael Scott; Ricardo Dahab. *Implementing Cryptographic Pairings over Barreto-Naehrig Curves*. 2007. URL: https://eprint.iacr.org/2007/390.pdf

[ECDSA-ANSI]
Public Key Cryptography for the Financial Services Industry - Key Agreement and Key Transport Using Elliptic Curve Cryptography ANSI X9.63-2011 (R2017). 2017. URL: https://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.63-2011+(R2017)

[FIDOEcdaaAlgorithm]
R. Lindemann; J. Camenisch; M. Drijvers; A. Edgington; A. Lehmann; R. Urian. *FIDO ECDAA Algorithm*. Review Draft. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-ecdaa-algorithm-v1.2-rd-20171128.html

[FIPS140-2]
FIPS PUB 140-2: Security Requirements for Cryptographic Modules. May 2001. URL: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[FIPS180-4]
FIPS PUB 180-4: Secure Hash Standard (SHS). March 2012. URL: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

[FIPS186-4]
FIPS PUB 186-4: Digital Signature Standard (DSS). July 2013. URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[FIPS197]
FIPS PUB 197: Specification for the Advanced Encryption Standard (AES). November 2001. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[FIPS198-1]
FIPS PUB 198-1: The Keyed-Hash Message Authentication Code (HMAC). July 2008. URL: http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

[FIPS202]
FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions August 2015. URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

[ISO15946-5]
ISO/IEC 15946-5 Information Technology - Security Techniques - Cryptographic techniques based on elliptic curves - Part 5: Elliptic curve generation. URL: https://webstore.iec.ch/publication/10468

[RFC3447]
J. Jonsson; B. Kaliski. *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*. February 2003. Informational. URL: https://tools.ietf.org/html/rfc3447

[RFC5869]
H. Krawczyk; P. Eronen. *HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*. May 2010. Informational. URL: https://tools.ietf.org/html/rfc5869

[RFC8032]
S. Josefsson; I. Liusvaara. *Edwards-Curve Digital Signature Algorithm (EdDSA)*. January 2017. Informational. URL: https://tools.ietf.org/html/rfc8032

[SP800-108]
Lily Chen. *NIST Special Publication 800-107: Recommendation for Key Derivation Using Pseudorandom Functions* October 2009. URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf

[SP800-38B]
M. Dworkin. *NIST Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC*

Mode for Authentication. May 2005. URL: http://dx.doi.org/10.6028/NIST.SP.800-38B

[SP800-38C]
M. Dworkin. *NIST Special Publication 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*. July 2007. URL: http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf

[SP800-38D]
M. Dworkin. *NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. November 2007 URL: https://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

[SP800-38F]
M. Dworkin. *NIST Special Publication 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*. December 2012. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf

[SP800-56cr1]
Elaine Barker; Lily Chen; Rich Davis. *NIST Special Publication 800-56C revision 1: Recommendation for Key Derivation Methods in Key Establishment Schemes*. April 2018. URL: https://doi.org/10.6028/NIST.SP.800-56Cr1

[SP800-90C]
Elaine Barker; John Kelsey. *NIST Special Publication 800-90C: Recommendation for Random Bit Generator (RBG) Constructions*. August 2012. URL: http://csrc.nist.gov/publications/drafts/800-90/sp800_90c_second_draft.pdf

[SP800-90ar1]
Elaine Barker; John Kelsey. *NIST Special Publication 800-90a: Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. August 2012. URL: http://dx.doi.org/10.6028/NIST.SP.800-90Ar1

[SP800-90b]
Elaine Barker; John Kelsey. *NIST Special Publication 800-90b: Recommendation for the Entropy Sources Used for Random Bit Generation*. April 2016. URL: http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90b.pdf

[TPMv2-Part4]
Trusted Platform Module Library, Part 4: Supporting Routines URL: http://www.trustedcomputinggroup.org/files/static_page_files/8C6CABBC-1A4B-B294-D0DA8CE1B452CAB4/TPM%20Rev%202.0%20Part%204%20-%20Supporting%20Routines%2001.16-code.pdf

A.2 Informative 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

FIDO Authenticator Allowed Restricted Operating Environments List

FIDO Alliance 29 June 2018

This version:
https://fidoalliance.org/specs/fido-v1.0--20180629/fido-allowed-AROE-v1.0--20180629.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://www.fidoalliance.org.

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 Requirements 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 the Requirements 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 REQUIREMENTS 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.

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.

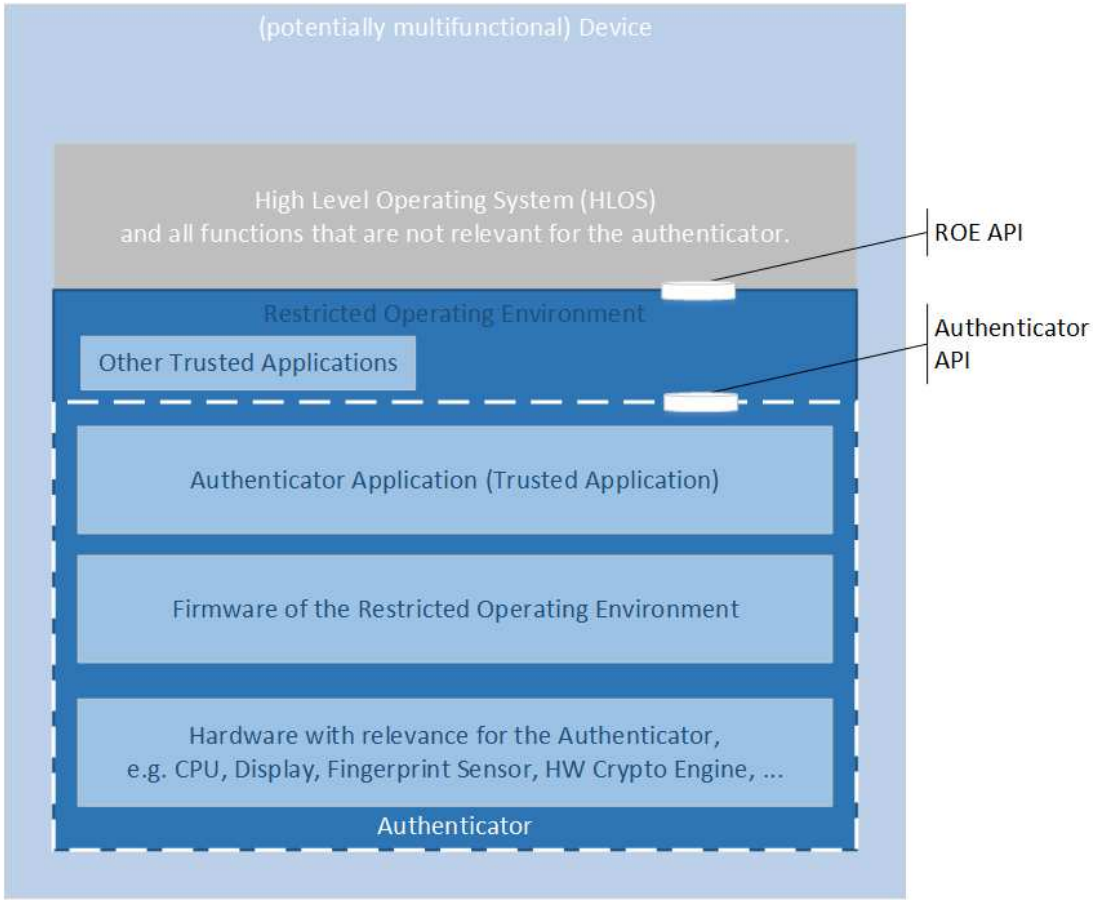

Fig. 1 Restricted Operating Environments Architectural Overview

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 Level 1, we are concenred about the protection against scalable attacks on the server side an on the communication channel. At FIDO Security Levels 2 and 3, we are mostly concerned about the protection against client side scalable attacks (e.g. malware). At FIDO Security Levels 4 and 5 we also require protection against physical attacks.

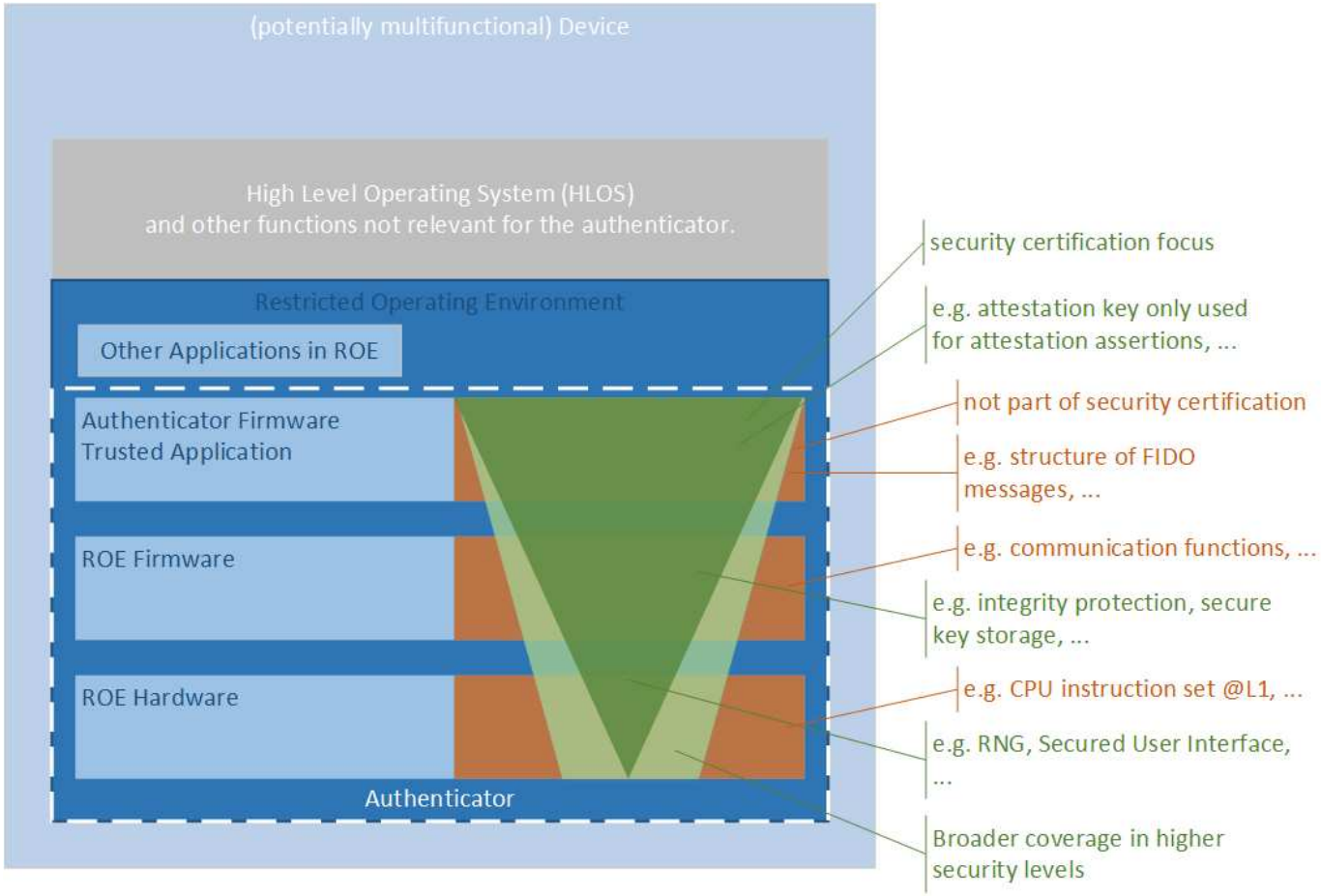

Fig. 2 Restricted Operating Environments Security Certification Focus

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

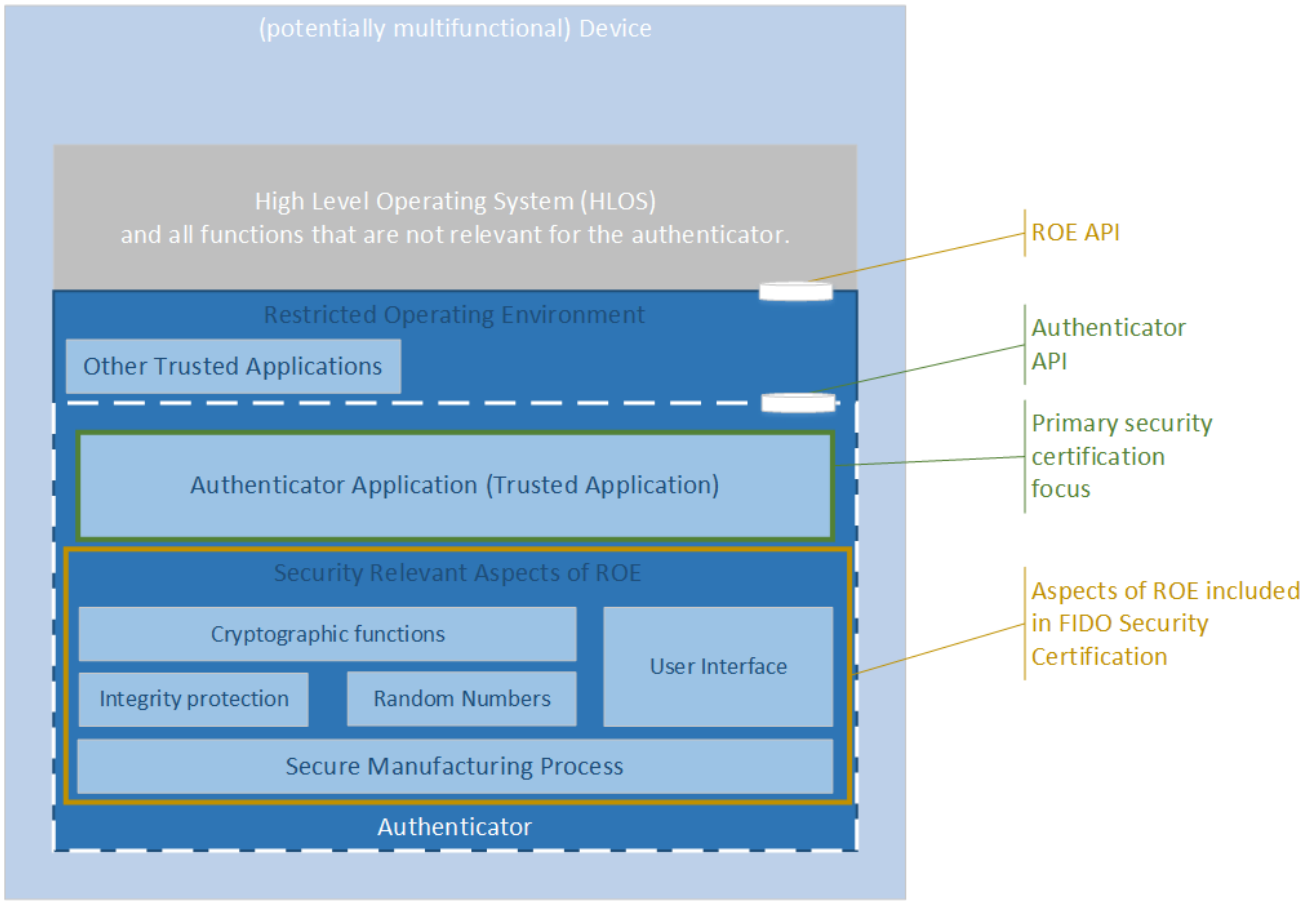

Fig. 3 AROE Aspects Relevant for FIDO Security Certification

3. Allowed Restricted Operating Environments

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

Operating Environment	Notes
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 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 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 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 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
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.
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] are accepted as AROE as required for Level 2 FIDO Authenticator Certification.
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.

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. URL: http://www.trustedcomputinggroup.org/resources/tpm_main_specification

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

FIDO Authenticator Metadata Requirements

FIDO Alliance 29 June 2018

This version:
https://fidoalliance.org/specs/fido-v1.0--20180629/fido-auth-metadata-v1.0--20180629.html
Editor:
Meagan Karlsson, FIDO Alliance

Abstract

This document supports the FIDO Authenticator Certification program.

The fields in the Authenticator Metadata will be the primary method of communicating Authenticator Certification status and details about implementations to Relying Parties (RPs).

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://www.fidoalliance.org.

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 Requirements 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 the Requirements 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 REQUIREMENTS 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.

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

This document reflects the Metadata Requirements for Authenticator Certification.

Mandatory fields are required to be evaluated by the FIDO Security Secretariat (Level 1), or the FIDO Accredited Security Laboratory (Level 2+) and submitted to FIDO as part of the Certification Request. Submitted metadata will be verified to be an accurate representation of the implementation.

Submission of Metadata to the FIDO Metadata Service (MDS) is optional, and can be done after recieving FIDO Authenticator Certification. If Metadata is submitted to MDS, the elements marked herin as Mandatory must be submitted and must match the Metadata submitted to FIDO during Authenticator Certification.

Functional Metadata Fields

The following Functional Metadata Fields are Mandatory for Authenticator Certification.

Field	Section	Description
VerificationMethodDescriptor	3.4	A descriptor for a specific base user verification method as implemented by the authenticator. A base user verification method must be chosen from the list of those described in [FIDORegistry].
verificationMethodANDCombination	3.5	VerificationMethodANDCombinations must be non-empty. It is a list containing the base user verification methods which must be passed as part of a successful user verification.
AAID	4.1	The Authenticator Attestation ID. See [UAFProtocol] for the definition of the AAID structure. This field must be set if the authenticator implements FIDO UAF.
AAGUID	4.1	The Authenticator Attestation GUID. See [FIDOKeyAttestation] for the definition of the AAGUID structure. This field must be set if the authenticator implements FIDO 2.0.
attestationCertificateKeyIdentifiers	4.1	A list of the attestation certificate public key identifiers encoded as hex string. This value must be calculated according to method 1 for computing the keyIdentifier as defined in [RFC5280] section 4.2.1.2. The hex string must not contain any non-hex characters (e.g. spaces). All hex letters must be lower case. This field must be set if neither AAID nor AAGUID are set. Setting this field implies that the attestation certificate(s) are dedicated to a single authenticator model.
description	4.1	A human-readable short description of the Authenticator.
authenticatorVersion	4.1	Earliest (i.e. lowest) trustworthy authenticatorVersion meeting the requirements specified in this metadata statement. Adding new StatusReport entries with status UPDATE_AVAILABLE to the metadata TOC object [FIDOMetadataService] must also change this authenticatorVersion if the update fixes severe security issues, e.g. the ones reported by preceding StatusReport entries with status code USER_VERIFICATION_BYPASS, ATTESTATION_KEY_COMPROMISE, USER_KEY_REMOTE_COMPROMISE, USER_KEY_PHYSICAL_COMPROMISE, REVOKED.
protocolFamily	4.1	The FIDO protocol family. The values "uaf", "u2f", and "fido2" are supported. If this field is missing, the assumed protocol family is "uaf".
upv	4.1	The FIDO unified protocol version(s) (related to the specific protocol family) supported by this authenticator. See [UAFProtocol] for the definition of the Version structure.
userVerificationDetails	4.1	A list of alternative VerificationMethodANDCombinations. Each of these entries is one alternative user verification method. Each of these alternative user verification methods might itself be an "AND" combination of multiple modalities. All effectively available alternative user verification methods must be properly specified here. A user verification method is considered effectively available if this method can be used to either: 1) enroll new verification reference data to one of the user verification methods, or 2) unlock the UAuth key directly after successful user verification.
attachmentHint	4.1	A 32-bit number representing the bit fields defined by theATTACHMENT_HINT

Field	Section	Description
isSecondFactorOnly	4.1	Indicates if the authenticator is designed to be used only as a second factor, i.e. requiring some other authentication method as a first factor (e.g. username+password).
tcDisplay	4.1	A 16-bit number representing a combination of the bit flags defined by the TRANSACTION_CONFIRMATION_DISPLAY constants in the FIDO Registry of Predefined Values [FIDORegistry]. This value must be 0, if transaction confirmation is not supported by the authenticator.
tcDisplayContentType	4.1	Supported MIME content type [RFC2049] for the transaction confirmation display, such as text/plain or image/png. This value must be present if transaction confirmation is supported, i.e. tcDisplay is non-zero.

3. Security Metadata Fields

The following Security-related Metadata Fields are Mandatory for Authenticator Certification.

Field	Section	Description
CodeAccuracyDescriptor	3.1	The *CodeAccuracyDescriptor* describes the relevant accuracy/complexity aspects of passcode user verification methods.
PatternAccuracyDescriptor	3.3	The *PatternAccuracyDescriptor* describes relevant accuracy/complexity aspects in the case that a pattern is used as the user verification method.
EcdaaTrustAnchor	3.8	In the case of ECDAA attestation, the ECDAA-Issuer's trust anchor must be specified in this field.
attestationRootCertificate	3.8	In the case of ECDAA attestation, the ECDAA-Issuer's trust anchor must be specified in this field.
assertionScheme	4.1	The assertion scheme supported by the authenticator. Must be set to one of the enumerated strings defined in the FIDO UAF Registry of Predefined Values [UAFRegistry].
authenticationAlgorithm	4.1	The authentication algorithm supported by the authenticator. Must be set to one of the ALG_ constants defined in the FIDO Registry of Predefined Values [FIDORegistry]. This value must be non-zero.
publicKeyAlgAndEncoding	4.1	The public key format used by the authenticator during registration operations. Must be set to one of the ALG_KEY constants defined in the FIDO Registry of Predefined Values [FIDORegistry]. Because this information is not present in APIs related to authenticator discovery or policy, a FIDO server must be prepared to accept and process any and all key representations defined for any public key algorithm it supports. This value must be non-zero.
attestationTypes	4.1	The supported attestation type(s). (e.g. TAG_ATTESTATION_BASIC_FULL) See UAF Registry for more information [UAFRegistry].
keyProtection	4.1	A 16-bit number representing the bit fields defined by the KEY_PROTECTION constants in the FIDO Registry of Predefined Values [FIDORegistry]. This value must be non-zero.
matcherProtection	4.1	A 16-bit number representing the bit fields defined by the MATCHER_PROTECTION constants in the FIDO Registry of Predefined Values [FIDORegistry]. This value must be non-zero.
isKeyRestricted	2.16	This entry is set to true, if the Uauth private key is restricted by the authenticator to only sign valid FIDO signature assertions. This entry is set to false, if the authenticator doesn't restrict the Uauth key to only sign valid FIDO signature assertion. In this case, the calling application could potentially get any hash value signed by the authenticator. If this field is missing, the assumed value is isKeyRestricted=true.
isFreshUserVerificationRequired		This entry is set to true, if Uauth key usage always requires a fresh user verification. If this field is missing, the assumed value is isFreshUserVerificationRequired=true. This entry is set to false, if the Uauth key can be used without requiring a fresh user verification, e.g. without any additional user interaction, if the user was verified a (potentially configurable) caching time ago. In the case of isFreshUserVerificationRequired=false, the FIDO server MUST verify the registration response and/or authentication response and verify that the (maximum) caching time (sometimes also called "authTimeout") is acceptable. This

Field	Section	Description
		entry solely refers to the user verification. In the case of transaction confirmation, the authenticator MUST always ask the user to authorize the specific transaction.

4. Biometric Metadata Fields

Providing the biometry related Metadata Statement field (i.e. *BiometricAccuracyDescriptor*) [FIDOMetadataStatement] is not mandatory for passing FIDO Authenticator Certification.

Use of Metadata Service 1.1 Status Dictionary

SRWG recommends the use of the Status Dictionary to report the issue dates of Certifications within the array of status report entries. Default status to as “not FIDO Certified” and status is updated to include Certifications as they are achieved. Each Certification would have a separate entry.

New Authenticator Certification Fields

SRWG recommends the following fields to be added to MDS, and that they become Mandatory for Security Certification.

Field	Description
certificationDescriptor (in StatusReport)	Describes the externally visible aspects of the Security Certification evaluation.
certificateNumber (in StatusReport)	The Authenticator certificate number. This is a unique per-Security Certified implementation identifier.
certificationRequirementsVersion (in Status Report)	The Document Version of the Authenticator Security Requirements (DV) [FIDOAuthenticatorSecurityRequirements] the implementation is certified to, e.g. "1.2.0".
cryptoStrength (in Metadata Statement)	A claimed level of the overall cryptographic security, intended to give a Relying Party or consumer some insight into the level of cryptographic security supported by the Authenticator. Each key used by the Authenticator has a specified Cryptographic Strength, and the overallClaimedCryptographicStrength is less than or equal to the smallest of these Cryptographic Strengths. If this field is absent it indicates an unknown claimed overall cryptographic strength. For L2+ certified Authenticators the claimed overall cryptographic strength MUST be known and specified.
operatingEnv (in Metadata Statement)	A description of the particular operating environment that is used for the Authenticator. These are specified in [FIDORestrictedOperatingEnv].

A. References

A.1 Normative references

[FIDOAuthenticatorSecurityRequirements]
Rolf Lindemann; Dr. Joshua E. Hill; Douglas Biggs. *FIDO Authenticator Security Requirements*. August 2017. Draft. URL: https:./fido-authenticator-security-requirements-v1.0-wd-20180629.html

[FIDOKeyAttestation]
FIDO 2.0: Key attestation format. URL: https://fidoalliance.org/specs/fido-v2.0-ps-20150904/fido-key-attestation-v2.0-ps-20150904.html

[FIDOMetadataService]
R. Lindemann; B. Hill; D. Baghdasaryan. *FIDO Metadata Service v1.0*. Implementation Draft. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-metadata-service-v1.2-rd-20171128.html

[FIDOMetadataStatement]
B. Hill; D. Baghdasaryan; J. Kemp. *FIDO Metadata Statements v1.0*. Implementation Draft. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-metadata-statement-v1.2-rd-20171128.html

[FIDORegistry]
R. Lindemann; D. Baghdasaryan; B. Hill. *FIDO Registry of Predefined Values*. Implementation Draft. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-registry-v1.2-rd-20171128.html

[FIDORestrictedOperatingEnv]
Laurence Lundblade; Meagan Karlsson. *FIDO Authenticator Allowed Restricted Operating Environments List*. August 2017. Draft. URL: https:./fido-authenticator-allowed-restricted-operating-environments-list-v1.0-wd-20180629.html

[RFC2049]
N. Freed; N. Borenstein. *Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples (RFC 2049)*. November 1996. URL: http://www.ietf.org/rfc/rfc2049.txt

[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

[RFC5280]
D. Cooper; S. Santesson; S. Farrell; S.Boeyen; R. Housley; W. Polk. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. May 2008. URL: http://www.ietf.org/rfc/rfc5280.txt

[UAFProtocol]
R. Lindemann; D. Baghdasaryan; E. Tiffany; D. Balfanz; B. Hill; J. Hodges. *FIDO UAF Protocol Specification v1.0*. Proposed Standard. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-uaf-protocol-v1.2-rd-20171128.html

[UAFRegistry]
R. Lindemann; D. Baghdasaryan; B. Hill. *FIDO UAF Registry of Predefined Values*. Proposed Standard. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-uaf-reg-v1.2-rd-20171128.html