FIDO Authenticator Security Requirements

FIDO Alliance Final Requirements Document 02 November 2021

This version:
https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-security-requirements-v1.5-fd-20211102.html
Previous version:
https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-security-requirements-v1.4.1-fd-20210510.html
Editors:
Beatrice Peirani , Thales
Johan Verrept , OneSpan
Contributors:
Laurence Lundblade , NTT Docomo
Rolf Lindemann , Nok Nok Labs, Inc.
Dr. Joshua E. Hill , InfoGard Laboratories
Douglas Biggs , InfoGard Laboratories
Roland Atoui , The FIDO Alliance
Meagan Karlsson , The FIDO Alliance
Adam Powers , The FIDO Alliance
Carolina Lavatelli , Internet of Trust
Nitin Sarangdhar , Intel
Marcus Janke , Infineon

Abstract

This documents defines the security and privacy 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://fidoalliance.org.

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

Table of Contents

1. Introduction

1.1 Version

This document version (DV) is DV 1.5.0.

	L1	L1+	L2	L2+	L3	L3+
Security Requirements version (RV)	RV 1.4.0	RV 1.5.0	RV 1.4.0	-	RV 1.4.0	RV 1.4.0
Allowed Cryptography List version (CV) [FIDOAllowedCrypto]	CV 1.3.0	CV 1.3.0	CV 1.3.0	-	CV 1.3.0	CV 1.3.0
Allowed Restricted Operating Environments version (EV) [FIDORestrictedOperatingEnv]	-	-	EV 1.2.0	-	EV 1.2.0	EV 1.2.0
Authenticator Metadata Requirements version (MV) [FIDOMetadataRequirements]	MV 1.2.0	MV 1.3.0	MV 1.2.0	-	MV 1.2.0	MV 1.2.0
Vendor Questionnaire version (QV)	QV 1.4.0	QV 1.5.0	QV 1.4.0	-	QV 1.4.0	QV 1.4.0
Test Procedures version (PV)	PV 1.4.0	PV 1.5.0	PV 1.4.0	-	PV 1.4.0	PV 1.4.0

Table 1: Versions represented by this document

Associated documents to this document include FIDO Security Laboratory Accreditation Policy [FIDOLabPolicy] and FIDO Authenticator Certification Policy [FIDOAuthenticatorCertificationPolicy].

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 Definitions and Acronyms

1.3.1 Definitions

- ***Anti-emulation***: a technique to protect from code emulation, where a binary code is fed to a virtual/software processing unit rather than a physical processor. The virtual unit mimics what a physical one would do, though at a much slower speed.
  NOTE Emulation is a powerful approach as it lets attackers do cross-platform analysis: for example, an ARM emulator can run on an x86-64 platform. The virtual unit can be turned into an analysis tool, providing an in-depth view of the behavior of a binary and the possibility to analyze, react or interfere with it while it is being processed. By placing the virtual processor in a chosen context, it is even possible to emulate a part of the whole binary, letting an attacker focus on very specific aspects of its target. Anti-emulation typically relies on discrepancies between a physical processor and its emulator to detect whether a code is run on an actual device or not. For example: execution speed is much slower on an emulator an emulator could implement only a subset of the instructions available on a real processor a side-effect of the execution of an instruction could differ slightly between the two
- ***Anti-tracing***: a software protection technique to prevent dynamic information collection from a target application through a tool such as a debugger, an emulator or a dynamic binary instrumentation framework.
- ***Authenticator***: a set hardware and software that implements the Authenticator portion of the FIDO UAF, FIDO U2F, or FIDO2 protocols.
- ***Authenticator Application***: 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.
- ***Bucketing Computation Analysis (BCA)***: a chosen-plaintext attack on block-ciphers such as DES or AES. It detects a correct key guess by checking if two sets of intermediate values have an empty intersection, as an expected result of a choice of messages for a given key hypothesis. It is an attack that requires access to intermediate values during an execution, which is suitable in the whitebox context.
  NOTE See https://www.cosade.org/presentations/another_look.pdf
- ***Configuration item***: 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.
- ***Consumer Profile***: applicable by default, the Authenticator is intended to be used by consumers and sold on the open market. In a Consumer Profile, Enterprise

Attestation is not be supported.

- ***Dynamic Binary Instrumentation framework (DBI)***: a tool that lets you analyze into detail the behavior of a target program. Initially designed for performance or memory leak detection, this kind of feature also is of great interest for side-channel analysis (through data collection) or fault injection techniques (through dynamic data or control flow modification).
  NOTE Frida (https://www.frida.re/) and Triton (https://triton.quarkslab.com/) are DBIs that are security-oriented, while Pin (https://software.intel.com/en-us/articles/pin-a-dynamic-binary-instrumentation-tool), Valgrind (http://valgrind.org/docs/valgrind2007.pdf) or DynamoRio (https://www.dynamorio.org/) have plugins meant for security analysis.
- ***Enterprise***: some form of organization, often a business entity.
- ***Enterprise Attestation***: a per-authenticator unique attestation, which may be configured to support either of both:
  - **vendor-facilitated enterprise attestation (also called EA mode 1)**
    In this case, the Authenticator Vendor pre-configures into the Authenticator, upon request of the Enterprise, a (non-updateable) list of RP IDs, for those RPs allowed to request enterprise attestation.
  - **platform-managed enterprise attestation(also called EA mode 2)**
    In this case, the platform/browser, managed by the Enterprise, knows which RPs are allowed to request enterprise attestation, e.g. through a local policy lookup.
- ***Enterprise Profile***: it applies if the Authenticator is intended for employees of an enterprise and the authenticator is sold directly to the Enterprise. It allows the Enterprise Attestation option to be enabled on a FIDO Authenticator compliant with CTAP 2.1 ([FIDOCTAP]). Enterprise Attestation allows Enterprises to uniquely identify Authenticators upon registration with their corporate systems. In the Enterprise Profile, Enterprise Attestation MAY be supported.
- ***Factory reset***: a function allowing the user resetting the Authenticator to the original (factory) state, i.e. deleting all user specific information.
- ***Key protection type***: SW, HW, TEE, SE or remote, as described in [FIDORegistry]. Key protection means here where the key is stored and manipulated.
- ***Operating Environment: a set of hardware and software components (e.g. hardware processing unit, physical memory, etc.) that provides facilities (e.g. Computing, Memory Management, input/output, etc.), necessary to support running of applications.***
- ***Profile***: a context for certification, assigning an intended user environment for the authenticator. The current version of this document defines Consumer Profile and Enterprise Profile.
- ***Secure boot (or verified boot)***: a process that ensures that the device boots an unmodified, authorized image.
- ***Zero Difference Enumeration attack (ZDE)***: a chosen-plaintext attack on AES, which detects a correct key guess by minimizing the number of differences in the algorithm state for a given key hypothesis and carefully chosen messages. It is an attack that requires access to intermediate values during an execution, which is suitable in the whitebox context.
  NOTE See https://eprint.iacr.org/2017/183.pdf

1.3.2 Acronyms

- ***AES***: Advanced Encryption Standard (cryptographic algorithm)
- ***AROE***: Allowed ROE
- ***ASM***: Authenticator Specific Module
- ***ASP***: Authenticator Security Parameters
- ***CC***: Common Criteria
- ***CTAP***: Client To Authenticator Protocol
- ***DCA***: Differential Computation Analysis

- ***DFA***: Differential Fault Analysis
- ***ECC***: Elliptic Curve Cryptography
- ***ECDAA***: Elliptic Curve based Direct Anonymous Attestation (cryptographic algorithm)
- ***FAR***: False Acceptance Rate
- ***GDPR***: General Data Privacy Regulation (regulation on data protection and privacy in the European Union)
- ***HLOS***: High-Level Operating System
- ***HW***: Hardware
- ***KDF***: Key Derivation Function
- ***PIN***: Personal Identification Number
- ***PP***: Protection Profile
- ***ROE***: Restricted Operating Environment
- ***RP***: Relying Party
- ***RP ID***: Relying Party Identifier
- ***RNG***: Random Number Generator
- ***RSA***: Rivest Shamir Adleman (cryptographic algorithm)
- ***SAR***: Security Assurance Requirements (CC context)
- ***SE***: Secure Element
- ***SFR***: Security Functional Requirements (CC context)
- ***SoC***: System on Chip
- ***SW***: Software
- ***TEE***: Trusted Execution Environment
- ***TOE***: Target Of Evalutation
- ***TUI***: Trusted User Interface
- ***UV***: User Verification
- ***UVM***: User Verification Method
- ***WBC***: White Box Cryptography

1.4 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)
- **Profile**: The profile for which this Requirement is applicable. Each requirement is assigned one or more profiles. For example, Consumer, Enterprise , or

Consumer + Enterprise (meaning it is applicable to Consumer and Enterprise). A requirements is valid for that profile if it is tagged with that profile.

- ***Testing Style***: The testing style of the Security Requirement, explained in the Testing Style section below.
- **Requirement Level**: The Security Level to which the Requirement applies.

  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>.

- **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 Companion Program**: This describes how the Requirement can be met by a particular Companion Program. Whether a requirement can be met through a Companion Program or not varies by Requirement, Security Level and the Companion Program. Companion Programs are explained in the Companion 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]; [Profile];[Testing Style]; [Level] Requirement text. NOTE Note text. Relation to Companion Program **[Level] [Companion Program]**: Relation to Companion Program text.	

	Calibration Calibration text. **[Level] Vendor Questionnaire** Vendor Questionnaire text. **[Level] Test Procedure** {Test Assurance Mode } Test Procedure text.	[Security Measures]

Example Requirement

1.5 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.

1.6 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].

1.7 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.

1.7.1 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).

1.7.2 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 Companion 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. Security and Certification

This section is normative.

2.1 Security levels

2.1.1 Enhanced software based authenticator (L1+)

At L1+, the Authenticator Application executes in an operating environment it has no control, that can be compromised and which cannot be a priori trusted. The Authenticator Application cannot solely rely on hardware security features of the operating environment. All security features are provided by the Authenticator Application itself. The following figure gives a high level view of architecture for L1+.

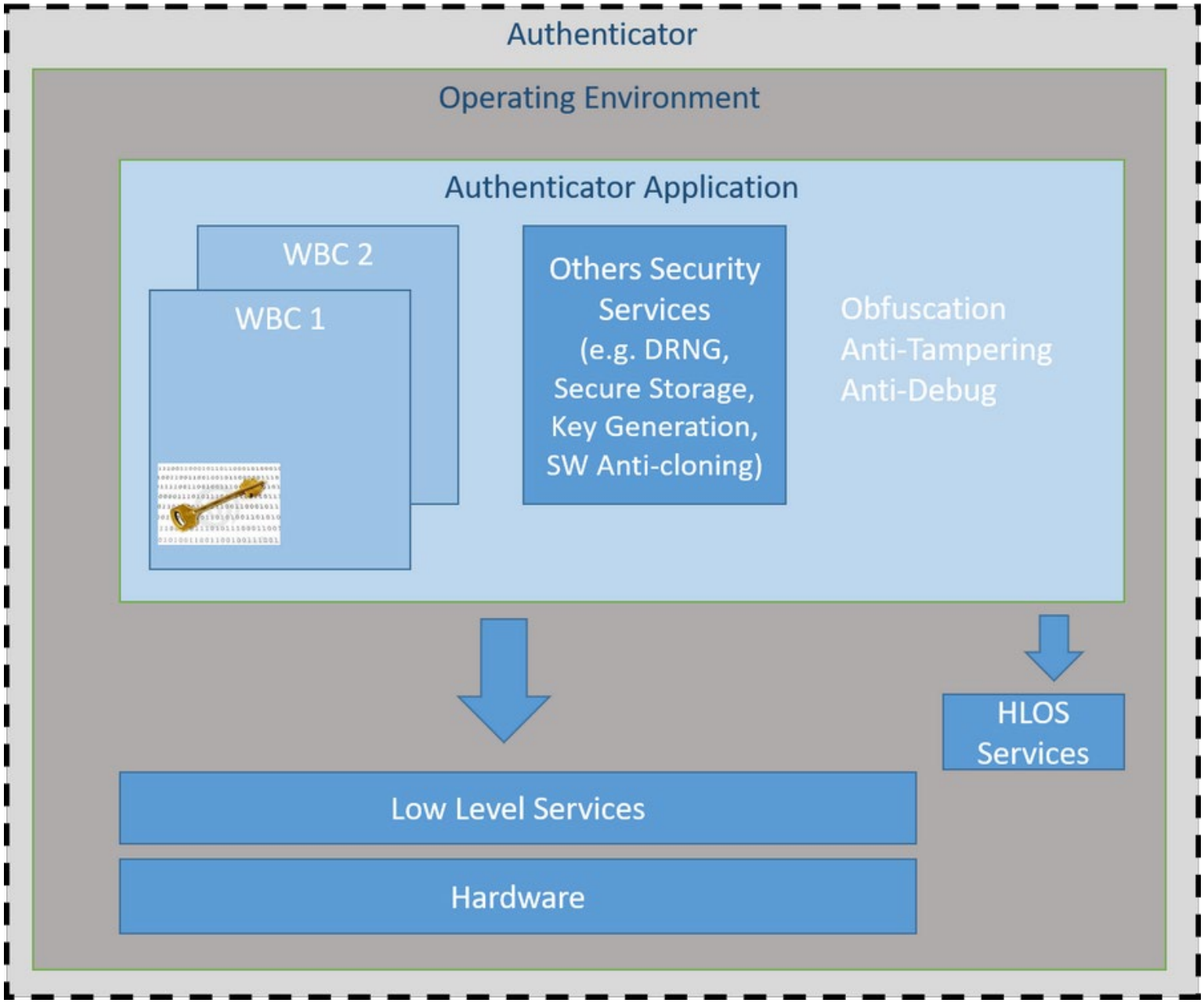

Fig. 1 Typical High Level Architecture of a Level 1+ Authenticator Application

There are several tools available for software protection. ETSI CYBER TR 103 642 [CYBER] provides a list of such tools, with description of attacks in a white box model. **In this model, software attacks (including side-channel and fault attacks) are the most straightforward means**. A detailed description of the tools, including white box crypto and code and data protection (obfuscation, anti-tampering, anti-debug, ...) can be found in [CYBER]. The use of these tools is not mandatory but it is unlikely that the Authenticator Application can achieve the targeted security level without their use.

The following terms are used in this document and their definition can be found in section 3.1 of [CYBER]:

- obfuscation
- anti-tampering
- anti-debug
- anti-reversing
- anti-cloning
- anti-xxx (see section 5.3.2 in [CYBER]) includes the four previous ones
- whitebox crypto (or WBC)
- differential computation analysis (or DCA)
- differential fault analysis (or DFA)
- device binding

2.1.2 Authenticator Hardware Examples

This section is non-normative.

These examples are solely illustrative and demonstrative. No information in this section may be used as justification for requirements met.

The relation between FIDO certification levels and the attacks defended against is roughly summarized in the following table.

FIDO Security Level	HW & SW Requirements	Defends against	Implementation examples
L1	Any device HW or SW	Unprivileged client applications and data cloning but only assuming execution environment is genuine.	L1 is the by-default security level required for any functional certification.
L1+	Authenticator Application only implementation with security focus (state-of-the-art software protection)	Temporary privileged escalation on HLOS (others applications and some root exploits)	As defined and certified by FIDO: • Use of whitebox crypto (WBC) for handling of secrets • Use of software protection techniques (e.g. anti-tampering) for protecting Authenticator usage

L2	Authenticator implementation supported by a Restricted Operating Environment (ROE). ROE is supporting segregation protection but is sharing computational resources with the HLOS (same CPU, same memory, same cache …). A list of Allowed ROE (AROE) is published in [FIDORestrictedOperatingEnv].	Permanent privilege escalation on HLOS including kernel level exploits (e.g. root exploit)	Within the list of Allowed ROE: Security Key (BLE/NFC/USB) TEE based on ARM Trustzone TEE Based on Intel VT HW …
L2+	ROE has access to fully isolated resources (segregation enforced by a hardware CPU mechanism or by usage of distinct computational resource)	Permanent privilege escalation on HLOS including hypervisor level exploits	TBD (no Companion Program is available for this level)
L3	Authenticator implementation supported by a ROE with security resistance against physical attacks	Attacker with physical access to the device HW but with non-invasive attacks (probing, emanations analysis, limited fault injections)	GlobalPlatform certified TEE (L3 GlobalPlatform Companion Program) CC certified Secure Element (L3 CC Companion Program)
L3+	Authenticator implementation supported by a ROE or standalone with security resistance against advanced physical attacks	Attacker with physical access to the device HW but with invasive attacks (tampering, advanced emanations analysis and fault injections)	CC certified Secure Element (L3+ CC Companion Program)

Table 2.1: Sample Device Hardware and Software Requirements Defence Profile

The following table contains examples of underlying platform on which an authenticator executes to illustrate the possible security levels to be targeted for a FIDO certification.

The typical FIDO certification levels given are again only illustrative. The actual certification level granted depends on many things other than what is listed in this table. The authenticator must meet all the FIDO security and privacy requirements for the given level.

Case#	Examples	(May target) FIDO security level	Companion Program
A	Mobile phone with HW key store	L1	NA
B	IoT device 100MHz 32-bit CPU accessing DIMM socket memory. Low speed memory	L2+	No Companion Program for L2+ is available at the moment.

	socket interface		
C	Laptop with high performance 2GHz CPU accessing DDR4 memory in a SO-DIMM. High speed memory socket interface	L2 by default. L2+ or L3 if there is an existing certification.	No Companion Program for L2+ is available at the moment. FIDO proposes 2 Companion Programs, based on Common Criteria, to target FIDO L3 security level.
D	Laptop with high performance 2GHz CPU accessing DDR4 memory in a SO-DIMM with buried trace	L2 by default. L2+ or L3 if there is an existing certification.	No Companion Program for L2+ is available at the moment. FIDO proposes 2 Companion Programs, based on Common Criteria, to target FIDO L3 security level.
E	Mobile phone SoC with 2GHz CPU with PoP memory	L2 by default. L2+ or L3 if there is an existing certification.	No Companion Program for L2+ is available at the moment. FIDO proposes 2 Companion Programs, based on Common Criteria, to target FIDO L3 security level.
F	Mobile phone SoC with 2GHz CPU with memory and CPU die in the same package	L2 by default. L2+ or L3 if there is an existing certification.	No Companion Program for L2+ is available at the moment. FIDO proposes 2 Companion Programs, based on Common Criteria, to target FIDO L3 security level.
G	IoT device 32-bit 100MHz CPU with memory and CPU on the same die	L2 by default. L2+ if there is an existing certification.	No Companion Program for L2+ is available at the moment.
H	SoC built on a CC-certified TEE	L3	FIDO proposes a dedicated Companion Program based on GlobalPlatform, with security level L3.
I	SoC with CPU with strong inline memory encryption and integrity protection HW	L2 by default. L3/L3+ if there is an existing certification for	Eurosmart is developing a new PP for a Secure Sub-System (3S) in SoC, compliant with AVA_VAN.5 (high attack potential), based on Common Criteria. It could target L3+ with the development of a new companion program.

		the SoC .	
J	Smart Card or Secure Element. Memory and CPU on the same die with hardware countermeasures	L2 by default. L3/L3+ if there is an existing certification for the SE.	FIDO proposes 2 dedicated Companion Programs for SE devices, targeting L3 or L3+, based on CC.

Table 2.2: Examples of underlying platforms used by FIDO Authenticators

2.2 Certification and Companion Programs

The FIDO Alliance is the issuer of FIDO certifications. All vendors receiving certification must go through a process with the FIDO Alliance including paying a fee to the FIDO Alliance . At all levels the authenticator vendor must fill out a detailed vendor questionnaire and provide supporting documents. At L1, certification is through design document review by the FIDO Alliance Security Certification Secretariat. No lab is involved. For all except L1, the authenticator vendor must engage a FIDO-accredited lab. At L2, the security lab performs only a comprehensive design document review. At L1+, L2+, L3 and L3+ the lab performs a deeper evaluation including penetration testing and sometimes source code review.

To qualify for Certification, an Authenticator needs to fulfill all Security and Privacy Requirements (this document), depending on the targeted security level, and more generally be compliant with the set of documents listed in Table 1.

Companion Programs make use of Certification Programs independent from FIDO with which FIDO relies on to offer joint FIDO Certification Programs to reduce the certification burden on Vendors. In this version, Companion Programs are relevant to certification levels 3 and 3+. All vendors targetting L3 or L3+ certification MUST provide responses to cover the FIDO Authenticator Security Requirements using a mapping table including supported Companion Programs. This mapping SHOULD be based on [FIDO-SR-Mapping-Table] provided by FIDO.

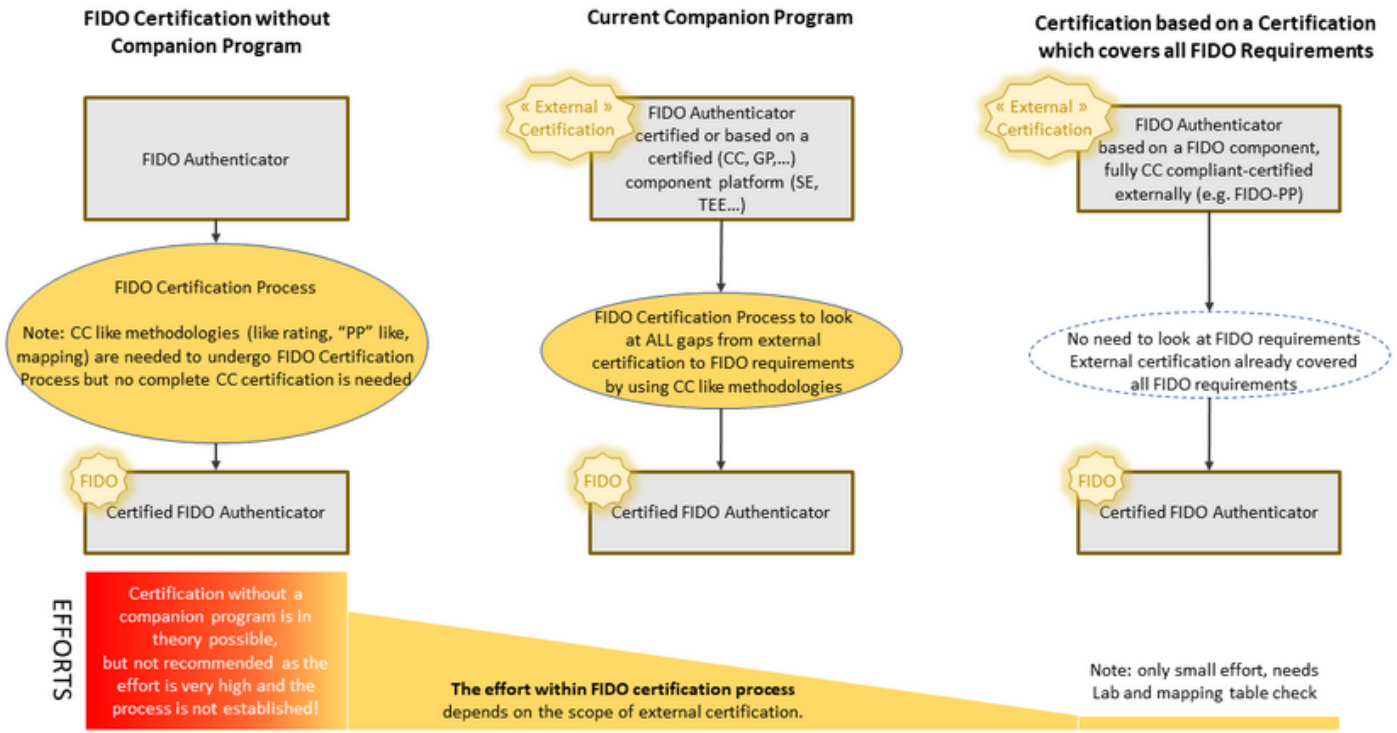

Fig. 2 Scenarios for FIDO L3/L3+ certification and their efforts

There is no Companion Program for certification level 1+. FIDO has developed a methodology for evaluation of a software authenticator protected using software techniques such as white box cryptography. This method is based on a combination of other related industry methods such as [CEMV3-1R5]], [AttackPotentialSmartcards] and Annex A of [TEE-PP] but adapted to software specificities [L1plus-Eval].

In the Companion Program boxes, the term ***linked to*** indicates that the FIDO Security Requirement is related to the Companion Program Requirement but is not completely fulfilled by it. The term ***fulfilled by*** means that if the Companion Program Requirement is fulfilled, this automatically fulfills the FIDO Security Requirement.

NOTE

This table is provided only as a guidance document for both vendors and labs to simplify evidence writing and evaluation tasks. This mapping table does not add or replace any FIDO Authenticator 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 maps these to either the Java Card Open Configuration Protection Profile (PP) [JCPP], Security IC Platform PP [PP0084], FIDO U2F Authenticator PP [U2FPP] or GP TEE PP [TEE-PP]

NOTE

This version of the FIDO Security Requirements accepts Common Critera (for L3 and L3+) and the GlobalPlatform TEE Protection Profile (for L3). Future FIDO Companion Programs may cover certifications endorsed by the security industry such as FIPS 140-2, EMVCo, DSC PP and more.

2.2.1 Specific calibration for L1+

Starting from Common Criteria and its Common Methodology for Information Technology Security Evaluation [ISOIEC-18045], which is the default applicable method to all Common Criteria certified products or systems, and inspiring from existing recognized exceptions to it, specific to a particular domain (e.g. JIL Smart Card [AttackPotentialSmartcards] or GlobalPlatform Trusted Execution Environment [TEE-EM]), the method has been adapted to software products specificities, where not all software instances are identical, where software attacks are multi-steps and where the environment has some influence. The calibration for L1+ thus deviates from the calibration of the other (higher) levels and is based on this new method, described in [L1plus-Eval].

The security requirement is evaluated by penetration testing, conducted by an Accredited Security Laboratory (mixing reverse engineering, side-channel and crypto skills), in a restricted time period (i.e. carried out in 40 man days, within a calendar period of 10 weeks).

The threat model is the white-box model. The analysis will determine the effectiveness of the FIDO security requirements proposed by the product.

The vendor will provide to the Lab for testing:

1. the binary code (for a given platform, iOS or Android) of the Authenticator Application,
2. or a demo application (in case of a SDK certification) with an integration guide describing the security requirements to be fulfilled when integrating the SDK to the final application

The evaluation will try at least (but not limited) to reverse engineer and/or modify the Authenticator Application code (including defeating anti-tampering mechanisms), to exploit interfaces between components and system and external calls (e.g. to spy exchanged data and/or to inject fake data), to extract assets at rest or in runtime and/or modify the Authenticator Application code flow (analyze and bypass anti-tamper protection), including:

- For white box crypto
  - Statistical analysis (including DCA if applicable)
  - Fault analysis (including DFA if applicable)
- For code and data protection
  - Identification of control flows and data flows
  - Obfuscation measures analysis
  - De-obfuscation of protected code
  - Circumvent anti-debug protection
  - Circumvent anti-emulation, anti-rooting, anti-hooking and anti-DBI protections
- Internal communication channel monitoring and manipulation

2.3 Documents for Certification

Depending on which level you wish to certify at, you will need to submit one or more of the following documents. These can be submitted as a single document or as separate documents.

- ***FIDO Biometric Evaluation Report***: This report is delivered by the FIDO accredited lab for the biometric certification program after evaluating the biometric sensor against FIDO biometric requirements.
- ***Configuration Management Scope and Capabilities***: All documentation covering the configuration items, their system records, plan and usage. This evidence is intended to prove that there is discipline and control in the processes of refinement and modification of the TOE and the related information. These are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking any changes, and by ensuring that all changes are authorized.
- ***Development Information***: A set of documents describing the TOE such as its design, security architecture, implementation of the security requirements, source code, etc. These are used as the basis for conducting vulnerability analysis and testing by the lab.
- ***Development Security Life-Cycle Support***: Documentation describing the life-cycle phases of the TOE, the developer's physical, procedural, personnel, and other security measures; tools and implementation standards used; measures handling of security flaws and the procedures used for the delivery of the TOE to the consumer.
- ***Operational User Guidance***: Documentation that is intended to be used by all types of users of the TOE in its evaluated configuration: end-users, persons responsible for maintaining and administering the TOE in a correct manner for maximum security, and by others (e.g. programmers) using the TOE's external interfaces. Operational User Guidance describes the security functionality, provides instructions and guidelines (including warnings), includes the security-critical information, and the security-critical actions required, for its secure use.
- ***Preparative Procedures Guidance***: Documentation useful for ensuring that the TOE has been received and installed in a secure manner as intended by the developer. The requirements for preparation call for a secure transition from the delivered TOE to its initial operational environment. This includes investigating whether the TOE can be configured or installed in a manner that is insecure but that the user of the TOE would reasonably believe to be secure.
- ***Security Target***: A document including implementation-dependent statements of security needs for a specific identified TOE. The TOE in the context of the FIDO authentication certification program corresponds to the Authenticator security boundary.
- ***Test Documentation***: A set of documents describing the security and functional tests procedures and how these cover the security functionality. The goal is to provide evidence that all security functionalities operate according to the design descriptions. Note that this does not address penetration testing which is based upon an analysis that specifically seeks to identify vulnerabilities in the design and implementation.

3. Requirements

This section is normative.

3.1 Authenticator definition Derived Requirements

For the purpose of these requirements, the Authenticator is the set of hardware and software within the Authenticator boundary, as defined in the response to requirement 1.1.

The underlying operating environment of the Authenticator Application 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).

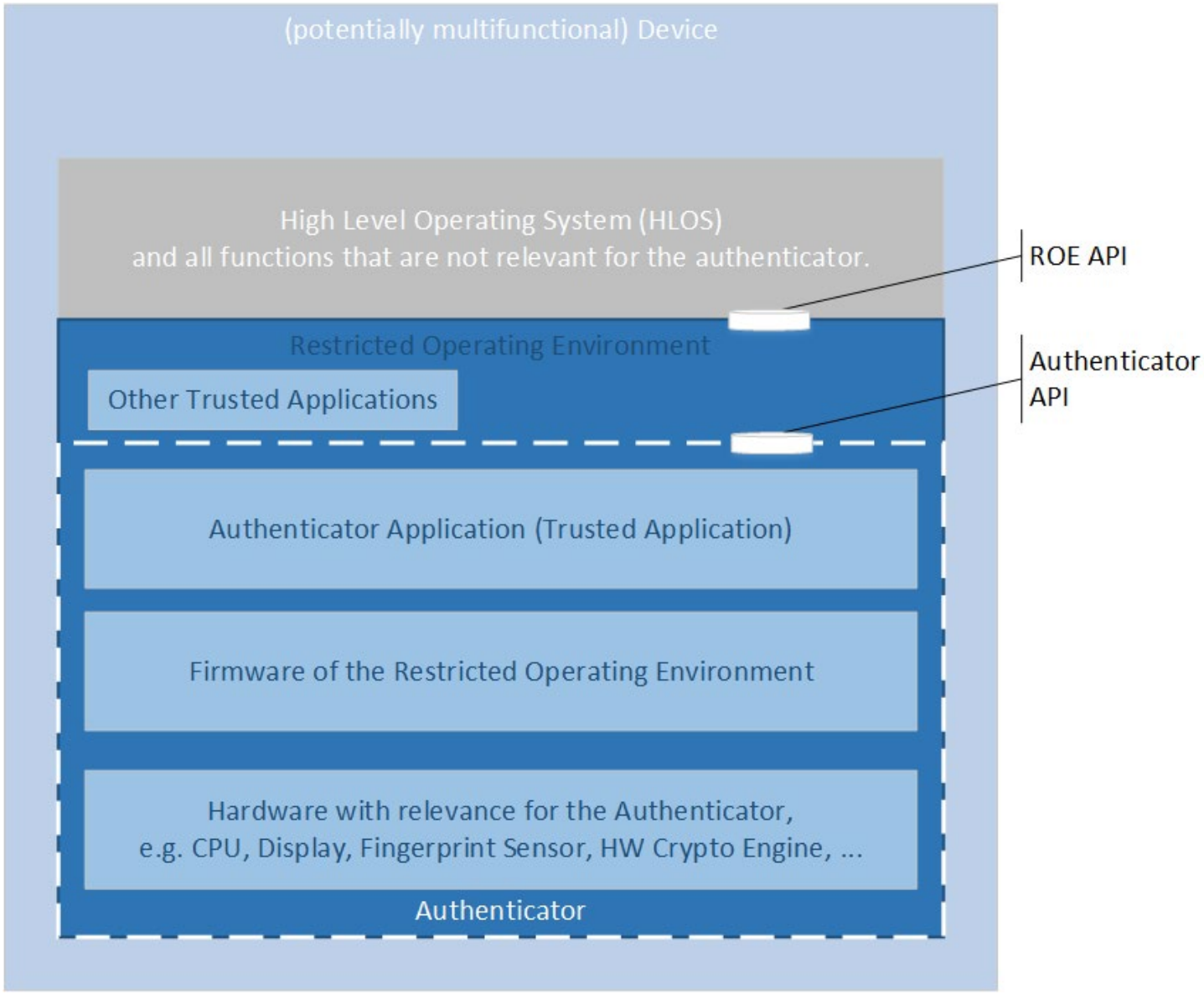

Fig. 3 Restricted Operating Environments Architectural Overview

At L1 and 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 is 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, 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). 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; Consumer + Enterprise; 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 [UAFProtocol] 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. Authenticators meeting #2, might qualify for L1+ Authenticator Certification. Authenticators meeting the following category might qualify for L1+ Authenticator Certification: Authenticator Application running on some HLOS *with* an effective protection of the Authenticator Security Parameters against most other applications running in the same environment - with breaking the HLOS.	

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:
- 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.

Relation to Companion Program

L3 GlobalPlatform: The AROE Security Target MUST be provided to support this requirement (see [TEE-PP] and [TEE-EM]).

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

This requirement is linked to ASE_INT and ASE_SPD (see [CC3V3-1R5]).

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

This requirement is linked to ASE_INT and ASE_SPD (see [CC3V3-1R5]).

1.1

Calibration

No calibration required.

(SM-1, SM-9, SM-26)

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 .

L1+ Vendor Questionnaire

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

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence 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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance and Preparative Procedures Guidance MUST be provided (see [TEE-EM]).

This requirement is linked to the FCS_COP.1, FCS_RNG.1 and FCS_CKM.1 components (see [TEE-PP]).

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

This requirement is linked to Class FCS and ADV (see [CC2V3-1R5] and [CC3V3-1R5]).

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

This requirement is linked to 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).

1.2

(SM-1, SM-9, SM-16, SM-26)

L1+ Vendor Questionnaire

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

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence 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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Development Information , Operational User Guidance and Preparative Procedures Guidance MUST be provided to support this requirement (see [TEE-EM]).

L3 Common Criteria: Development Information MUST be provided

This requirement is linked to Class ADV (see [CC3V3-1R5]).

L3+ Common Criteria: Development Information MUST be provided

This requirement is linked to 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.

L1+ Vendor Questionnaire

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

1.3

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

L3 Test Procedure

(SM-1, SM-6, SM-26)

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: The AROE Security Target MUST be provided to support this requirement (see [TEE-PP] and [TEE-EM]).

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

This requirement is linked to ASE_INT (see [CC3V3-1R5]).

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

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

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

1.4	• Development Information (Architecture and Interfaces) • Mapping to Companion Program Requirements • Source Code (optionally) **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Development Information (High Level Design) • Mapping to Companion 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: • Development Information (Low Level Design) • Mapping to Companion Program Requirements • Source Code **L1 Test Procedure** {A0} The Security Secretariat SHALL *verify* the requirement during Interoperability Testing. **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 GlobalPlatform Test Procedure** The tester SHALL *verify* that the provided rationale and evidence 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.	(SM-26)
	UAF + FIDO2; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: Not applicable to AROE.

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

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

If Yes, *Provide* the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

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:

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_COP.1 component (see [TEE-PP]).

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

1.6

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

(SM-16)

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target, Development Information, Operational User Guidance, Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FDP_IFC.1, FDP_IFF.1 and FCS_COP.1 components (see [TEE-PP]).

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

This requirement is linked to 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, Development Information and Test Documentation MUST be provided (see [CC1V3-1R5]).

This requirement is linked to FDP_IFC.1, FDP_IFF.1, 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

1.7 (SM-16)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FDP_IFC.1 and FDP_IFF.1 components (see [TEE-PP]).

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

1.8

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: (Applies if the Authenticator supports Transaction Confirmation and the Transaction Confirmation Display is implemented by the AROE) AROE Security Target, Development Information, Operational User Guidance, Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-PP] and [TEE-EM]).

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

This requirement is linked to FDP_IFC.1, FDP.IFF.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

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

If **Yes**, *provide* the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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.

1.9	**L3 GlobalPlatform Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting evidence: • Development Information (Architecture and Interfaces) • Test Documentation • Mapping to Companion Program Requirements • Source Code (optionally) **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Development Information (High Level Design) • Test Documentation • Mapping to Companion 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: • Development Information (Low Level Design) • Test Documentation • Mapping to Companion Program Requirements • Source Code **L1 Test Procedure** {A0} The Security Secretariat SHALL *verify* the requirement during Interoperability Testing. **L1+ Test Procedure** {A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure** The tester SHALL *verify* that the provided rationale and evidence meet the requirement. The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the test results.	(SM-10)

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FAU_ARP.1, FDP_IFC.1, FDP_IFF.1 and FMT_MSA.3 components (see [TEE-PP]).

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

This requirement is linked to 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 Information and Test Documentation MUST be provided (see [CC1V3-1R5]).

This requirement is linked to 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.

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. This characteristic will be verified as specified in section Specific Calibration for Level 1+.

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 GlobalPlatform: At L3 GlobalPlatform, this requirement SHALL be met for all inputs to the Authenticator. At L3 GlobalPlatform, the protection mechanisms SHALL resist attackers with Enhanced-basic attack potential (see [TEE-PP]). The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]).

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 [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]).

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.

L1 Vendor Questionnaire

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

L1+ Vendor Questionnaire

1.10

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

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design). (SM-28)

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The Tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: (Applies if the Authenticator supports Transaction Confirmation and the Transaction Confirmation Display is implemented by the AROE) AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-PP] and [TEE-EM]).

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

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

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

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

Calibration

No calibration required.

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements

1.11

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion Program Requirements

(SM-10)

L3+ Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion Program Requirements

L3 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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 Key Management and Authenticator Security Parameters

3.2.1 Documentation

No.	Requirement	Security Measures
	UAF + U2F + FIDO2; Consumer + Enterprise; 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, privacy sensitive data, 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. NOTE Note that the User Verification Token defined by UAF is different from the `pinToken` and `pinUvAuthToken` defined by CTAP [FIDOCTAP]. It is entirely internal to the authenticator whereas the others are passed in and out of the authenticator via CTAP. NOTE Note that the keys generated when using FIDO2 ClientPIN subcommands are considered ASPs. **Relation to Companion Program**	

L3 GlobalPlatform: The AROE Security Target MUST be provided to support this requirement (see [TEE-PP] and [TEE-EM]).

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

This requirement is linked to ASE_SPD (see[CC3V3-1R5]).

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

This requirement is linked to ASE_SPD (see[CC3V3-1R5]).

Calibration

L1+: At L1+, the code of the Authenticator Application is considered an ASP.

L1 Vendor Questionnaire

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

L1+ Vendor Questionnaire

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

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Mapping to Companion Program Requirements
- Source code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Mapping to Companion Program Requirements

L3+ Vendor Questionnaire

2.1.1

(SM-1, SM-2, SM-6, SM-13, SM-15, SM-16, SM-26)

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

- Development Information (Low Level Design)
- Mapping to Companion Program Requirements

L1 Test Procedure

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

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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence 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; Consumer + Enterprise; 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.

> NOTE
>
> Please note that the keys stored for the FIDO2 large-blob support and for credBlob extension are Authentiator Security Parameters but not Secret Authenticator Security Parameters as they are passed outside the Authenticator Boundary.

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target, Development Information, Operational User Guidance and Preparative Procedures Guidance MUST be provided to support this requirement (see [TEE-PP] and [TEE-EM]).

Remark: Protection of biometric data should be provided through the AROE biometric system.

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

This requirement is linked to FDP_IFF.1 and Class ADV (see [CC2V3-1R5] and [CC3V3-1R5]).

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

This requirement is linked to 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 environment for those Authenticator Security Parameters which are not fully maintained in the Authenticator Application .

2.1.2

L1+ Vendor Questionnaire

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

L2 Vendor Questionnaire

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

(SM-1, SM-2, SM-6, SM-13, SM-15, SM-16, SM-26)

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Mapping to Companion Program Requirements
- Source code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Mapping to Companion Program Requirements

L3+ Vendor Questionnaire

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

- Development Information (Low Level Design)
- Mapping to Companion Program Requirements

L1 Test Procedure

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

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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence 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; Consumer + Enterprise; 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 security strength. This claimed security strength SHALL NOT be larger than the maximal allowed claimed security 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 security strength for this key SHALL be zero.

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

Relation to Companion Program

L3 GlobalPlatform: Security Target , Development Information , Operational User Guidance and Preparative Procedures Guidance MUST

be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_CKM.1 component (see [TEE-PP]).

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

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

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

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

Calibration

L1+: At L1+, the key may be used with an algorithm listed on the "Allowed Cryptography List" [FIDOAllowedCrypto] but with a different configuration (e.g. AES with different configuration taken from Rijndael specification [AES-Proposal]) than the standard one. In this case, the claimed security strength is equivalent to the one with a standard configuration.

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 security strength, the security strength of that key is unknown.

2.1.3

L1+ Vendor Questionnaire

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

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Mapping to Companion Program Requirements
- Source code (optionally)

(SM-1, SM-2, SM-6, SM-13, SM-16, SM-26)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Mapping to Companion Program Requirements

L3+ Vendor Questionnaire

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

- Development Information (Low Level Design)
- Mapping to Companion Program Requirements

L1 Test Procedure

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

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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence 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; Consumer + Enterprise; DaD; L1 and higher

The vendor SHALL document the Authenticator's ***Overall Claimed Security Strength***; the Overall Authenticator Claimed Security Strength SHALL be less than or equal to the claimed security strength of all the Authenticator Security Parameters that are cryptographic keys.

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target, Development Information, Operational User Guidance, Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_COP.1 components (see [TEE-PP]).

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

This requirement is linked to ASE_SPD, FCS_COP.1 and AGD_OPE.1 (see [CC2V3-1R5] and [CC3V3-1R5]).

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

This requirement is linked to ASE_SPD, FCS_COP.1 and AGD_OPE.1 (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

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

L1+: At L1+, the Authenticator's Overall Claimed Security Strength SHALL at least be greater than or equal to 100 bits and it SHOULD be greater than or equal to 112 bits.

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

L3 GlobalPlatform: At L3 GlobalPlatform, the Authenticator's Overall Claimed Security 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 Security 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 Security 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.

2.1.4 (SM-1, SM-16, SM-26)

L1+ Vendor Questionnaire

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

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Operational User Guidance
- Mapping to Companion Program Requirements

L3+ Vendor Questionnaire

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

- Development Information (Low Level Design)
- Operational User Guidance
- Mapping to Companion Program Requirements

L1 Test Procedure

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

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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence 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; Consumer + Enterprise; GaVR-3; L1 and higher

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

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target, Development Information, Operational User Guidance, Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FDP_ACC.1, FDP_ACF.1, FDP_IFC.2, FDP_IFF.1, FDP_ITT.1, FDP_ROL.1, FDP_SDI.2, FMT_MSA.3, FMT_MTD.1, FPT_FLS.1, FPT_INI.1, FPT_ITT.1 and FPT_TEE.1 components (see [TEE-PP]).

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

This requirement is linked to 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 Information and Test Documentation MUST be provided (see [CC1V3-1R5]).

This requirement is linked to 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.

L1+: At L1+, the Authenticator Application SHOULD minimize its dependency to the underlying operating environment and it SHALL implement software protection techniques to protect against modification and substitution (e.g. device binding and anti-tampering). This characteristic will be verified as specified in section Specific Calibration for Level 1+.

The code of the Authenticator Application is considered a Security Parameter and hence need to be protected against modification.

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

L3 GlobalPlatform: At L3 GlobalPlatform, the protection mechanisms SHALL resist attackers with Enhanced-basic attack potential (see [TEE-PP]). The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]).

2.1.5	**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. **L1+ Vendor Questionnaire** *Provide* the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design). **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 GlobalPlatform Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting evidence: • Development Information (Architecture and Interfaces) • Test Documentation • Mapping to Companion Program Requirements • Source Code (optionally) **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Development Information (High Level Design) • Test Documentation • Mapping to Companion Program Requirements • Source Code	(SM-1, SM-6, SM-13, SM-15, SM-16)

L3+ Vendor Questionnaire

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

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The Tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; GaVR-3; L1 and higher

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

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target, Development Information, Operational User Guidance, Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FDP_ACC.1, FDP_ACF.1, FDP_IFC.2, FDP_IFF.1, FDP_ITT.1, FDP_ROL.1, FMT_MSA.1, FMT_MSA.3, FPT_ITT.1 and FPT_INI.1 components (see [TEE-PP]).

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

This requirement is linked to 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 Information and Test Documentation MUST be provided (see [CC1V3-1R5]).

This requirement is linked to 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 disclosed to (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 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]).

L1+: At L1+, the Authenticator Application SHOULD minimize its dependency on the underlying operating environment and it SHALL implement software protection techniques to protect against reverse engineering (e.g. with encryption, obfuscation and whitebox cryptography for secret keys), against software induced side-channel and fault attacks, and against WBC code/data lifting (e.g. with anti-emulation, device binding). This characteristic will be verified as specified in section Specific Calibration for Level 1+.

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

L3 GlobalPlatform: At L3 GlobalPlatform, the protection mechanisms SHALL resist attackers with Enhanced-basic attack potential (see [TEE-PP]). The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]).

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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation

- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The Tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target, Development Information, Operational User Guidance, Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_COP.1, FDP_ACC.1, FDP_ACF.1 and FDP_SDI.2 components (see [TEE-PP]).

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

2.1.7	**L2 Vendor Questionnaire** ***Describe*** how this requirement can be verified through documentation review. Please provide explicit design document references. **L3 GlobalPlatform Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting evidence: • Development Information (Architecture and Interfaces) • Test Documentation • Mapping to Companion Program Requirements • Source Code (optionally) **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Development Information (High Level Design) • Test Documentation • Mapping to Companion 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: • Development Information (Low Level Design) • Test Documentation • Mapping to Companion Program Requirements • Source Code **L1 Test Procedure** {A1} The Security Secretariat SHALL ***review*** the provided rationale to verify the requirement is met. **L1+ Test Procedure** {A2} The tester SHALL ***verify*** that the documentation meets 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 GlobalPlatform Test Procedure**	(SM-1, SM-6, SM-13, SM-15, SM-16, SM-25)

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_COP.1, FDP_ACC.1 and FDP_ACF.1 components (see [TEE-PP]).

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

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

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

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

Calibration

No calibration required.

2.1.8

L1 Vendor Questionnaire

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

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

(SM-1, SM-6, SM-13, SM-15, SM-16, SM-25)

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 security strength greater than or equal to the claimed security strength of the key being wrapped.

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_COP.1 components (see [TEE-PP]).

L3 Common Criteria: Security Target , Development Information , Test Documentation and Preparative Procedures Guidance MUST be provided (see [CC1V3-1R5]).

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

L3+ Common Criteria: Security Target , Development Information , Test Documentation and Preparative Procedures Guidance MUST be provided (see [CC1V3-1R5]).

This requirement is linked to FCS_COP.1, AGD_PRE.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, externally-stored means stored outside the Authenticator boundary . In the case of L1 this Authenticator boundary includes the underlying operating environment.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source code (optionally)

2.1.9 (SM-1, SM-6, SM-16, SM-25)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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.

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 Companion Program

L3 GlobalPlatform: AROE Security Target, Development Information, Operational User Guidance, Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_CKM.1, FCS_COP.1 and FCS_RNG.1 components (see [TEE-PP]).

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

This requirement is linked to FCS_COP.1, FMT_MTD.3, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

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

This requirement is linked to 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.

L1+: At L1+, this Authenticator boundary includes the underlying operating environment.

L2: No calibration required.

L3 GlobalPlatform: 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

2.1.10

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

(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:

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_COP.1, FDP_IFF, FDP_IFC and FIA_USB.1 components (see [TEE-PP]).

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

This requirement is linked to 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 Information and Test Documentation MUST be provided (see [CC1V3-1R5]).

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

2.1.11 (SM-13)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FDP_IFC.1, FDP_IFF.1 and FCS_COP.1 components (see [TEE-PP]).

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

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

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

This requirement is linked to FCS_COP.1, 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlaform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

2.1.12

(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:

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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) will only be used for authenticating one user account to one particular Relying Party.

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_CKM.1, FCS_COP.1 and FCS_RNG.1 components (see [TEE-PP]).

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

This requirement is linked to 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 Information and Test Documentation MUST be provided (see [CC1V3-1R5]).

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

2.1.13	**L3 GlobalPlatform Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting evidence: • Development Information (Architecture and Interfaces) • Test Documentation • Mapping to Companion Program Requirements • Source Code (optionally) **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Development Information (High Level Design) • Test Documentation • Mapping to Companion 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: • Development Information (Low Level Design) • Test Documentation • Mapping to Companion Program Requirements • Source Code **L1 Test Procedure** {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. **L1+ Test Procedure** {A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale. **L3 GlobalPlatform Test Procedure** The tester SHALL *verify* that the provided rationale and evidence meet the requirement.	(SM-1, SM-2, SM-27)

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; TVFR; L1+ 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_COP.1 components (see [TEE-PP]).

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

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

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

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

Calibration

No calibration required.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

2.1.14

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_COP.1 components (see [TEE-PP]).

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

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

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

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

Calibration

No calibration required.

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

2.1.15

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L3 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; TVFR; L1 and higher

In the event that an Authenticator Security Parameter is “destroyed” it 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_CKM.4 and FDP_RIP.1 components (see [TEE-PP]).

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

This requirement is linked to FCS_CKM.4, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

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

This requirement is linked to 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.

L1+: At L1+, the Authenticator Application SHALL follow best security practices to protect the Authenticator Security Parameters against being recovered and used (e.g. by erasing with zeroes or randoms).

This characteristic will be verified as specified in section Specific Calibration for Level 1+ .

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

L3 GlobalPlatform: At L3 GlobalPlatform, the means for making the Authenticator Security Parameter permanently unavailable SHALL resist attackers with Enhanced-basic attack potential (see [TEE-PP]). The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]).

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.

2.1.16

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

(SM-1, SM-24)

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation

- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; TVFR; L2 and higher

Authenticators might support ***factory reset***.

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 Companion Program

L3 GlobalPlatform: AROE Security Target, Development Information, Operational User Guidance, Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_CKM.4, FCS_RNG.1, FDP_IFF.1, FDP_RIP.1 and FMT_MSA.1 components (see [TEE-PP]).

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

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

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

This requirement is linked to 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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

2.1.17

L3 Vendor Questionnaire

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

- Development Information (High Level Design)

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

- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_CKM.1 and FCS_RNG.1 components (see [TEE-PP]).

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

2.1.18 **L3 Vendor Questionnaire** (SM-1, SM-16,

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

SM-21)

L3+ Vendor Questionnaire

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

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_CKM.1 and FCS_COP.1 components (see [TEE-PP]).

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

2.1.19	**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 GlobalPlatform Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting evidence: • Development Information (Architecture and Interfaces) • Test Documentation • Mapping to Companion Program Requirements • Source Code (optionally) **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Development Information (High Level Design) • Test Documentation • Mapping to Companion 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: • Development Information (Low Level Design) • Test Documentation • Mapping to Companion Program Requirements • Source Code **L1 Test Procedure** {A1} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met. **L1+ Test Procedure** {A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.	(SM-27)

L3 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_CKM.1 and FCS_COP.1 components (see [TEE-PP]).

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

2.1.20 (SM-1, SM-6, SM-26)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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.

3.2.2 Random Number Generation

No.	Requirement	Security Measures
	UAF + U2F + FIDO2; Consumer + Enterprise; 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. An Allowed Random Number Generator or Allowed Key Derivation Function SHALL be used to generate the `pinToken` or `pinUvAuthToken` in FIDO2 if used by the authenticator. **Relation to Companion Program**	

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_CKM.1, FCS_COP.1 and FCS_RNG.1 components (see [TEE-PP]).

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

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

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

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

Calibration

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.

L1+: At L1+, if a Key Derivation Function is used and if it is not listed on the “Allowed Cryptography List” [FIDOAllowedCrypto], the security strength SHALL at least be greater than or equal to 100 bits and it SHOULD be greater than or equal to 112 bits. This characteristic will be verified as specified in section Specific Calibration for Level 1+ .

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

L3 GlobalPlatform: 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

2.2.1 (SM-16)

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 security 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 security level of they key generated or used.

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_RNG.1 component (see [TEE-PP]).

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

2.2.2 (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:

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_RNG.1 components (see [TEE-PP]).

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

2.2.3

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

(SM-16)

L3+ Vendor Questionnaire

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

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_RNG.1 component (see [TEE-PP]).

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

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

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

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

Calibration

No calibration required.

2.2.4 **L3 GlobalPlatform Vendor Questionnaire** (SM-8, SM-22)

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L3 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_RNG.1 component (see [TEE-PP]).

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

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

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

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

Calibration

No calibration required.

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

2.2.5 (SM-16)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L3 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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.

3.2.3 Signature Counters

Authenticators can set the signature counter value in the assertions to "0" to indicate that signature counters are not supported.

An Authenticator that sets the signature counter to any value other than "0" "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
	UAF + U2F + FIDO2; Consumer + Enterprise; DaD; L1 and higher	
	Support of Signature counters is OPTIONAL. The vendor SHALL document whether the Authenticator supports Signature Counters and if they are supported, the vendor SHALL document which of the following the authenticator implements: • one Signature Counter *per authentication key* • one (global) Signature Counter for all authentication keys (i.e. at least one counter covering multiple keys) If the Authenticator does not use a Signature counter per authentication key, the Vendor SHALL document if additional measures are implemented, for example, if the Authenticator uses a single Signature Counter and an offset per authentication key. NOTE The Vendor will provide a rationale for implementing any another mechanism satisfying this requirement. **Relation to Companion Program** **L3 GlobalPlatform**: Not applicable to the AROE. **L3 Common Criteria**: A Security Target document MUST be provided (see [CC1V3-1R5]). This requirement is linked to ASE_INT and ASE_SPD (see [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target document MUST be provided (see [CC1V3-1R5]). This requirement is linked to ASE_INT and ASE_SPD (see [CC3V3-1R5]). **Calibration** **L1**: At L1, Authenticators not running in an Allowed Restricted Operating Environment (AROE) [FIDORestrictedOperatingEnv], SHALL	

support signature counter(s).

L1+: At L1+, Authenticators (not running in an Allowed Restricted Operating Environment, AROE) [FIDORestrictedOperatingEnv], SHALL support signature counter(s).

L2: No calibration required.

L3 GlobalPlatform: No calibration required.

L3: No calibration required.

L3+: No calibration required.

2.3.1 (SM-15)

L1 Vendor Questionnaire

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

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence 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; Consumer + Enterprise; 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) strictly 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.

The signature counter can nevertheless be set to "0" when it goes into a permanent error state (counter error).

NOTE

Once a signature counter value *contained in a FIDO signature assertion* for one specific authentication key has been set to "0" it will 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 Companion Program

L3 GlobalPlatform: Not applicable to the AROE.

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

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

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

This requirement is linked to FDP_IFF, FDP_IFC, 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.

L1+ Vendor Questionnaire

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

If Yes, *provide* the tester with documentation that specifies 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.

2.3.2

(SM-15)

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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 Authenticator's Test for User Presence and User Verification

An ***External User Verification*** is the same as a user verification except that its user input comes from outside the authenticator boundary. It is marked as such with an `_EXTERNAL` suffix in the User Verification Methods in the "FIDO Registry of Predefined Values" [FIDORegistry] and may appear anywhere the `USER_VERIFY` constants are used (e.g., Metadata and userVerificationMethod extension). For example, `USER_VERIFY_PASSCODE_EXTERNAL` is a PIN authenticator for which the PIN input (keyboard, touch screen or such) is outside of the authenticator boundary.

The only user verification methods that may be designated as `_EXTERNAL` are PIN, password, passcode and pattern. Biometric user verification may not be designated as `_EXTERNAL`.

Implementations of clientPIN and common HLOS PINs (lock screen) can be either external user verification or internal (no `_EXTERNAL` suffix) depending on where the authenticator boundary is drawn. At L1 and L1+ the HLOS is often inside the authenticator boundary. At L2 and higher, since the HLOS is rarely inside the authentication boundary, they will typically have to be external user verification.

PIN entry is considered to provide a user presence check. While external user verification is allowed, external user presence checking is not, generally implying that a user verification that is also providing a user presence check must be inside the authenticator boundary.

> NOTE
>
> A common scenario occurs with an authenticator typically called a *security key* that has a user presence check that is inside the authenticator boundary, but relies on the CTAP clientPIN for user verification. It would thus declare `USER_VERIFY_PASSCODE_EXTERNAL` and `USER_VERIFY_PRESENCE` in its metadata or UVM extension and is certifiable at L2 and higher.

> NOTE

Some may consider external user verification methods to have different security characteristic from those that are not.

Also see the "FIDO Technical Glossary" [FIDOGlossary]. The definitions here are normative and take precedence over those in the FIDO Glossary.

No.	Requirement	Security Measures
	UAF + U2F + FIDO2; Consumer + Enterprise; TVFR; L1 and higher	
3.1	If the Authenticator indicates it can perform or has performed a user presence check, the Authenticator shall provide a mechanism to obtain a gesture or action from the user establishing the user authorizes the given authentication action. For U2F, indication is by the user presence bit in the Authentication Response Message (see [U2FRawMsgs]). In UAF, this is indicated by `USER_VERIFY_PRESENCE` being set in the `USER_VERIFY` flags defined in the "FIDO Registry of Predefined Values" [FIDORegistry]. This indication may appear in the VerificationMethodDescriptor in the metadata for the authenticator. It may also appear in the userVerificationMethod extension (fido.uaf.uvm) [UAFRegistry] in either a registration assertion (TAG_UAFV1_REG_ASSERTION) or an authentication assertion (TAG_UAFV1_AUTH_ASSERTION). If it is indicated in the metadata and the userVerificationMethod extension is present, it must also be indicated in the extension. It is not allowed for the metadata to indicate `USER_VERIFY_PRESENCE` and for there to be no user presence check performed (see [UAFAuthnrCommands], [UAFAuthnrMetadata]). In FIDO2 this is indicated by the "up"=1 flag in the MakeCredential or GetAssertion responses (see [FIDOCTAP]). NOTE This requirement prevents remote attacks. The user has to confirm an action by pressing a button or providing some other (physical) gesture. NOTE A user presence check could be implicit as part of a user verification such as the case with a fingerprint Authenticator where the user always performs an action. A user presence check could also be part of but separate from an authentication such having to push a button at the same time face recognition is happening. It can also just be a simple push of a button with no user verification at all. NOTE Any user verification method that implicitly performs a user presence check must explicitly indicate that it does, or it will be assumed that it does not. For example, all fingerprint Authenticators should indicate they perform user presence check by setting "up"=1 for FIDO2 and `USER_VERIFY_PRESENCE` for UAF.	(SM-1, SM-5)

NOTE

The metadata indication of support for user presence check is irrelevant for certification for U2F and FIDO2, but not UAF. Metadata is the only way for UAF implementations that do not support the fido.uaf.uvm extension to indicate support for user presence check to the relying party.

Calibration

No calibration required.

All Levels Vendor Questionnaire

This requirement MUST be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.

All Levels Test Procedure

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

UAF + U2F + FIDO2; Consumer + Enterprise; TVFR; L1 and higher

For FIDO2, if an Authenticator indicates "uv"=1 in either a GetAssertion or a MakeCredential, then the Authenticator MUST have a mechanism to verify the user and have performed user verification or have accepted and verified the pinAuth parameter. (see [FIDOCTAP]).

Similarly, for UAF, if an Authenticator indicates it performed user verification in either a registration or authentication by way of the User Verification Method Extension (fido.uaf.uvm) [UAFRegistry], it MUST have performed a user verification.

If either a UAF, U2F or FIDO2 authenticator supplies metadata, it MUST correctly indicate how it supports user verification in the `userVerificationDetails` field [FIDOMetadataStatement]. If it is capable of performing user verification, it must list at least one alternative that is a user verification (e.g., one that is not just `USER_VERIFY_PRESENCE` or `USER_VERIFY_NONE` [FIDORegistry]). It must list all the user verification alternatives for all the types it supports.

If either a UAF, U2F or FIDO2 authenticator supplies metadata and implements a mode where no user verification is performed or might not be performed, it MUST list one user verification as `USER_VERIFY_NONE` in the metadata. (All FIDO2 and U2F 1.2 Authenticators are like this. UAF Authenticators can be like this, but almost never are.)

NOTE

The definition of user verification in the "FIDO Technical Glossary" [FIDOGlossary] considers user presence check to be a form of user verification. That definition is not applicable for this requirement.

3.2

NOTE

See note above on explicitly indicating User Presence for Authenticators that intrinsically perform User Presence as a part of User Verification.

(SM-1, SM-5)

NOTE

This requirement does not, nor any other requirement, gaurantee that user verification is always performed when FIDO2 MakeCredential or UAF registration happens. If a relying party wants this behavior, then it must make sure that it requests it during those operations or that the authenticator does not indicate `USER_VERIFY_NONE` in its metadata.

Calibration

No calibration required.

All Levels Vendor Questionnaire

This requirement MUST be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.

All Levels Test Procedure

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

3.3	**3.3 was removed.**

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

A time period after a successful user verification, user presence check or both is defined as the *cached period*. During the cached period the user verification and/or presence check stays valid and the authenticator can perform multiple operations such as registration, generating authentication assertions, enrolling new biometrics without further user verification or presence check. The cached period starts when user verification and/or presence check completes successfully.

A cached period is one of three types:

1. user verification
2. user presence check
3. user verification and user presence check

A cached period's type is set when it starts and cannot be changed. If another type is needed, a new user verification and/or presence check must be performed; all timeouts and the associated relying party reset.

The time from the start of the cached period until the first authenticator operation starts is the *time-to-start* and has a maximum:

- The maximum time-to-start the authenticator reports to the relying party in a FIDO protocol response message.
- If no report to the relying party, the fixed maximum time-to-start the authenticator lists in its metadata.
- If none of the above, a base value of 30 seconds.

The time from the start of the cached period until the last authenticator operation completes is the *time-to-complete* and has a maximum:

- The maximum time-to-complete the authenticator reports to the relying party in a FIDO protocol response message.
- If no report to the relying party, the fixed maximum time-to-complete the authenticator lists in its metadata.
- If none of the above, a base value of 10 minutes.

During the cached period, multiple operations (e.g. CTAP methods), may be invoked in the authenticator. A relying party is associated with each cached period. This may be set when it is first created. If not set explicitly when created, then it is set to the first relying party the cached period is used with. If a subsequent operation is invoked for a different relying party, the authenticator must either reject that operation or initiate a new cached period by performing a new user verification and/or presence check.

Only one use of the cached user presence check is allowed. Once it is used, a new user presence check must be performed.

Any authenticator-external identifier (e.g., `pinUvAuthToken`) used by a client to refer to a particular cached period instance must be unique for that the authenticator (See also requirement 2.2.1).

> NOTE
>
> This requirement is general and applies to all user verification and/or user presence check caching mechanisms. It covers `pinToken`, `pinUvAuthToken`, future mechanisms, proprietary mechanisms and so on.
>
> This requirement is general and applies to any FIDO protocol mechanisms or extensions for the relying party to request a particular timeout and for the authenticator to report the timeout in effect. This requirement applies to existing mechanisms like `UserVerificationCaching`, modifications to `UserVerificationCaching` or any future mechanisms or extensions, either standardized or proprietary.
>
> This requirement is designed to work equally for authenticators that do user verification, biometric enrollment and credential management within the authenticator boundary as for authenticators that use External User Verification (collect PIN input outside the authenticator boundary).

> NOTE
>
> To follow this requirement, an authenticator must either adhere to the base maximum timeout values, report a different value in the metadata or report a different value in FIDO protocol messages.
>
> For operations like biometric enrollment that do not associate a relying party, timeouts are either fixed as described in the metadata or are the base values.
>
> As of the initial writing of this requirement (January 2020), there are no metadata fields to report the time-to-start or the time-to-complete. There is only one protocol mechanism, `UserVerificationCaching`, and it only allows selecting and reporting time-to-complete only for UAF. Until additions are made to the metadata statements or `UserVerificationCaching` is defined for FIDO2 or such, all certified FIDO2 implementations must implement only the base values and there is no way for the relying party to request otherwise.
>
> It is allowed for the authenticator to implement additional timeouts such as a lack-of-activity timeout that expires after 30 seconds of receiving no CTAP commands as long as the above requirements are still met.

These timeouts are maximums. An authenticator may use shorter timeouts. If an authenticator uses shorter timeouts it is does not need to report them to the relying party.

The purpose of the maximum time-to-start is to be sure the user can know that they are authorizing for a particular relying party and only that relying party. For example, they might verify for a transaction for First Bank. Something may go wrong with that transaction with no assertion generated for it. If there is no maximum time-to-start, many minutes later, an assertion for Second Bank might be generated without any user verification required.

The purpose of the maximum time-to-complete is to limit the time for which authentication is valid for the associated relying party. To give an example of what happens without this timeout, an attacker may come to "own" the non-authenticator part of a user's phone that was used to log in to a bank. That attacker would be able to log back into that bank for hours or days. The bank's server timeouts do not help because the attacker can just re authenticate.

The 10-minute base value for time-to-complete is for two reasons. The first is to allow biometric enrollment, which may involve a number of steps to complete. The second is to accommodate worst-case scenarios such a slow and simple authenticator working with a large number of credentials over a slow CTAP connection that might take as much as 10 minutes to complete.

The [FIDOCTAP] specification has text discussing the lifetime of getting a `pinToken` from the authenticator, suggesting they can be generated once at power up implying no timeouts are necessary. To pass certification, even at L1, the timeouts described here are required.

Some may consider these timeouts to be of little benefit for authenticators using External User Verification because the attacker outside the authenticator boundary can capture and replay the PIN whenever the timeout goes off to renew their authentication. While this is true, not all authenticators collect the PIN outside the authenticator boundary and it is simpler to have a uniform timeout requirement for all authenticators.

NOTE

The first operation in a cached period may have no associated relying party (e.g. a biometric enrollment). It is currently allowed for subsequent authenticator operations for the same cached period to then have an associated relying party. For example, the user might initiate and complete a biometric enrollment in 5 minutes and then 4 minutes later authenticate to a relying party. There would be a user verification when the biometric enrollment started, but not necessarily for the authentication to the relying party. Similar is true when the relying party operation is first. Note that this gives a 10-minute window after the start of a biometric enrollment for an attacker controlling the platform to generate authentications for one relying party. This non-requirement allows for biometric enrollment and registration with a relying party to be performed in line / together and require only one user verification.

3.4

NOTE

The CTAP specification refers to the authenticator-external identifier as the `pinToken` or `pinUvAuthToken`, a randomly generated byte string whose length is a multiple of 16 bytes. Some versions of the CTAP specification say it should be generated once on power up. For certification, this is not allowed. It must be a new identifier for each cached period.

Multiple cached periods (e.g., `pinUvAuthTokens`) are allowed simultaneously, but not required.

See also requirement 2.2.1 which requires the identifier be generated with a certified random number generator.

(SM-5)

Calibration

L1: At L1, the Authenticator Application SHALL follow best security practices specific to the underlying operating environment to enforce the cached periods.

L1+: At L1+, the Authenticator Application SHOULD minimize its dependency to the underlying operating environment. This characteristic will be verified as specified in section Specific Calibration for Level 1+ ..

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

L3 GlobalPlatform: At L3 GlobalPlatform, the protection mechanisms SHALL resist attackers with *Enhanced-basic* attack potential [TEE-PP]. The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]).

L3: At L3, the requirement SHALL be fulfilled so as to protect 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 requirement SHALL be fulfilled so as to protect 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.

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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test 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:

- Development Information (High Level Design)
- Test 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Partner Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

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

The Tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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.

3.5

UAF; Consumer + Enterprise; GaVR-1; L1 and higher

3.5 was removed.

3.6

UAF; GaVR-1; L1 and higher

3.6 was removed.

UAF + U2F + FIDO2; Consumer + Enterprise; L2 and higher

All Authenticator user input and output must 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 software outside of the AROE.

At some certifications levels an exception is made to this requirement for external user verification. See the calibration for this requirement.

UAF Transaction Confirmation only has to adhere to this requirement and use a trusted path when it sets either the `TRANSACTION_CONFIRMATION_DISPLAY_TEE` or `TRANSACTION_CONFIRMATION_DISPLAY_HARDWARE` flag in `tcDisplay`. There is no exception for FIDO2 ***Transaction Authorization Extensions*** [WebAuthn].

NOTE

All Authenticators have a need to accept user input or provide user output except those that are Silent Authenticators [FIDOGlossary] or exclusively implement external user verification.

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 any user output performed under this requirement needs to be protected from a display overlay attack.

The exception for external user verification methods is only for the user input and output. Stored / enrolled reference data (templates) and the comparison of the input to these must still be protected per requirements at the required calibration level.

Relation to Companion Program

L3 GlobalPlatform: (If Authenticator is not silent) AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM] and [TEE-PP]).

Remark: The input/output from/to the user should be provided through the AROE's TUI and/or biometric system.

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

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

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

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

Calibration

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

Authenticators may implement external user verification. If they do so, they must indicate so in both the metadata and in the UVM extension.

L3 GlobalPlatform: At L3 GlobalPlatform, the protection mechanisms SHALL resist attackers with Enhanced-basic attack potential (see [TEE-PP]). The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]).

Authenticators that implement external user verification methods must indicate so in both the metadata and in the UVM extension.

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation

- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The Tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; GaVR-3; L1 and higher

If the Authenticator claims to accept any input from the user, then the Authenticator SHALL protect against injection or replay of user verification data (e.g. password, PIN, biometric data and such) and/or the user presence check signal.

When we say "the Authenticator claims to accept any input from the user", we mean that the Authenticator declares a user verification or user presence check method other than external user verification methods.

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to FTP_ITC.1 component (see [TEE-PP]).

Remark: Protection of user verification data should be provided through the AROE TUI and/or biometric system.

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

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

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

This requirement is linked to 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 or user presence checkdata. This especially means that the Authenticator Application SHALL NOT provide any API for injecting FIDO user verification or user presence data.

L1+: At L1+, the Authenticator Application SHOULD minimize its dependency to the underlying operating environment and it SHALL implement software protection techniques to protect against replay and injection (e.g. obfuscation and anti-tracing). This characteristic will be verified as specified in section Specific Calibration for Level 1+ .

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

Authenticators may implement external user verification methods. If they do so, they must indicate so in both the metadata and in the UVM extension.

L3 GlobalPlatform: At L3 GlobalPlatform, the protection mechanisms SHALL resist attackers with Enhanced-basic attack potential (see [TEE-PP]). The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]).

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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

3.8

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-5, SM-27)

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The Tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 attack s. [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 dealing with such attacks.

NOTE

- The rate limiting requirement applies to all user verification methods (other than user presence check).
- The below calibration of the rate limiting for the different levels is expressed as a formula that expresses the chance a false input is accepted in a determined time period. The chance that your UV method accepts a false input (ie, randomly guessing the correct PIN, the FAR of a fingerprint, ...) times the allowed number of attempts in that period must be smaller or equal to this chance. Because of how the formula is constructed, you can allow a certain number of tries and then block without keeping time, as long as that puts the chance below the 170/10000. Note that if you increase the time period, the allowed chance will increase too but the higher you go in levels, the smaller the chance is per time period.
- Implementing a more strict rate limiting method is allowed.
- The rate limits were set to accomodate certain mobile phone PIN settings and are considered way too lax, which is why we recommend a much higher standard below.
- 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 16th 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 Companion Program

L3 GlobalPlatform: (Applicable if the implementation relies on AROE time stamp services) AROE Security Target , Development Information, Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement(see [TEE-EM]).

This requirement is linked to FPT_STM.1 (see [TEE-PP]).

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

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

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

This requirement is linked to FIA_UAU.2, 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

$P(t) \leq$ 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.

For a 6 digit PIN it means up to 17000 non-biometric user verification attempts in the first 6.4 days and then at least 1 hour delay per 100 of them.

For a biometric, the FAR times the number of allowed attempts must be smaller than 0.017 for the first 6.4 days. After those 6.4 days, the allowed chance will increase.

L1+: At L1+, the Authenticator Application SHOULD minimize its dependency to the underlying operating environment and it SHALL implement software protection techniques to protect the implementation of the measure (e.g. obfuscation and anti-tampering). The time dependent probability of a successful brute-force attack on the authenticator SHALL be

$P(t) \leq$ 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.

For a 6 digit PIN it means up to 17000 non-biometric user verification attempts in the first 12.8 days and then at least a two hour delay per 100 of them.

3.9	For a biometric, the FAR times the number of allowed attempts must be smaller than 0.017 for the first 12.8 days. After those 12.8 days, the allowed chance will increase. **L1+**: This characteristic will be verified as specified in section Specific Calibration for Level 1+ . **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. For a 6 digit PIN it means up to 17000 non-biometric user verification attempts in the first 12.8 days and then at least a two hour delay per 100 of them. For a biometric, the FAR times the number of allowed attempts must be smaller than 0.017 for the first 12.8 days. After those 12.8 days, the allowed chance will increase. At L2, the requirement SHALL be fulfilled by mechanisms functioning entirely inside the Authenticator Boundary, i.e. inside the AROE. **L3 GlobalPlatform**: At L3 GlobalPlatform, the protection mechanisms SHALL resist attackers with Enhanced-basic attack potential (see [TEE-PP]). The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]). 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. **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 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. **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	(SM-1, SM-5, SM-27)

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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The Tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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.

3.10	UAF + U2F + FIDO2; Consumer + Enterprise; 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 Companion Programs, Vendor Questionnaires, and Test Procedures for this requirement are all specified in [FIDOBiometricsRequirements]. **Calibration** **L3**: At L3, the requirement SHALL be fulfilled by mechanisms functioning entirely inside the AROE. **L3+**: At L3+, the requirement SHALL be fulfilled by mechanisms functioning entirely inside the AROE. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Operational User Guidance and Preparative Procedures Guidance • Mapping to Companion Program Requirements • FIDO Biometric Evaluation Report **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Operational User Guidance and Preparative Procedures Guidance • Mapping to Companion Program Requirements • FIDO Biometric Evaluation Report **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement. **L3+ Test Procedure** The Tester SHALL *conduct* vulnerability analysis and penetration testing to meet the calibration requirements.	(SM-1, SM-5, SM-27)
	UAF + FIDO2; Consumer + Enterprise; TVFR; L1 and higher A FIDO authenticator MUST indicate it supports user verification in its GetInfo response if at any time it indicates it performed user verification in	

a FIDO2 MakeCredential or GetAssertion response (see [FIDOCTAP]), or in a UAF authentication or UAF registration response. (see [UAFProtocol])

If an authenticator indicates it always performs user verification in its metadata statement then it must always indicate it performs user verification in its GetInfo response. Indication that user verification is always performed in the metadata is by way of setting one or more of the defined bits for the different types of user verification (e.g., setting `USER_VERIFY_FINGERPRINT`). That is, setting any bit other than `USER_VERIFY_PRESENCE`, `USER_VERIFY_NONE` or `USER_VERIFY_ALL`. (see [UAFAuthnrCommands], [UAFAuthnrMetadata])

If an authenticator indicates it supports user verification in its GetInfo response then it MUST always indicate that in its GetInfo response until factory reset is performed.

If an authenticator indicates it supports user verification in its GetInfo response, it MUST perform user verification before these three operations:

1. Enabling additional user verification methods.
2. Adding, changing or removing user verification reference data (e.g. PIN or biometric templates).
3. Un-enrolling or removing credentials.

> NOTE
>
> This requirement is to ensure that authentication keys created under the control of one set of user verification data stay under control of the that set until factory reset, even through expansion of that set of user verification data through additional verification data and methods.

> NOTE
>
> This requriement assumes there is only one set of user verification reference data per authenticator and every biometric template, PIN and such is equivalent.

> NOTE
>
> If any one of the authenticator's user verification methods is an external user verification, this may be used to allow changing the user verification reference data of a user verification method inside the authenticator boundary. Some relying parties may consider this to reduce the security of the user verification methods inside the authenticator boundary.

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation documentation MUST be provided to support this requirement (see [TEE-EM] and [TEE-PP]).

Remark: The User Verification should be provided through the AROE's TUI and/or biometric system.

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

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

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

This requirement is linked to 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.

3.11

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

(SM-1, SM-5)

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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.

3.4 Privacy

		Security

No.	Requirement	Measures
	UAF + U2F + FIDO2; Consumer; GaVR-1; L1 and higher	
	An Authenticator SHALL NOT have any ***Correlation Handle*** that is visible across multiple Relying Parties. If the authenticator puts the exact identical attestation key into a group of Authenticators (e.g., group of devices, phones, security keys...) so that the attestation key doesn't become a Correlation Handle, then each group of Authenticators MUST be at least 100,000 in number. If less than 100,000 Authenticators are made, then they MUST all have the same attestation key. NOTE The goal of this requirement is that, for privacy reasons, the Authenticator will not leak information about the user across multiple Relying Parties by sharing a Correlation Handle . This requirement specifically applies to KeyIDs/CredentialIDs, KeyHandles etc. The public key used to verify a signed attestation, or the key ID of the public key used to verify an attestation becomes a Correlation Handle when it is unique per Authenticator and used with an attestation scheme like Full Basic Attestation. One approach to mitigate this is to use the indentical key in 100,000 or more authenticators. **Relation to Companion Program** **L3 GlobalPlatform**: Not applicable to the AROE. **L3 Common Criteria**: A Security Target , Development Information and Test Documentation MUST be provided (see [CC1V3-1R5]). This requirement is linked to FPR_ANO.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). Alternatively, FPR_UNL.1.1 can be used. **L3+ Common Criteria**: A Security Target , Development Information and Test Documentation MUST be provided (see [CC1V3-1R5]). This requirement is linked to FPR_ANO.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). Alternatively, FPR_UNL.1.1 can be used. **Calibration** No calibration required. **L1 Vendor Questionnaire** *Provide* the Security Secretariat with a rationale of how the requirement above is met.	

4.1

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

(SM-23)

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The Tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer; 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 Companion Program

L3 GlobalPlatform: Not applicable to the AROE.

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

4.2

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The Tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_RNG.1 component (see [TEE-PP]).

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

This requirement is linked to FPR_UNL.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

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

This requirement is linked to FPR_UNL.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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

4.3

(SM-23)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The Tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; GaVR-1; L1 and higher

The Authenticator's response to a "Deregister" command SHALL NOT reveal whether the provided KeyID was registered.

Relation to Companion Program

L3 GlobalPlatform: Not applicable to the AROE.

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

4.4

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: Not applicable to the AROE.

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

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

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

This requirement is linked to 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, this requirement MUST be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)

4.5 SM-5

- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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.

4.6	FIDO2; Consumer + Enterprise; GaVR-1; L1 and higher The Authenticator SHALL implement the CredProtect extension. **All levels** This requirement MUST be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required. **All Levels Test Procedure** {A0} The Security Secretariat SHALL *verify* the requirement during Interoperability Testing.	SM-5
	FIDO2; Consumer + Enterprise; GaVR-1; L1 and higher Depending on the CredProtect Level of the created Credential, an Authenticator SHALL NOT reveal certain information. This includes in the protocol response, on any display the authenticator may have or any other method. **Presence of credentials** If the credential was created with the **userVerificationOptionalWithCredentialIDList** option, the Authenticator SHALL NOT reveal whether a key was registered for the given RP ID without the Authenticator either (1) requiring a Credential ID as input or (2) verifying the user (using a method other than user presence check). If the credential was created with the **userVerificationRequired** option, the Authenticator SHALL NOT reveal whether a key was registered for the given RP ID without the Authenticator verifying the user (using a method other than user presence check). **User fields** If the Credential was created with the **userVerificationOptionalWithCredentialIDList**, **userVerificationRequired** or **userVerificationOptional** option, the Authenticator SHALL NOT reveal Name, DisplayName and Icon of a User without verifying the user (using a method other than user presence check). The User ID field MAY be returned if a signature is returned. **RP fields.** If the Credential was created with the **userVerificationRequired** option, the Authenticator SHALL NOT reveal ID, Name and Icon of a RP without verifying the user (using a method other than user presence check). If the Credential was created with the **userVerificationOptionalWithCredentialIDList**, the Authenticator SHALL NOT reveal ID, Name and Icon of an RP without either (1) requiring a Credential ID as input or (2) verifying the user (using a method other than user presence check). If the Credential was created with the **userVerificationOptional** option, the Authenticator MAY reveal Name, DisplayName and Icon of an RP without verifying the user. NOTE If User Verifcation is NOT performed this comes down to: **Information** | **userVerificationRequired** | **userVerificationOptionalWithCredentialIDList** | **userVerificationOptional**	

Presence of credentials	No	If provided in the credential list	Yes
User Name, User DisplayName, User Icon	No	No	No
User ID	No	If provided in the credential list	Yes
RP ID, RP Name and RP Icon	No	If provided in the credential list	Yes

NOTE

This requirement does not specify a default for the CredProtect value because this depends on the version of the technical specification. Because the CredProtect extension was defined after the initial spec (FIDO_2_0) was released, the default is **userVerificationOptional** as this is the behavior specified in that spec. With this default, it is possible to implement the CredProtect extension without violating the initial spec.

Once a new specification is released (or at least defined), we can either define the default here provided we link it to the technical spec version identifier or we can leave the definition of the default up to the technical spec.

Relation to Companion Program

L3 GlobalPlatform: Not applicable to the AROE.

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

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

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

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

Calibration

No calibration required.

4.7	**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. **L1+ Vendor Questionnaire** *Provide* the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design). **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 GlobalPlatform Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting evidence: • Development Information (Architecture and Interfaces) • Test Documentation • Mapping to Companion Program Requirements • Source Code (optionally) **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Development Information (High Level Design) • Test Documentation • Mapping to Companion 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: • Development Information (Low Level Design) • Test Documentation	(SM-5, SM-10)

- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; GaVR-1; L1 and higher

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

Relation to Companion Program

L3 GlobalPlatform: Not applicable to the AROE.

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

4.8

L3 Vendor Questionnaire

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

- Development Information (High Level Design)

(SM-5, SM-10)

- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; GaVR-1; L1 and higher

The Authenticator SHALL NOT output unencrypted AppIDs or KeyIDs that are associated with a Key Handle prior to verifying the user.

Relation to Companion Program

L3 GlobalPlatform: Not applicable to the AROE.

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

This requirement is linked to FPT_ITC.1, FIA_UAU.2, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

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

This requirement is linked to FPT_ITC.1, 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation

Mapping to Companion Program Requirements

- Source Code (optionally)

L3 Vendor Questionnaire

4.9 Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: (SM-5, SM-23)

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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.

FIDO2; Enterprise; GaVR-1; L1 and higher

An Authenticator SHALL NOT have any ***Correlation Handle*** that is visible across multiple Relying Parties, except the unique identifier present in the Enterprise Attestation Certificate or the Enterprise Attestation Certificate itself.

NOTE

The goal of this requirement is that, for privacy reasons, the Authenticator will not leak information about the user across multiple Relying Parties by sharing a Correlation Handle, except what is available through Enterprise Attestation.

This requirement specifically applies to KeyIDs/CredentialIDs, KeyHandles etc.

Relation to Companion Program

L3 GlobalPlatform: Not applicable to the AROE.

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

4.10 (SM-23)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The Tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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.

FIDO2; Consumer; GaVR-1; L1 and higher

The Authenticator SHALL NOT support Enterprise Attestation. If the firmware supports Enterprise Attestation, it shall be disabled through the Security Configuration of the Authenticator in such a way only the vendor or its delegates can enable it.

Relation to Companion Program

L3 GlobalPlatform: Not applicable to the AROE.

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

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

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

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Calibration

No calibration required.

L1 Vendor Questionnaire

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

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

4.11

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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.

FIDO2; Enterprise; GaVR-1; L1 and higher

The FIDO2 Enterprise Attestation feature, mode 1, allows the Authenticator to be configured with a RP ID list. Authenticators that do

not support mode 2 will fall back to mode 1 when mode 2 is requested for compatibility reasons, this requirement also applies in that case.

The Authenticator MUST NOT return an Enterprise Attestation for RP IDs not on this list.

An Authenticator MAY require additional conditions before returning an Enterprise Attestation.

This list MUST contain only RP IDs owned by the Customer or its Data Processors (as defined by the GDPR).

This RP ID list MUST only be modifyable by the Vendor or its delegates, specifically, it MUST NOT be modifiable by the Customer.

Relation to Companion Program

L3 GlobalPlatform: Not applicable.

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

This requirement is linked to FDP_IFC/Authentication and FDP_IFF/Authentication (see [CC2V3-1R5] and [CC3V3-1R5]). The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows]

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

This requirement is linked to FDP_IFC/Authentication and FDP_IFF/Authentication (see [CC2V3-1R5] and [CC3V3-1R5]). The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows]

Calibration

No calibration required.

L1 Vendor Questionnaire

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

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

4.12 (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:

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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.

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

No.	Requirement	Security Measures
	UAF + U2F + FIDO2; Consumer + Enterprise; DaD; L2 and higher	
	The vendor SHALL document the physical security and side channel attack protections used by the Authenticator. **Relation to Companion Program** **L3 GlobalPlatform**: AROE Development Information , Operational User Guidance and Preparative Procedures Guidance MUST be provided to support this requirement (see [TEE-EM]). **L3 Common Criteria**: Development Information MUST be provided. This requirement is linked to Class ADV (see [CC3V3-1R5]). **L3+ Common Criteria**: Development Information MUST be provided. This requirement is linked to Class ADV (see [CC3V3-1R5]).	

5.1	**Calibration** No calibration required. **L2 Vendor Questionnaire** *Provide* the tester with documentation that specifies how the requirement above is met. **L3 GlobalPlatform Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting evidence: • Development Information (Architecture and Interfaces) • Mapping to Companion Program Requirements • Source Code (optionally) **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Development Information (High Level Design) • Mapping to Companion 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: • Development Information (Low Level Design) • Mapping to Companion Program Requirements • Source Code **L2 Test Procedure** {A2} The tester SHALL *verify* that the documentation meets the requirement. **L3 GlobalPlatform Test Procedure** The tester SHALL *verify* that the provided rationale and evidence meet the requirement. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement.	(SM-1, SM-20, SM-24, SM-26, SM-29)

L3+ Test Procedure

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

5.1.1	UAF + U2F + FIDO2; Consumer + Enterprise; DaD; L1+	(SM-1, SM-20, SM-24, SM-26, SM-29)

The vendor shall document the logical security and side channel attack protections used by the Authenticator.

Calibration

No calibration required.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L1+ Test Procedure

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

5.2	N/A

5.2 was removed.

UAF + U2F + FIDO2; Consumer + Enterprise; L3 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.

NOTE

Resistance to physical tampering obviates the need for physical tamper evidence.

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance and Preparative Procedures Guidance MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the AVA_VAN_AP.3 component (see [TEE-PP]).

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

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

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

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

5.3

Calibration

L3 GlobalPlatform: At L3 GlobalPlatform, the protection mechanisms SHALL resist attackers with Enhanced-basic attack potential (see [TEE-PP]). The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Mapping to Companion Program Requirements
- Source Code

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet 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.

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; Consumer + Enterprise; TVFR; L1+ and higher

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.

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 2.1.3, 2.2.4, 5.5, 5.6.

This is a requirement that provides flexibility in satisfying other requirements. The idea is that key use limit could 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 can 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 could 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 Companion Program

L3 GlobalPlatform: Not applicable to the AROE.

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

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

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

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

Calibration

No calibration required.

5.4

(SM-24, SM-26)

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 security strength of the key, even after an attacker has observed all allowed key uses.

> NOTE
>
> This interacts with requirement 5.4.

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance and Preparative Procedures Guidance MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the AVA_VAN_AP.3 component (see [TEE-PP]).

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

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

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

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

Calibration

L3 GlobalPlatform: At L3 GlobalPlatform, the protection mechanisms SHALL resist attackers with Enhanced-basic attack potential (see [TEE-PP]). The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]).

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]).

5.5

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Mapping to Companion Program Requirements
- Source Code (optionally)

(SM-20)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Mapping to Companion Program Requirements
- Source Code

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet 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.

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; Consumer + Enterprise; GaVR-3; L1+, 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 security strength.

NOTE

This requirement is mandatory for L1+, 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 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 will need to consider randomization of the control flow so that there is no fixed relation between the execution path and the cache set. Or, it will 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.

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target, Development Information, Operational User Guidance and Preparative Procedures Guidance MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the Enhanced-basic attack potential component (see [TEE-PP]).

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

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

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

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

Calibration

L1+: At L1+, the Authenticator Application SHALL implement adequate countermeasures to protect against timing attacks. This characteristic will be verified as specified in section Specific Calibration for Level 1+.

L3 GlobalPlatform: At L3 GlobalPlatform, the protection mechanisms SHALL resist attackers with Enhanced-basic attack potential (see [TEE-PP]). The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]).

5.6

(SM-20, SM-29)

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 tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Mapping to Companion Program Requirements
- Source Code

L1+ Test Procedure

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

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance and Preparative Procedures Guidance MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the AVA_VAN_AP.3 component (see [TEE-PP]).

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

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

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

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

Calibration

No calibration required.

5.7	**L3 GlobalPlatform Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting evidence: • Development Information (Architecture and Interfaces) • Mapping to Companion Program Requirements • Source Code (optionally) **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Development Information (High Level Design) • Mapping to Companion 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: • Development Information (Low Level Design) • Mapping to Companion Program Requirements • Source Code **L3 GlobalPlatform Test Procedure** The tester SHALL *verify* that the provided rationale and evidence meet the requirement. The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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. **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-20, SM-29)

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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance and Preparative Procedures Guidance MUST be provided to support this requirement (see [TEE-EM] and [TEE-PP]).

L3 Common Criteria: A Security Target , Development Information , Test Documentation and Preparative Procedures Guidance documentation MUST be provided.

This requirement is linked to FPT_TST.1, AGD_PRE, Class ADV and ATE.

L3+ Common Criteria: A Security Target , Development Information , Test Documentation and Preparative Procedures Guidance documentation MUST be provided.

This requirement is linked to FPT_TST.1, AGD_PRE, Class ADV and ATE.

Calibration

No calibration

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source code (optionally)

L3 Vendor Questionnaire

5.8 Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: (SM-23,

- Development Information (High Level Design)
- Test Documentation
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source Code

SM-26)

L3+ Vendor Questionnaire

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

- Development Information (Low Level Design)
- Test Documentation
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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.

5.8.1

The Authenticator should detect any debug activity and prevent from violation of FIDO Authenticator Security Goals or FIDO Authenticator Security Requirements.

Calibration

At L1+, the Authenticator Application SHOULD minimize its dependency to the underlying operating environment and it SHALL implement anti-debugging techniques.

This characteristic will be verified as specified in section Specific Calibration for Level 1+.

(SM-23, SM-26)

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L1+ Test Procedure

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

UAF + U2F + FIDO2; Consumer + Enterprise; L1+, L3 and higher

The Authenticator SHALL be resistant to induced fault attacks.

> NOTE
>
> This requirement is mandatory for L1+, L3 and higher but it is still relevant for L2 and higher as a developer guideline. The developer will need to take into account SW-based fault induction side channel attack and implement relevant countermeasures such as enabling memory error detection.

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target, Development Information, Operational User Guidance and Preparative Procedures Guidance MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the AVA_VAN_AP.3 component (see [TEE-PP]).

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

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

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

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

Calibration

L1+: At L1+, the Authenticator Application SHOULD minimize its dependency to the underlying operating environment and it SHALL implement software protection techniques to protect against induced fault attack (e.g. whitebox crypto and anti-tampering). This characteristic will be verified as specified in section Specific Calibration for Level 1+.

L3 GlobalPlatform: At L3 GlobalPlatform, the protection mechanisms SHALL resist attackers with Enhanced-basic attack potential (see [TEE-PP]). The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]).

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]).

5.9

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design). (SM-28, SM-21)

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Mapping to Companion Program Requirements
- Source Code

L1+ Test Procedure

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

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* the provided rationale and evidence meet 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.

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.

3.6 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; Consumer + Enterprise; TVFR; L1+ and higher	
	The vendor SHALL use attestation certificates / ECDAA Issuer public keys [FIDOEcdaaAlgorithm] dedicated to a single Authenticator model.	

Relation to Companion Program

L3 GlobalPlatform : Not applicable to the AROE.

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

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

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

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

Calibration

No calibration required.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source Code

6.1 (SM-3)

L3+ Vendor Questionnaire

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

- Development Information (Low Level Design)
- Test Documentation
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source Code

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform : Not applicable to the AROE.

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source code (optionally)

6.2 (SM-3)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence 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; Consumer + Enterprise; GaVR-1; L1 and higher

The Authenticator SHALL accurately describe itself in its provided metadata. The vendor SHALL provide all mandatory Metadata Statement fields see [FIDOMetadataRequirements].

Relation to Companion Program

L3 GlobalPlatform : Not applicable to the AROE.

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

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

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

This requirement is linked to 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.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)

6.3	• Operational User Guidance and Preparative Procedures Guidance • Mapping to Companion Program Requirements • Source code (optionally) **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Development Information (High Level Design) • Operational User Guidance and Preparative Procedures Guidance • Mapping to Companion 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: • Development Information (Low Level Design) • Operational User Guidance and Preparative Procedures Guidance • Mapping to Companion Program Requirements • Source Code **L1 Test Procedure** {A0} The Security Secretariat SHALL *verify* the requirement during Interoperability Testing. **L1+ Test Procedure** {A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale. **L3 GlobalPlatform Test Procedure** The Tester SHALL *verify* that the provided rationale and evidence meet the requirement. **L3 Test Procedure** The Tester SHALL *verify* the provided rationale and documentation meets the requirement.	(SM-3)

L3+ Test Procedure

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

UAF + U2F + FIDO2; Consumer + Enterprise; DaD; L1+ 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 Companion Program

L3 GlobalPlatform : Not applicable to the AROE.

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

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

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

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

Calibration

No calibration required.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements

6.4	• Source code (optionally) **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Development Information (High Level Design) • Operational User Guidance and Preparative Procedures Guidance • Mapping to Companion 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: • Development Information (Low Level Design) • Operational User Guidance and Preparative Procedures Guidance • Mapping to Companion Program Requirements • Source Code **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 GlobalPlatform Test Procedure** The tester SHALL *verify* that the provided rationale and evidence 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.	(SM-3)
	UAF + FIDO2; Consumer + Enterprise; DaD; L1+ and higher	
	The vendor SHALL document whether the attestation certificate includes the Authenticator model (e.g. AAID or AAGUID).	

Relation to Companion Program

L3 GlobalPlatform : Not applicable to the AROE.

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

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

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

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

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source code (optionally)

6.5

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source Code

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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence 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.

FIDO2; Enterprise; GaVR-1; L1+ and higher

An Enterprise Attestation capable Authenticator that inserts a unique identifier in its Enterprise Attestation certificate SHALL use a unique private key per identifier.

Calibration

No calibration required.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

6.6

(SM-23)

L3+ Vendor Questionnaire

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

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The Tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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.

3.7 Operating Environment

NOTE

At L1 and L1+ we allow the Authenticator Application to run in any operating environment. At L1+ we expect the Authenticator Application to have substantial self-protection measures against hostile operating environments. For the levels L2 through L3+, the Authenticator Application needs to run in an Allowed Restricted Operating Environment [FIDORestrictedOperatingEnv]. Consequently the requirements in this section only apply to L2 and higher, except requirement 7.7.

No.	Requirement	Security Measures
	UAF + U2F + FIDO2; Consumer + Enterprise; GaVR-1; L2 and higher	
	The Authenticator Application SHALL run in an Allowed Restricted Operating Environment (AROE)[FIDORestrictedOperatingEnv].	

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target, Operational User Guidance and Preparative Procedures Guidance MUST be provided to support this requirement (see [TEE-EM] and [TEE-PP]).

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

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

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

This requirement is linked to 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.

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source code (optionally)

7.1 (SM-1)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion 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 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence 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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Operational User Guidance and Preparative Procedures Guidance MUST be provided to support this requirement (see [TEE-EM] and [TEE-PP]).

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

This requirement is linked to ASE_SPD, AGD_OPE, AGD_PRE and Class ATE (see [CC3V3-1R5]).

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

This requirement is linked to 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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source code (optionally)

7.2

L3 Vendor Questionnaire

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

(SM-1)

- Development Information (High Level Design)
- Operational User Guidance and Preparative Procedures Guidance
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Operational User Guidance and Preparative Procedures Guidance
- Test Documentation
- Mapping to Companion 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Operational User Guidance and Preparative Procedures Guidance MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_COP.1, FDP_ACC.1 , FDP_ACF.1 , FDP_IFC.2 , FDP_IFF.1 , FDP_ITT.1 , FDP_RIP.1, FDP_ROL.1, FIA_ATD.1, FIA_UID.2, FIA_USB.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FPT_FLS.1, FPT_INI.1 and FPT_ITT.1 components (see [TEE-PP]).

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

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

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

This requirement is linked to 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 GlobalPlatform: At L3 GlobalPlatform, the protection mechanisms SHALL resist attackers with Enhanced-basic attack potential (see [TEE-PP]). The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]).

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

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source code (optionally)

(SM-1)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion 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:

- Development Information (Low Level Design)

- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion 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 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Operational User Guidance and Preparative Procedures Guidance MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FAU_ARP.1, FPT_FLS.1, FPT_INI.1 and FPT_TEE.1 components (see [TEE-PP]).

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

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

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

This requirement is linked to 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 GlobalPlatform: At L3 GlobalPlatform, the protection mechanisms SHALL resist attackers with Enhanced-basic attack potential (see [TEE-PP]). The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]).

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.

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)

7.4 (SM-1)

- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion 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 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet 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.

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; Consumer + Enterprise; 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 will include all security configuration items available to the user.

Relation to Companion Program

L3 GlobalPlatform: AROE Security Target , Operational User Guidance and Preparative Procedures Guidance MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FPT_INI.1, FPT_FLS.1 and FPT_TEE.1 components (see [TEE-PP]).

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

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

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

This requirement is linked to 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.

7.5

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Operational User Guidance and Preparative Procedures Guidance

(SM-1, SM-28)

- Mapping to Companion Program Requirements
- Source code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion 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 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence 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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Preparative Procedures Guidance and Operational User Guidance MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FCS_COP.1, FPT_INI.1, FPT_FLS.1 and FPT_TEE.1 components (see [TEE-PP]).

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

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

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

This requirement is linked to 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.

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source code (optionally)

7.6 (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:

- Development Information (High Level Design)
- Operational User Guidance and Preparative Procedures Guidance

- Mapping to Companion 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:

- Development Information (Low Level Design)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion 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 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence 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.

FIDO2; Enterprise; GaVR-1; L1 and higher

The Vendor MUST verify that the RP ID list provided by the Customer and configured into the device only contains RP IDs owned by the Customer or the Customer's Data Processors (as defined by the GDPR).

If the device supports EA mode 2, the Vendor SHALL inform the Customer that the RP IDs configured in the browsers can only be RP IDs owned by the Customer or the Customer's Data Processors (as defined by the GDPR).

Relation to Companion Program

L3 GlobalPlatform: Not Applicable.

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

This requirement is linked to AGD_OPE and AGD_PRE (see [CC3V3-1R5]).

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

This requirement is linked to AGD_OPE and AGD_PRE (see [CC3V3-1R5]).

Calibration

No calibration required.

L1 Vendor Questionnaire

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

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source code (optionally)

7.7 (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:

- Development Information (High Level Design)

- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Operational User Guidance and Preparative Procedures Guidance
- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

{A2} The Security Secretariat SHALL *review* the provided rationale to verify the requirement is met.

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 are consistent with the vendor's provided rationale.

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence 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.

3.8 Self-Tests and Firmware Updates

No.	Requirement	Security

		Measures
	UAF + U2F + FIDO2; Consumer + Enterprise; 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 Companion Program** **L3 GlobalPlatform**: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]). This requirement is linked to the FAU_ARP.1, FPT_TEE.1, FPT_INI.1, FCS_COP.1 and FPT_FLS.1 components (see [TEE-PP]). **L3 Common Criteria**: A Security Target , Development Information and Test Documentation MUST be provided (see [CC1V3-1R5]). This requirement is linked to 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 Information and Test Documentation MUST be provided (see [CC1V3-1R5]). This requirement is linked to 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 GlobalPlatform Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting evidence: • Development Information (Architecture and Interfaces) • Test Documentation • Mapping to Companion Program Requirements • Source Code (optionally)	

8.1	**L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Development Information (High Level Design) • Test Documentation • Mapping to Companion 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: • Development Information (Low Level Design) • Test Documentation • Mapping to Companion 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 GlobalPlatform Test Procedure** The tester SHALL *verify* that the provided rationale and evidence meet the requirement. The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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. **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-21, SM-24)

8.1.1	UAF + U2F + FIDO2; Consumer + Enterprise; GaVR-2; L1+ An Authenticator shall either (a) be resistant to induced fault analysis (requirement 5.9) or (b) during runtime an Authenticator shall run known answer self-tests 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. **Calibration** No calibration required. **L1+ Vendor Questionnaire** Is this requirement applicable to the Authenticator? If **No**, then *describe* why. *Provide* the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design). **L1+ Test Procedure** {A2} The tester SHALL *verify* that the documentation meets the requirement.	(SM-21, SM-24)
	UAF + U2F + FIDO2; Consumer + Enterprise; 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 Companion Program** **L3 GlobalPlatform**: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]). This requirement is linked to the FAU_ARP.1, FPT_TEE.1, FPT_INI.1, FCS_COP.1 and FPT_FLS.1 components (see [TEE-PP]). **L3 Common Criteria**: A Security Target , Development Information and Test Documentation MUST be provided (see [CC1V3-1R5]). This requirement is linked to FCS_COP.1, FPT_TST.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]). **L3+ Common Criteria**: A Security Target , Development Information and Test Documentation MUST be provided (see [CC1V3-1R5]). This requirement is linked to 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.

L1+ Vendor Questionnaire

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

If Yes, *provide* the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

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:

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation

- Mapping to Companion Program Requirements
- Source Code

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE Security Target , Development Information , Operational User Guidance , Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]).

This requirement is linked to the FAU_ARP.1, FPT_TEE.1, FPT_INI.1, FCS_COP.1 and FPT_FLS.1 components (see [TEE-PP]).

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

This requirement is linked to 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 Information and Test Documentation MUST be provided (see [CC1V3-1R5]).

This requirement is linked to 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 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code (optionally)

8.3

(SM-21)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion 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 GlobalPlatform Test Procedure

The tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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; Consumer + Enterprise; L1+, L2+ and higher

If the Authenticator is not resistant to induced fault analysis as defined in requirement 5.9, the Authenticator SHALL verify that any produced signature is valid prior to outputting the signature.

Relation to Companion Program

L3 GlobalPlatform: If requirement 5.9 holds, then AROE Security Target, Development Information, Operational User Guidance, Preparative Procedures Guidance and Test Documentation MUST be provided to support this requirement (see [TEE-EM]). Otherwise, not applicable to the AROE.

This requirement is linked to the AVA_VAN_AP.3 component (see [TEE-PP]).

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

This requirement is linked to 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 Information and Test Documentation MUST be provided (see [CC1V3-1R5]).

This requirement is linked to FPT_PHP.3 and/or FPT_TST.1, Class ADV and ATE (see [CC2V3-1R5] and [CC3V3-1R5]).

Calibration

L1+: At L1+, the Authenticator Application SHOULD minimize its dependency to the underlying operating environment and it SHALL implement software protection techniques to protect against induced fault attacks (e.g.whitebox crypto for crypto operations, and anti-tampering to protect the signature verification).

This characteristic will be verified as specified in section Specific Calibration for Level 1+ .

L3 GlobalPlatform: At L3 GlobalPlatform, the protection mechanisms SHALL resist attackers with Enhanced-basic attack potential (see [TEE-PP]). The vulnerability assessment methodology is defined by AVA_VAN_AP.3 (see [TEE-PP] and [TEE-EM]).

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 tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L3 GlobalPlatform Vendor Questionnaire

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

- Development Information (Architecture and Interfaces)
- Test Documentation
- Mapping to Companion Program Requirements

8.4 (SM-21)

- Source Code (optionally)

L3 Vendor Questionnaire

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

- Development Information (High Level Design)
- Test Documentation
- Mapping to Companion 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:

- Development Information (Low Level Design)
- Test Documentation
- Mapping to Companion Program Requirements
- Source Code

L1+ Test Procedure

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

L3 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence meet the requirement.

The Tester SHALL *execute* independent tests and/or a sample of vendor tests to verify the 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.

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.

3.9 Manufacturing and Development

NOTE

At L1 and L1+, the creation of the final Authenticator Application is considered the Authenticator manufacturing.

No.	Requirement	Security Measures
	UAF + U2F + FIDO2; Consumer + Enterprise; 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 Companion Program** **L3 GlobalPlatform**: Not applicable to the AROE. **L3 Common Criteria**: A Security Target , Preparative Procedures Guidance and Development Security Life-Cycle Support MUST be provided (see [CC1V3-1R5]). This requirement is linked to ASE_SPD, AGD_PRE and ALC_DVS.1 (see [CC3V3-1R5]) **L3+ Common Criteria**: A Security Target , Preparative Procedures Guidance and Development Security Life-Cycle Support MUST be provided (see [CC1V3-1R5]). This requirement is linked to ASE_SPD, AGD_PRE and ALC_DVS.2 (see [CC3V3-1R5]) **Calibration** **L1**: At L1, the creation of the final Authenticator Application is considered the Authenticator manufacturing. **L1+**: At L1+, the creation of the final Authenticator Application (either final compilation or individualization of the compiled code) is	

considered the Authenticator manufacturing.

L2: No calibration required.

L3 GlobalPlatform: No calibration required.

L3: No calibration required.

L3+: No calibration required.

9.1

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.

L1+ Vendor Questionnaire

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

If Yes, *provide* the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

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 documentation references.

L3 GlobalPlatform 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:

- Operational User Guidance and Preparative Procedures Guidance
- Development Security Life-Cycle Support
- Mapping to Companion Program Requirements

L3+ Vendor Questionnaire

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

(SM-28)

- Operational User Guidance and Preparative Procedures Guidance
- Development Security Life-Cycle Support
- Mapping to Companion Program Requirements

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence 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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: Not applicable to the AROE.

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

This requirement is linked to ASE_SPD, AGD_PRE and ALC_DVS.1 (see [CC1V3-1R5]).

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

This requirement is linked to ASE_SPD, AGD_PRE and ALC_DVS.2 (see [CC3V3-1R5]).

Calibration

L1+: At L1+, this characteristic will be verified as specified in section Specific Calibration for Level 1+ .

The 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.

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 will 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.

L3 GlobalPlatform: At L3 GlobalPlatform, 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 will 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).

9.2 Security measures for protecting the life cycle management of the key generation and key provisioning SHALL be provided in the Vendor Questionnaire. (SM-28)

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.

L3: At L3, ALC_DVS.1 MUST be applied.

L3+: At L3+, ALC_DVS.2 MUST be applied.

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements. Please provide explicit documentation references.

L3 Vendor Questionnaire

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

- Development Security Life-Cycle Support
- Mapping to Companion Program Requirements

L3+ Vendor Questionnaire

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

- Development Security Life-Cycle Support
- Mapping to Companion Program Requirements

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and documentation 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; Consumer + Enterprise; TVFR; L1+ 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 Companion Program

L3 GlobalPlatform: Not applicable to the AROE.

L3 Common Criteria: A Development Security Life-Cycle Support documentation MUST be provided (see [CC1V3-1R5]).

This requirement is fulfilled 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 fulfilled by ALC_DVS.2 (see [CC3V3-1R5]).

9.3

Calibration

L1+: At L1+, this characteristic will be verified as specified in section Specific Calibration for Level 1+ .

All Authenticator Security Parameters must be protected by some form of integrity protection and all Secret Authenticator 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).

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.

L3 GlobalPlatform: At L3 GlobalPlatform, 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.

L3: At L3, ALC_DVS.1 (see [CC3V3-1R5]) MUST be applied.

L3+: At L3+, ALC_DVS.2 (see [CC3V3-1R5]) MUST be applied.

(SM-28)

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements. Please provide explicit documentation references.

L3 Vendor Questionnaire

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

- Development Security Life-Cycle Support
- Mapping to Companion Program Requirements

L3+ Vendor Questionnaire

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

- Development Security Life-Cycle Support
- Mapping to Companion Program Requirements

L1+ Test Procedure

{A2} The tester SHALL ***verify*** that the documentation meets 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 GlobalPlatform Test Procedure

The Tester SHALL ***verify*** that the provided rationale and documentation 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; Consumer + Enterprise; 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 Companion Program

L3 GlobalPlatform: AROE configuration management documentation MUST be provided to support this requirement.

This requirement is linked to the ALC_CMC.2 and ALC_CMS.2 (see [TEE-PP]).

L3 Common Criteria: A Configuration Management Scope and Capabilities documentation MUST be provided (see [CC1V3-1R5]).

This requirement is linked to 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 linked to 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 .

L1: At L1+, the use of a revision control system SHALL only be proven for the Authenticator Application .

L2: No calibration required.

L3 GlobalPlatform: No calibration required.

L3: No calibration required.

L3+: No calibration required.

9.4	**L1 Vendor Questionnaire** ***Provide*** the Security Secretariat with a rationale of how the requirement above is met. **L1+ Vendor Questionnaire** ***Provide*** the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design). **L2 Vendor Questionnaire** ***Describe*** how this requirement can be verified through documentation review. Please provide explicit design documentation references. **L3 GlobalPlatform Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements. Please provide explicit documentation references. **L3 Vendor Questionnaire** TProvide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Development Security Life-Cycle Support • Mapping to Companion Program Requirements **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements, including the following supporting documents: • Development Security Life-Cycle Support • Mapping to Companion 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. **L1+ Test Procedure** {A2} The tester SHALL ***verify*** that the documentation meets 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 GlobalPlatform Test Procedure** The Tester SHALL ***verify*** that the provided rationale and documentation meet the requirement.	(SM-28)

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; Consumer + Enterprise; TVFR; L1 and higher

Each version of each configuration item that comprises the Authenticator and associated documentation SHALL be assigned a unique identification.

Relation to Companion Program

L3 GlobalPlatform: AROE configuration management documentation MUST be provided to support this requirement.

This requirement is linked to the ALC_CMC.2 and ALC_CMS.2 (see [TEE-PP]).

L3 Common Criteria: A Configuration Management Scope and Capabilities documentation MUST be provided (see [CC1V3-1R5]).

This requirement is linked to 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 linked to ALC_CMC.4 and ALC_CMS.1 (see [CC3V3-1R5]).

Calibration

L1: At L1, the configuration items comprising the Authenticator Application are relevant.

L1+: At L1+, the configuration items comprising the Authenticator Application are relevant.

L2: No calibration required.

L3 GlobalPlatform: No calibration required.

L3: No calibration required.

L3+: No calibration required.

9.5

L1 Vendor Questionnaire

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

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

(SM-28)

L3 GlobalPlatform Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements. Please provide explicit documentation references.

L3 Vendor Questionnaire

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

- Development Security Life-Cycle Support
- Mapping to Companion Program Requirements

L3+ Vendor Questionnaire

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

- Development Security Life-Cycle Support
- Mapping to Companion Program Requirements

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and documentation 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; Consumer + Enterprise; TVFR; L1+ 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 Companion Program

L3 GlobalPlatform: Not applicable to the AROE.

L3 Common Criteria: A Development Security Life-Cycle Support documentation MUST be provided (see [CC1V3-1R5]).

This requirement is fulfilled 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 fulfilled by ALC_DVS.2 (see [CC3V3-1R5]).

Calibration

L1+: At L1+, 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.

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 GlobalPlatform: At L3 GlobalPlatform, 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

L1+ Vendor Questionnaire

Provide the tester with a rationale of how the implementation meets the requirements, including Development Information (High level design).

L2 Vendor Questionnaire

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

L3 GlobalPlatform Vendor Questionnaire

Provide the tester with a rationale for how the implementation meets the requirements. Please provide explicit documentation references.

L3 Vendor Questionnaire

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

- Development Security Life-Cycle Support
- Mapping to Companion Program Requirements

L3+ Vendor Questionnaire

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

- Development Security Life-Cycle Support
- Mapping to Companion Program Requirements

L1+ Test Procedure

(SM-28)

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and documentation 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

3.10 Operational Guidance

No.	Requirement	Security Measures
	FIDO2; Enterprise; TVFR; L1 and higher	
	If the Authenticator supports Enterprise Attestation, it MUST be sold to an Enterprise for use with its employees, contracters or defined members. It MUST NOT be used with the customers of the Enterprise. It MUST NOT be sold to end-users on the open market. **Relation to Companion Program** **L3 GlobalPlatform**: Not applicable to the AROE. **L3 Common Criteria**: Not Applicable. **L3+ Common Criteria**: Not Applicable.	

10.1	**Calibration** **L1**: No calibration required. **L1+**: No callibration required. **L2**: No calibration required. **L3 GlobalPlatform**: 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 a rationale of how the requirement above is met. **L1+ Vendor Questionnaire** Is this requirement applicable to the Authenticator? If **No**, then *describe* why. If Yes, *provide* the tester with a rationale of how the implementation meets the requirements. **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. **L3 GlobalPlatform Vendor Questionnaire** Describe how this requirement can be verified through documentation review. **L3 Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements. **L3+ Vendor Questionnaire** Provide the tester with a rationale for how the implementation meets the requirements.	(SM-28)

L1 Test Procedure

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

L1+ Test Procedure

{A2} The tester SHALL *verify* that the documentation meets 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 GlobalPlatform Test Procedure

The Tester SHALL *verify* that the provided rationale and evidence 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

A. Differences between versions

Differences between FIDO 1.4 and 1.5 security certification requirements

The L1+ security level is added

This allows software-protected authenticators using security mechanisms described in ETSI TR 103 642 to get certified.

Differences between FIDO 1.3 and 1.4 security certification requirements

The GlobalPlatform Companion Program is added

This allows authenticators using GP-certified TEE's to get speedier certification.

This is slotted in at L3, so there are now two paths to get L3 certification. A vendor must pick one and stick to it.

The HW Examples Table is Updated

This table now gives very specific examples rather than describing classes or groups of hardware. These are only examples. Vendor's HW is likely to be different and must be specifically evaluated. The examples table is not a short cut or used in certification.

Major Clarification for User Verification

Requirements 3.1, 3.2, 3.4 and 3.7 are updated and 3.11 is added.

How an authenticator indicates it supports user presence and user verification is better specified and described. This is for indication in the metadata, in the response to the server and in the user verification method extension.

Timeouts when changing the PIN, enrolling more fingerprints and such are more clearly specified.

L2 Calibration was added for requirement 3.7 to day that trusted path must be implemented inside the AROE.

Some of the user verification requirements are now completely verified at interop test. Documentation is not required.

Allow clientPIN and smartphone lock screen PIN at L2

Requirements 3.2, 3.7 and 3.8 are updated and 3.11 is added.

At L2 and higher authenticators that implement multiple user verification methods must support the user verification method extension.

External PIN, password and pattern authenticators are allowed for L2 and above certification. Authenticators that do this must explicitly indicate this in metadata and the user verification method extension. New authentication "_EXTERNAL" methods are defined in the FIDO registry for this. This allows L2 certification of FIDO2 clientPIN and authenticators making use of smart phone lock screen PINs.

There is a clear requirement that no new user verification methods or templates are added for an authenticator without a user verification from existing templates or methods. For example, the user must successfully enter a PIN or pass fingerprint verification to add a new finger for an authenticator that support PIN and fingerprint.

Privacy Requirements Partially Restored

Requirements 3.5 and 3.6, which are UAF-only, are restored and give strong privacy.

Requirement 4.6 was added. It is FIDO2 only. It gives the calibrated per security level requirements for implementation of the FIDO 2 privacy extension.

Clarification on sharing identical attestation key in 100,000 devices…

No change in concept. Just clarification on how attestation keys should be shared with 100,000 devices.

Induced Fault Clarification

L3 and L3+ calibration was removed for requirement 8.4 as it was unnecessary

Minor Level Naming Fix

Some leftover references to L4 and L5 were corrected.

Minor Correlation Handle Definition Fix

Correlation Handle was defined twice.

Version Number Corrections

Some of the version older numbers in cross references in the document set were wrong.

Partner Program Renamed

"Partner Program" is renamed to "Companion Program".

External References Corrections

Many of the external references had broken links and other issues. They have been corrected.

Enterprise Attestation

The Enterprise and Consumer profiles were added and defined.

The Enterprise Attestation feature was restricted to the Enterprise profile

The Enterprise profile requirements were adjusted for Enterprise Attestation

Differences between FIDO 1.4 and 1.5 security certification requirements

B. Old version of Table 2.2

This section is non-normative.

The objective of this table, "Examples of underlying platforms and physical attacks", was to describe various implementations of an Authenticator, and the potential certification level they can target, to help the reader decide which security level certification he could apply for the Authenticator. To this effect, there were two columns describing examples and corresponding certification level. However, the table was also describing ratings for the different implementations, based on JIL Rating (smart card type evaluation) or TEE rating (TEE type evaluation). These ratings apply to different evaluation schemes and cannot be compared.

CC rating and evaluation methodology (CEM, [CEMV3-1R5]) is generic and thus adapted to all types of products. This was the basis of the other evaluation methodologies below, but there are significant differences in the approaches leading to not comparable rating scores (split of identification and exploitation, different criteria, different weights for criteria, etc.):

- JIL rating and evaluation methodology are adapted to smart cards [AttackPotentialSmartcards].
- TEE rating and evaluation methodology are adapted to TEE [TEE-EM].
- FIDO L1+ rating and evaluation methodology are adapted to SW-only products [L1plus-Eval].

Comparatively, the evaluations against CC Protection Profiles done by Microsoft (for laptops, e.g. https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-platform-common-criteria) and Google (for mobile devices, e.g. https://www.niap-ccevs.org/Product/Compliant.cfm?PID=10941) to rate their products are relying on the generic CEM methodology and the conformance claimed for vulnerability is AVA_VAN.1.

The JIL methodology is not suited for TEE products, the TEE methodology is not suited for smart cards products, and neither JIL nor GP TEE evaluation methodologies are suited for laptops and for mobile devices. It is therefore inadequate to present in the table multiple ratings for the same products. Each methodology answer the needs and objectives of the relevant stakeholders and are specified, and maintained, by the industry actors, which are deeply experimented in the evaluation of their products (RETEX). In addition, the table may erroneously suggest the proposed implementation examples can be certified at highest assurance level while no details on the implementation are given: what is the authenticator boundary, how is authenticator logically protected on that implementation etc. In fact, the examples given could be rated at 30, but could also be rated at 15 or 20, this will highly depend on the implementation, and the type of attacks it defends. As such, it is not because a given implementation has some resistance to physical attacks (directly on the die or memories as suggested in examples) that the product will succeed the certification: a security certification shall consider all the possible attack paths and must conclude there is no attack path below a defined threshold defined specifically in each evaluation method: the “absolute” rating, meaning the product is “resistant against attacker with potential X” can only be given through an evaluation/certification, where all attack paths are examined.

This is why the following table, kept here for history, has been replaced in the core document.

Case#	Examples	Common-Criteria CC Companion Program Smart Card (JIL Rating)	GlobalPlatform GP Companion Program (TEE Rating)	Typical FIDO Certification Level
AA	Mobile phone with HW key store	NA	NA	L1
A	IoT device 100MHz 32-bit CPU accessing DIMM socket memory. Low speed memory socket interface	7	10	L2
B	Laptop with high performance 2GHz CPU accessing DDR4 memory in a SO-DIMM. High speed memory socket interface	18	20	L2..L3
C	Laptop with high performance 2GHz CPU accessing DDR4 memory in a SO-DIMM with buried trace	18	21	L2..L3
D	Mobile phone SoC with 2GHz CPU with PoP memory	20	23	L2..L3
E	Mobile phone SoC with 2GHz CPU with memory and CPU die in the same package	23	26	L3
F	IoT device 32-bit 100MHz CPU with memory and CPU on the same die	27	30	L3+
G	SoC with CPU with strong inline memory encryption and integrity protection HW	33	34	L3+
H	Smart Card or Secure Element. Memory and CPU on the same die with hardware countermeasures	33	34	L3+

C. References

C.1 Normative references

[AttackPotentialSmartcards]
Application of Attack Potential to Smartcards. January 2019. URL: https://www.sogis.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v3-0.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

[FIDOAllowedCrypto]
Dr. Joshua E. Hill; Douglas Biggs. *FIDO Authenticator Allowed Cryptography List*. URL: https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-allowed-cryptography-list-v1.4-fd-20211102.html

[FIDOBiometricsRequirements]
Stephanie Schuckers; Greg Cannon; Elham Tabassi; Meagan Karlsson; Elaine Newton. *FIDO Biometrics Requirements*. October 2020. URL: https://fidoalliance.org/specs/biometric/requirements/Biometrics-Requirements-v2.0-fd-20201006.html

[FIDOCTAP]
C. Brand; A. Czeskis; J. Ehrensvärd; M. Jones; A. Kumar; R. Lindemann; A. Powers; J. Verrept. *FIDO 2.0: Client To Authenticator Protocol*. 30 January 2019. URL: https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html

[FIDOEcdaaAlgorithm]
R. Lindemann; J. Camenisch; M. Drijvers; A. Edgington; A. Lehmann; R. Urian. *FIDO ECDAA Algorithm*. 25 May 2021. Review Draft. URL: https://fidoalliance.org/specs/common-specs/fido-ecdaa-algorithm-v2.1-rd-20210525.html

[FIDOGlossary]
R. Lindemann; D. Baghdasaryan; B. Hill; J. Hodges; J. Verrept. *FIDO Technical Glossary*. 25 May 2021. Review Draft. URL: https://fidoalliance.org/specs/common-specs/fido-glossary-v2.1-rd-20210525.html

[FIDOMetadataRequirements]
Meagan Karlsson. *FIDO Authenticator Metadata Requirements*. URL: https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-metadata-requirements-v1.2-fd-20201102.html

[FIDOMetadataStatement]
B. Jack; R. Lindemann; Y. Ackermann. *FIDO Metadata Statements*. 18 May 2021. Proposed Standard. URL: https://fidoalliance.org/specs/mds/fido-metadata-statement-v3.0-ps-20210518.html

[FIDORegistry]
R. Lindemann; D. Baghdasaryan; B. Hill. *FIDO Registry of Predefined Values*. 25 May 2021. Review Draft. URL: https://fidoalliance.org/specs/common-specs/fido-registry-v2.2-rd-20210525.html

[FIDORestrictedOperatingEnv]
Laurence Lundblade; Meagan Karlsson. *FIDO Authenticator Allowed Restricted Operating Environments List*. URL: https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-allowed-restricted-operating-environments-list-v1.3-fd-20211102.html

[FIDOSecRef]
R. Lindemann; D. Baghdasaryan; B. Hill; J. Hill; D. Biggs. *FIDO Security Reference*. 25 May 2021. Review Draft. URL: https://fidoalliance.org/specs/common-

specs/fido-security-ref-v2.1-rd-20210525.html

[ISOIEC-18045]
Information technology -- Security techniques -- Methodology for IT security evaluation. August 2008. URL: https://www.iso.org/standard/46412.html

[JCPP]
. *Java Card Protection Profile - Open Configuration*. May 2012. URL: https://www.commoncriteriaportal.org/files/ppfiles/ANSSI-CC-profil_PP-2010-03en.pdf

[L1plus-Eval]
TBD. *Application of attack potential to FIDO L1+ (AAP)*. May 2019. URL: https://members.fidoalliance.org/wg/SPWG/document/10636

[PP0084]
. *BSI-CC-PP-0084-2014 Security IC Platform Protection Profile with Augmentation Packages*. URL: https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf

[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

[TEE-EM]
GlobalPlatform. *GPD_GUI_044 TEE Evaluation Methodology*. Most recent version applies. Available only to GlobalPlatform members. URL:

[TEE-PP]
. *GPD_SPE_021 TEE Protection Profile version 1.3*. September 2020. URL: https://globalplatform.org/specs-library/tee-protection-profile-v1-3/

[U2FImplCons]
D. Balfanz. *FIDO U2F Implementation Considerations v1.0*. Proposed Standard. 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; J. Ehrensvard; J. Lang. *FIDO U2F Raw Message Formats v1.2*. 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; J. Hodges; K. Yang. *FIDO UAF Authenticator Commands*. Proposed Standard. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-ps-20201020/fido-uaf-authnr-cmds-v1.2-ps-20201020.html

[UAFAuthnrMetadata]
B. Hill; D. Baghdasaryan; J. Kemp. *FIDO UAF Authenticator Metadata Statements*. Proposed Standard. URL: https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-metadata-statement-v2.0-id-20180227.html

[UAFProtocol]
R. Lindemann; D. Baghdasaryan; E. Tiffany; D. Balfanz; B. Hill; J. Hodges; K. Yang. *FIDO UAF Protocol Specification v1.2*. Proposed Standard. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-ps-20201020/fido-uaf-protocol-v1.2-ps-20201020.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-ps-20201020/fido-uaf-reg-v1.2-ps-20201020.html

[WebAuthn]
Dirk Balfanz (Google); Alexei Czeskis (Google); Jeff Hodges (Google); J.C. Jones (Mozilla); Michael B. Jones (Microsoft); Akshay Kumar (Microsoft); Rolf Lindemann (Nok Nok Labs); Emil Lundberg (Yubico); Vijay Bharadwaj (Microsoft); Arnar Birgisson (Google); Hubert Le Van Gong (PayPal); Angelo Liao (Microsoft); John Bradley (Yubico); Christiaan Brand (Google); Adam Langley (Google); Giridhar Mandyam (Qualcomm); Nina Satragno (Google); Nick Steele (Gemini); Jiewen Tan (Apple); Shane Weeden (IBM); Mike West (Google); Jeffrey Yasskin (Google). *Web Authentication: An API for accessing Public Key Credentials Level 2*. 8 April 2021. TR. URL: https://www.w3.org/TR/webauthn-2/

C.2 Informative references

[AES-Proposal]
Joan Daemen; Vincent Rijmen. *AES Proposal: Rijindael*. March 1999. URL: https://cs.ru.nl/~joan/papers/JDA_VRI_Rijndael_V2_1999.pdf

[CYBER]
ETSI TR 103 642 CYBER; Security techniques for protecting software in a white box model. October 2018. URL: https://www.etsi.org/deliver/etsi_tr/103600_103699/103642/01.01.01_60/tr_103642v010101p.pdf

[FIDO-SR-Mapping-Table]
R. Atoui; J. Hill. *FIDO Security Requirements Partner Program Mapping Table*. Working Draft. URL: https://fidoalliance.org/specs/fido-security-requirements/FIDO%20SRs%20L3-L3+%20Companion%20Program%20Mapping%20Table_20200824_RELEASE.xlsx

[FIDOAuthenticatorCertificationPolicy]
Rae Rivera; Roland Atoui; Beatrice Peirani. *FIDO Certification Program - Policy Authenticator Certification*. September 2020. URL: https://media.fidoalliance.org/wp-content/uploads/2020/12/FIDO-Authenticator_Certification_Program_policy_v1.3_FINAL_September2020.pdf

[FIDOLabPolicy]
CWG. *FIDO Certification Program - Security Laboratory Accreditation Policy*. May 2017. Published. URL: https://media.fidoalliance.org/wp-content/uploads/SecurityLaboratoryAccreditationPolicy_v1.1_20170526.pdf

[FIDOMetadataService]
B. Jack; R. Lindemann; Y. Ackermann. *FIDO Metadata Service*. 18 May 2021. Proposed Standard. URL: https://fidoalliance.org/specs/mds/fido-metadata-service-v3.0-ps-20210518.html

[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