



# FIDO Authenticator Security Requirements

FIDO Alliance 05 October 2017

**This version:**

<https://fidoalliance.org/specs/fido-uaf-v1.0-fd-20171005/fido-authnr-sec-reqs-v1.0-fd-20171005.html>

**Previous version:**

<http://fidoalliance.org/specs/fido-authenticator-security-requirements-v1.0-ps-20141208.html>

**Editor:**

[Rolf Lindemann](#), [Nok Nok Labs, Inc.](#)

**Contributors:**

[Dr. Joshua E. Hill](#), [InfoGard Laboratories](#)  
[Douglas Biggs](#), [InfoGard Laboratories](#)

Copyright © 2013-2017 [FIDO Alliance](#) All Rights Reserved.

---

## Abstract

This document defines the security requirements for FIDO Authenticators.

## Status of This Document

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

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

Implementation of certain elements of this Document may require licenses under third party intellectual property rights, including without limitation, patent rights. The FIDO Alliance, Inc. and its

Members and any other contributors to this Document are not, and shall not be held, responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.

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

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

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

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

## Table of Contents

- 1. [Notation](#)
  - 1.1 [Version](#)
  - 1.2 [Key Words](#)
  - 1.3 [Security Levels](#)
  - 1.4 [FIDO Specifications](#)
  - 1.5 [Security Measures](#)
  - 1.6 [Testing Style](#)
    - 1.6.1 [Test Assurance Modes](#)
- 2. [Requirements](#)
  - 2.1 [Authenticator Definition and Derived Authenticator Requirements](#)
  - 2.2 [Key Management and Authenticator Security Parameters](#)
    - 2.2.1 [Documentation](#)
    - 2.2.2 [Random Number Generation](#)
    - 2.2.3 [Signature Counters](#)
  - 2.3 [Authenticator’s Test for User Presence and User Verification](#)
  - 2.4 [Privacy](#)
  - 2.5 [Physical Security, Side Channel Attack Resistance and Fault Injection Resistance](#)
  - 2.6 [Attestation](#)
  - 2.7 [Operating Environment](#)
  - 2.8 [Self-Tests and Firmware Updates](#)
  - 2.9 [Manufacturing and Development](#)
- A. [References](#)
  - A.1 [Normative references](#)
  - A.2 [Informative references](#)

## 1. Notation

## 1.1 Version

This Document version (DV) is DV 1.0.2.

	L1	L2	L3	L4	L5
Security Requirements version (RV)	RV 1.0.1	RV 1.0.1	-	-	-
Vendor Questionnaire version (QV)	QV 1.0.1	QV 1.0.0	-	-	-
Test Procedures version (PV)	PV 1.0.1	PV 1.0.0	-	-	-

Table 1: Versions represented by this document

## 1.2 Key Words

The key words “**MUST**”, “**MUST NOT**”, “**REQUIRED**”, “**SHALL**”, “**SHALL NOT**”, “**SHOULD**”, “**SHOULD NOT**”, “**RECOMMENDED**”, “**MAY**”, and “**OPTIONAL**” in this document are to be interpreted as described in [\[RFC2119\]](#).

## 1.3 Security Levels

All requirements apply at all levels unless otherwise noted. Requirements marked with L3+, L4+, or L5+ are intended to be requirements that apply only to higher level Authenticators, not FIDO Authenticators certified to Level 1 or Level 2. They are present only for the reader’s reference.

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

## 1.4 FIDO Specifications

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

For requirements that relate to normative requirements of the UAF or U2F 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.

## 1.5 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 “(SM2)”. The security measure references are described in the the FIDO Security Reference document [\[FIDOSecRef\]](#).

## 1.6 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.

### 1.6.1 Test Assurance Modes

Because GaVR and TVFR relate to functional requirements, there are different modes of test assurance 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).

## 2. Requirements

### 2.1 Authenticator Definition and Derived Authenticator Requirements

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

We use the term **Authenticator Application** to refer to the entity that (a) is provided by the Authenticator vendor and (b) combines with the underlying **operating environment** (hardware and firmware) in a way that results in a FIDO Authenticator. This operating environment might be clearly separated from a high-level operating system (HLOS). In this case we call it "**Restricted Operating**

**Environment" (ROE).** If such separation meets the requirements defined in [FIDORestrictedOperatingEnv], we call it **Allowed Restricted Operating Environment (AROE).**

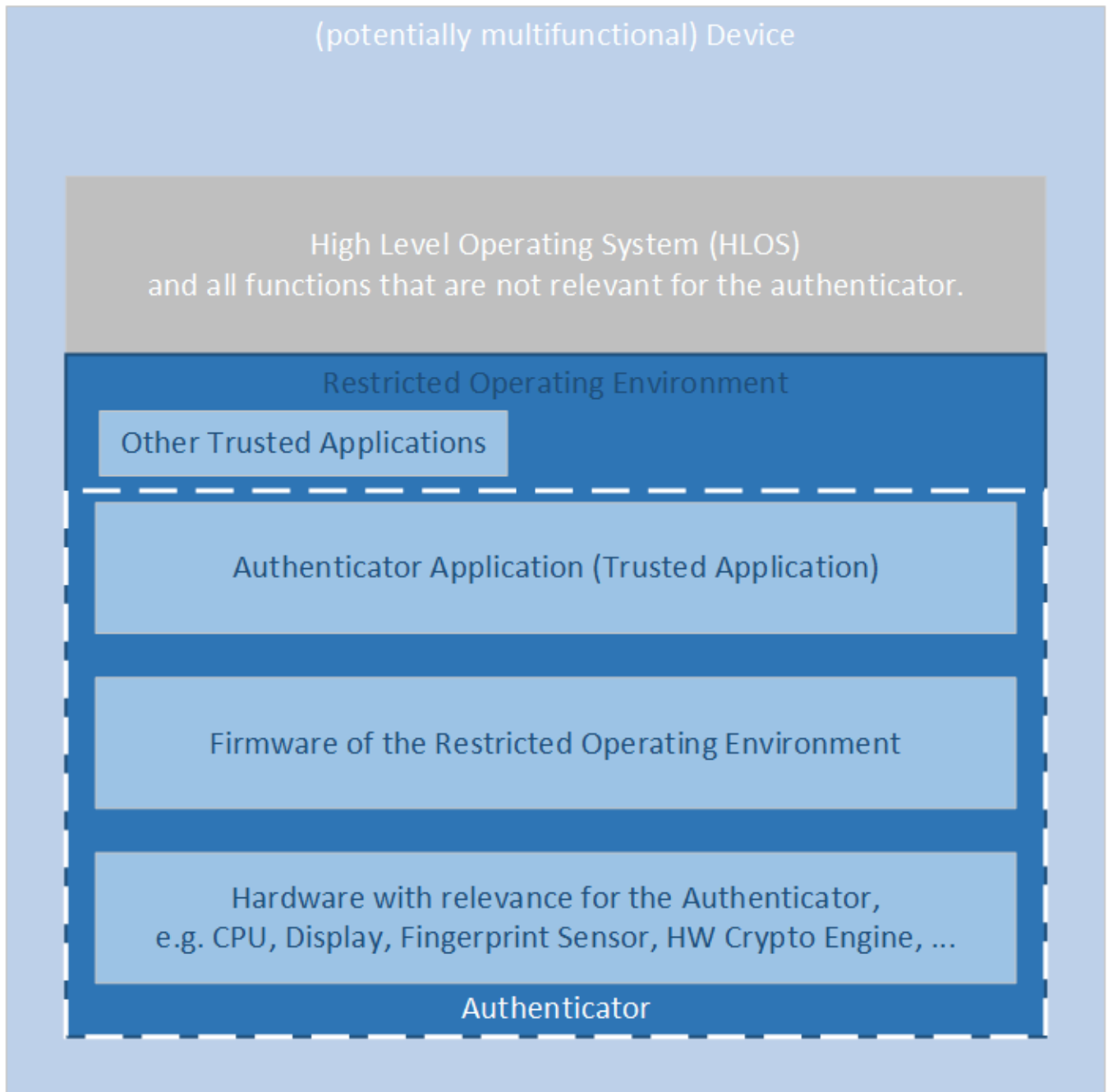


Fig. 1 Restricted Operating Environments Architectural Overview

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

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

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

NOTE

For the certification levels L1 and L2 the Authenticator doesn't need to restrict the private authentication key (Uauth.priv) to signing valid FIDO messages only (see requirement 2.1.15 being labeled L3+). As a consequence, the generation of the to-be-signed object could be performed outside of the Authenticator.

**NOTE**

Use the buttons below and within the requirement boxes to toggle the different elements of this document.

- **VQ** will show and hide Vendor Questionnaire boxes.
- **TP** will show and hide Test Procedure boxes.
- **L1-L5** will show and hide boxes for the Level selected.

When used inside a Requirement the buttons will show and hide for that Requirement only.

VQ TP L1 L2 L3 L4 L5

No.	Requirement	Security Measures
1.1	<p>UAF + U2F; DaD; L1+</p> <p>The vendor shall document an explicit <b>Authenticator boundary</b>. 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.</p> <p>The <u>Authenticator boundary</u> as defined by FIDO is comprised of the hardware and software where the Authenticator runs. The <u>Authenticator Application</u> 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.</p> <p>For L1 the vendor shall also describe what portions of functionality the Authenticator uses from any underlying <u>operating environment</u> that belongs to the Authenticator but that is not included in the <u>Authenticator Application</u>.</p> <p><b>NOTE</b> At L1, the Authenticator typically belongs to one of the 4 categories:</p> <ol style="list-style-type: none"> <li>1. <u>Authenticator Application</u> running on some HLOS <i>without</i> an effective protection of the <u>Authenticator Security Parameters</u> against most other applications running in the same environment.</li> <li>2. <u>Authenticator Application</u> running on some HLOS <i>with</i> an effective protection of the <u>Authenticator Security Parameters</u> against most</li> </ol>	(SM-1, SM-9, SM-26)

No.		Security Measures
	<p>other applications running in the same environment - without breaking the HLOS.</p> <ol style="list-style-type: none"> <li>3. as #2, but having the <u>Secret Authenticator Security Parameters</u> protected by an <u>AROE</u></li> <li>4. entire Authenticator is implemented in an <u>AROE</u> (i.e. typically qualifying for L2+)</li> </ol> <p>At L1, the Authenticator vendor shall declare and describe to which of the above mentioned categories the <u>Authenticator Application</u> belongs.</p> <p><b>NOTE</b></p> <p>The documentation provided by the vendor should cover software attack protection and, if required, hardware attack protection.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> the tester with documentation that specifies how the requirement above is met.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div style="display: flex; gap: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	
1.2	UAF + U2F; DaD; L1+	

No.	Requirement	Security Measures
	<p>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.</p> <p>At L1, the vendor shall mark the FIDO Relevant security and cryptographic functions implemented in the Authenticator but implemented <i>outside the Authenticator Application</i> (i.e. in the underlying OS or HW).</p> <p><b>NOTE</b></p> <p>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.</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> the tester with documentation that specifies how the requirement above is met.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div style="display: flex; gap: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	<p>(SM-1, SM-9, SM-16, SM-26)</p>
<p><b>1.3</b></p>	<p>UAF + U2F; DaD; L1+</p>	



No.	Requirement	Security Measures
	<p>The vendor shall document where Authenticator User Private Keys (Uauth.priv) are stored, the structure of all KeyIDs and Key Handles used by the Authenticator, and explain how these private keys are related to the KeyIDs and Key Handles used by the Authenticator.</p> <p>At L1, the private keys, KeyIDs etc. that are generated outside the <u>Authenticator Application</u> shall be documented, but their internal structure does not need to be explained in detail.</p> <div data-bbox="248 472 1325 625" style="border: 1px solid orange; padding: 5px; margin-bottom: 10px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="248 655 1325 808" style="border: 1px solid orange; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> the tester with documentation that specifies how the requirement above is met.</p> </div> <div data-bbox="248 840 1325 961" style="border: 1px solid blue; padding: 5px; margin-bottom: 10px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="248 993 1325 1083" style="border: 1px solid blue; padding: 5px; margin-bottom: 10px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div data-bbox="248 1087 672 1123" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-1, SM-6, SM-26)</p>
<p><b>1.4</b></p>	<p>UAF; DaD; L1+</p>	

No.	Requirement	Security Measures
	<p>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".</p> <div data-bbox="248 338 1325 590" style="border: 1px solid #ccc; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> <p>At L1, this requirement must be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.</p> </div> <div data-bbox="248 621 1325 747" style="border: 1px solid #ccc; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> the tester with documentation that specifies how the requirement above is met.</p> </div> <div data-bbox="248 779 1325 905" style="border: 1px solid #ccc; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A0} The Security Secretariat shall <i>verify</i> the requirement during Interoperability Testing.</p> </div> <div data-bbox="248 936 1325 1020" style="border: 1px solid #ccc; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div data-bbox="248 1020 672 1062" style="border: 1px solid #ccc; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-26)
1.5	UAF; TVFR; L1+	

No.	Requirement	Security Measures
	<p>If the Authenticator is a second-factor Authenticator, then the Authenticator shall not store user names inside a Raw Key Handle [UAFAuthnrCommands], [Section 5.1]. A cryptographically wrapped Raw Key Handle is called Key Handle.</p> <div data-bbox="248 338 1325 575" style="border: 1px solid orange; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p>Is this requirement applicable to the Authenticator? If <b>No</b>, then <i>describe</i> why.</p> <p>If Yes, <i>Provide</i> the Security Secretariat with a description of how the requirement above is met.</p> </div> <div data-bbox="248 611 1325 816" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p>Is this requirement applicable to the Authenticator? If <b>No</b>, then <i>describe</i> why.</p> <p>If Yes, <i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="248 852 1325 972" style="border: 1px solid blue; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="248 1008 1325 1127" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="248 1127 670 1167" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-23)
1.6	UAF; TVFR; L1+	

No.	Requirement	Security Measures
	<p>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]</p> <div data-bbox="248 304 1325 457" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="248 489 1325 642" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="248 674 1325 795" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="248 827 1325 949" style="border: 1px solid #ccc; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="248 1024 672 1066" style="margin-top: 20px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-16)
1.7	UAF; TVFR; L1+	

No.	Requirement	Security Measures
	<p>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, the Authenticator shall use an Allowed Hashing or Data Authentication Cryptographic Function to mix the ASM-provided KHAccessToken and AppID.</p> <p>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 relies on the underlying HLOS platform to work as expected.</p> <div data-bbox="248 611 1325 762" style="border: 1px solid orange; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="248 793 1325 919" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="248 951 1325 1077" style="border: 1px solid blue; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="248 1108 1325 1234" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="248 1234 670 1266" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-16)
1.8	UAF; TVFR; L1+	

No.	Requirement	Security Measures
	<p>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]</p> <div data-bbox="248 304 1325 457" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="248 489 1325 642" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="248 674 1325 795" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="248 827 1325 865" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Test Procedure</p> </div> <div data-bbox="248 930 1325 1014" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="248 1018 672 1056" style="border: 1px solid #ccc; padding: 5px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-13)
1.9	UAF; TVFR; L1+	

No.	Requirement	Security Measures
	<p>If the Authenticator supports Transaction Confirmation Display, then it shall display the transaction content supplied in the “Sign” command. [UAFAuthnrCommands], [Section 6.3.4] and [FIDOGlossary].</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> <p>At L1, this requirement must be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p>Is this requirement applicable to the Authenticator? If <b>No</b>, then <i>describe</i> why.</p> <p>If <b>Yes</b>, <i>describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Test Procedure</p> <p>{A0} The Security Secretariat shall <i>verify</i> the requirement during Interoperability Testing.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div style="display: flex; gap: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-10)
1.10	UAF + U2F; GaVR-3; L1+	

No.	Requirement	Security Measures
	<p>Authenticators shall validate all data input to the Authenticator to defend against buffer overruns, stack overflows, integer under/overflow or other such invalid input-based attack vectors.</p> <p>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.</p> <div data-bbox="248 436 1325 590" style="border: 1px solid orange; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="248 621 1325 863" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale that the Authenticator validates all data input to the Authenticator.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator’s design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div data-bbox="248 894 1325 1020" style="border: 1px solid blue; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="248 1052 1325 1205" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div data-bbox="248 1205 670 1247" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-28)
1.11	<p>UAF; DaD; L3+</p> <p>If the Authenticator has a Transaction Confirmation Display, the AppID shall be displayed to the user when a “Register”, “Sign”, or “Deregister” command is received.</p> <div data-bbox="248 1457 1325 1583" style="border: 1px solid orange; padding: 5px;"> <p>L3 Vendor Questionnaire</p> <p><i>Provide</i> the tester with documentation that specifies how the requirement above is met.</p> </div> <div data-bbox="248 1614 1325 1703" style="border: 1px solid blue; padding: 5px;"> <p>L3 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div data-bbox="248 1703 670 1745" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-10)

## 2.2 Key Management and Authenticator Security Parameters

### 2.2.1 Documentation



No.	Requirement	Security Measures
2.1.1	<p>UAF + U2F; DaD; L1+</p> <p>The vendor shall document all <b>Authenticator Security Parameters</b> (ASPs). Data parameters used by or stored within the Authenticator which are FIDO Relevant are called <b>Authenticator Security Parameter</b>. These shall, at minimum, include all FIDO user verification reference data, FIDO biometric data, Key Handle Access Tokens, User Verification Tokens, signature or registration operation counters, FIDO Relevant cryptographic keys, and FIDO relevant Allowed Random Number Generator state data. Biometric data is defined as raw captures off the sensor, stored templates, candidate match templates, and any intermediate forms of biometric data. Biometric data not used with FIDO is excluded.</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> the tester with documentation that specifies how the requirement above is met.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div style="display: flex; gap: 5px;"> <div style="border: 1px solid gray; padding: 2px;">VQ</div> <div style="border: 1px solid gray; padding: 2px;">TP</div> <div style="border: 1px solid gray; padding: 2px;">L1</div> <div style="border: 1px solid gray; padding: 2px;">L2</div> <div style="border: 1px solid gray; padding: 2px;">L3</div> <div style="border: 1px solid gray; padding: 2px;">L4</div> <div style="border: 1px solid gray; padding: 2px;">L5</div> </div>	<p>(SM-1, SM-2, SM-6, SM-13, SM-15, SM-16, SM-26)</p>
2.1.2	<p>UAF + U2F; DaD; L1+</p>	

No.	Requirement	Security Measures
	<p>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 “<b>Secret Authenticator Security Parameters</b>”; 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.</p> <p>At L1, the vendor shall describe the reliance of the <u>Authenticator Application</u> on the underlying operating environment for those <u>Authenticator Security Parameters</u> which are not fully maintained in the <u>Authenticator Application</u>.</p> <div data-bbox="272 783 1325 936" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="272 1003 1325 1125" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> the tester with documentation that specifies how the requirement above is met.</p> </div> <div data-bbox="272 1157 1325 1281" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="272 1312 1325 1398" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div data-bbox="272 1402 695 1440" style="border: 1px solid #ccc; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-1, SM-2, SM-6, SM-13, SM-15, SM-16, SM-26)</p>
<p><b>2.1.3</b></p>	<p>UAF + U2F; DaD; L1+</p>	

No.	Requirement	Security Measures
	<p>For each Authenticator Security Parameter that is a cryptographic key that is generated, used, or stored within the Authenticator, the vendor shall document how this key is generated, whether the key is unique to a particular Authenticator or shared between multiple Authenticators, and the key's claimed cryptographic strength. This claimed cryptographic strength shall not be larger than the maximal allowed claimed cryptographic strength for the underlying algorithm, as specified in the "Allowed Cryptography List" [FIDOAllowedCrypto]. If the key is used with an algorithm not listed on the "Allowed Cryptography List" [FIDOAllowedCrypto], then the claimed cryptographic strength for this key shall be zero.</p> <p>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.</p> <p>If a cryptographic key is generated using an RNG with an unknown cryptographic strength, the cryptographic strength of that key is unknown.</p> <p><b>NOTE</b></p> <p>This requirement interacts with requirement 5.4 as the cryptographic strength of a key might get degraded - depending on potential side channel attacks - slightly each time the key is used.</p> <div data-bbox="272 1087 1328 1241" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="272 1272 1328 1394" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> the tester with documentation that specifies how the requirement above is met.</p> </div> <div data-bbox="272 1425 1328 1518" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div data-bbox="272 1549 1328 1642" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div data-bbox="272 1642 695 1675" style="border: 1px solid #ccc; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-1, SM-2, SM-6, SM-13, SM-16, SM-26)</p>
<p><b>2.1.4</b></p>	<p>UAF + U2F; DaD; L1+</p>	

No.	Requirement	Security Measures
	<p>The vendor shall document the Authenticator's <b>Overall Claimed Cryptographic Strength</b>; the Overall Authenticator Claimed Cryptographic Strength shall be less than or equal to the claimed cryptographic strength of all the <u>Authenticator Security Parameters</u> that are cryptographic keys.</p> <p>At L2+, the Authenticator's Overall Claimed Cryptographic Strength shall at least be greater than or equal to 100 bits and it should be greater than or equal to 112 bits.</p> <p>At L1, if the security strength for the RNG is not known, an unknown Overall Claimed Cryptographic Strength shall be assumed - which is allowed at L1.</p> <div data-bbox="272 646 1328 804" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="272 835 1328 957" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> the tester with documentation that specifies how the requirement above is met.</p> </div> <div data-bbox="272 989 1328 1110" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="272 1142 1328 1230" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div data-bbox="272 1234 695 1272" style="border: 1px solid #ccc; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-1, SM-16, SM-26)</p>
<p><b>2.1.5</b></p>	<p>UAF + U2F; GaVR-3; L1+</p>	

No.	Requirement	Security Measures
	<p>All Authenticator Security Parameters within the Authenticator shall be protected against modification and substitution.</p> <p>At L1, the Authenticator Application shall follow best security practices specific to the underlying <u>operating environment</u> for protecting the <u>Authenticator Security Parameters</u> against being modified or substituted by (1) the user and (2) other applications.</p> <p>Due to the nature of L1 it is acceptable for the <u>Authenticator Application</u> to rely on the underlying <u>operating environment</u> for protecting the <u>Authenticator Security Parameters</u> against other applications running in the same <u>operating environment</u>.</p> <div data-bbox="272 604 1328 760" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="272 793 1328 1096" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale that all Authenticator Security Parameters within the Authenticator are protected against modification and substitution.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div data-bbox="272 1129 1328 1251" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="272 1285 1328 1440" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div data-bbox="272 1444 695 1482" style="border: 1px solid #ccc; padding: 5px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-1, SM-6, SM-13, SM-15, SM-16)</p>
<p><b>2.1.6</b></p>	<p>UAF + U2F; GaVR-3; L1+</p>	

No.	Requirement	Security Measures
	<p>All Secret Authenticator Security Parameters within the Authenticator shall be protected against unauthorized disclosure.</p> <p>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.</p> <p>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]).</p> <div data-bbox="272 915 1325 1068" style="border: 1px solid orange; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a rationale of how the requirement above is met.</p> </div> <div data-bbox="272 1100 1325 1341" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale that all Secret Authenticator Security Parameters within the Authenticator are protected against unauthorized disclosure.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div data-bbox="272 1373 1325 1497" style="border: 1px solid blue; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="272 1528 1325 1686" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div data-bbox="272 1686 695 1728" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-1, SM-13, SM-16)</p>
<p><b>2.1.7</b></p>	<p>UAF + U2F; TVFR; L1+</p>	

No.	Requirement	Security Measures
	<p>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.</p> <p><b>NOTE</b></p> <p>In this requirement, externally-stored refers to parameters stored outside of the <u>Authenticator boundary</u>. For example, cloud storage services.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div style="display: flex; gap: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	<p>(SM-1, SM-6, SM-13, SM-15, SM-16, SM-25)</p>
<p><b>2.1.8</b></p>	<p>UAF + U2F; TVFR; L1+</p>	

No.	Requirement	Security Measures
	<p>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.</p> <div data-bbox="272 306 1328 464" style="border: 1px solid orange; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="272 491 1328 617" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="272 644 1328 770" style="border: 1px solid blue; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="272 875 1328 917" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> </div> <div data-bbox="272 951 1328 1077" style="border: 1px solid blue; padding: 5px;"> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="272 1077 695 1115" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-1, SM-6, SM-13, SM-15, SM-16, SM-25)</p>
<p><b>2.1.9</b></p>	<p>UAF + U2F; TVFR; L1+</p>	



No.	Requirement	Security Measures
	<p>Any key used with an Allowed Key Protection Cryptographic Function to protect an externally-stored secret or private key which is an Authenticator Security Parameter shall have a claimed cryptographic strength greater than or equal to the claimed cryptographic strength of the key being wrapped.</p> <p><b>NOTE</b></p> <p>L1 externally-stored means stored outside the <u>Authenticator boundary</u>. In the case of L1 this <u>Authenticator boundary</u> includes the underlying operating environment.</p> <div data-bbox="272 615 1328 768" style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="272 800 1328 926" style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="272 957 1328 1083" style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="272 1115 1328 1268" style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="272 1268 695 1310" style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-1, SM-6, SM-16, SM-25)</p>
<p><b>2.1.10</b></p>	<p>UAF + U2F; TVFR; L1+</p>	

No.	Requirement	Security Measures
	<p>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 <b>Key Handle containing a key</b>.</p> <p>If the Authenticator uses such <b>Key Handle</b> 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].</p> <p><b>NOTE</b></p> <p>In the case of L1 this <u>Authenticator boundary</u> includes the underlying <u>operating environment</u>.</p> <div data-bbox="272 890 1325 1045" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="272 1075 1325 1199" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="272 1228 1325 1352" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="272 1381 1325 1541" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="272 1541 695 1583" style="border: 1px solid #ccc; padding: 5px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-1, SM-2, SM-16, SM-25, SM-27)</p>
<p><b>2.1.11</b></p>	<p>UAF; TVFR; L1+</p>	

No.	Requirement	Security Measures
	<p>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]</p> <div data-bbox="272 411 1328 562" style="border: 1px solid orange; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="272 632 1328 751" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="272 785 1328 905" style="border: 1px solid blue; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="272 938 1328 1094" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="272 1100 695 1136" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-13)
2.1.12	UAF + U2F; TVFR; L1+	

No.	Requirement	Security Measures
	<p>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) 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].</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div style="display: flex; gap: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	<p>(SM-1, SM-2, SM-16, SM-25, SM-27)</p>
<p><b>2.1.13</b></p>	<p>UAF + U2F; GaVR-1; L1+</p>	

No.	Requirement	Security Measures
	<p>The Authenticator shall generate an independent User Authentication Key for each registration [UAFAuthnrCommands], [Section 6.2.4].</p> <p><b>NOTE</b></p> <p>Any User Authentication Key (Uauth) shall only be used for authenticating one user account to one particular Relying Party.</p> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> the tester with documentation that specifies how the requirement above is met.</p> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> <p>VQ TP L1 L2 L3 L4 L5</p>	(SM-1, SM-2, SM-27)
2.1.14	<p>UAF + U2F; TVFR; L2+</p> <p>The Authenticator shall support Full Basic attestation (or an attestation method with equal or better security) or ECDAAs attestation.</p> <p>The Attestation Private Key shall only be used to sign well-formed FIDO attestation objects.</p> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> <p>VQ TP L1 L2 L3 L4 L5</p>	(SM-3)
2.1.15	<p>UAF + U2F; TVFR; L3+</p>	

No.	Requirement	Security Measures
	<p>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].</p> <div data-bbox="272 306 1325 430" style="border: 1px solid orange; padding: 5px;"> <p>L3 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="272 459 1325 617" style="border: 1px solid blue; padding: 5px;"> <p>L3 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="272 621 695 657" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-1)
2.1.16	<p>UAF + U2F; TVFR; L1+</p> <p>In the event that an Authenticator Security Parameter is destroyed, all plaintext instances of that parameter within the Authenticator shall be overwritten by data that is not dependent on the value of the parameter, e.g., overwriting the parameter with all 0s or some other fixed bit pattern. Authenticator Security Parameters that are cryptographically protected using an Allowed Confidentiality or Key Protection Cryptographic Function shall either be treated as plaintext (as above), or the key used to protect these Authenticator Security Parameters shall be destroyed.</p> <div data-bbox="272 1041 1325 1192" style="border: 1px solid orange; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="272 1222 1325 1346" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="272 1375 1325 1499" style="border: 1px solid blue; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="272 1528 1325 1686" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="272 1690 695 1726" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-1, SM-24)
2.1.17	UAF + U2F; TVFR; L2+	

No.	Requirement	Security Measures
	<p>Authenticators might support a function allowing the user resetting the Authenticator to the original (factory) state, i.e. deleting all user specific information. This process is called <b>factory reset</b> in this document.</p> <p>In the event of a <u>factory reset</u>, the Authenticator shall destroy all User-specific Secret Authenticator Security Parameters other than any Allowed Random Number Generator's state.</p> <div data-bbox="272 436 1328 562" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="272 590 1328 747" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="272 751 695 789" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-1, SM-18, SM-19)</p>
<p>2.1.18</p>	<p>UAF + U2F; TVFR; L1+</p> <p>Any time the Authenticator generates an <u>Authenticator Security Parameter</u> which is a key for use with an algorithm specified in the "Allowed Cryptography List" [<a href="#">FIDOAllowedCrypto</a>], the Authenticator shall generate keys as required by the standard referenced in the "Allowed Cryptography List" [<a href="#">FIDOAllowedCrypto</a>] for that algorithm.</p> <div data-bbox="272 1066 1328 1224" style="border: 1px solid orange; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="272 1251 1328 1377" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="272 1404 1328 1530" style="border: 1px solid blue; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="272 1558 1328 1715" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="272 1719 695 1757" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-1, SM-16, SM-21)</p>
<p>2.1.19</p>	<p>UAF + U2F; GaVR-1; L1+</p>	

No.	Requirement	Security Measures
	<p>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.</p> <p><b>NOTE</b></p> <p>Cryptographic Collision would be an exception.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator’s design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="display: flex; gap: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-31)
2.1.20	UAF + U2F; GaVR-1; L1+	



No.	Requirement	Security Measures
	<p>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.</p> <div data-bbox="272 304 1325 459" style="border: 1px solid orange; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="272 489 1325 699" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div data-bbox="272 728 1325 854" style="border: 1px solid blue; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="272 884 1325 1039" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div data-bbox="272 1045 695 1081" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-1, SM-6, SM-26)</p>

### 2.2.2 Random Number Generation

No.	Requirement	Security Measures
2.2.1	UAF + U2F; TVFR; L1+	

No.	Requirement	Security Measures
	<p>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.</p> <p>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.</p> <div data-bbox="256 506 1325 659" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="256 690 1325 814" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="256 921 1325 1083" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="256 1115 1325 1239" style="border: 1px solid #ccc; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="256 1241 678 1276" style="border: 1px solid #ccc; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-16)
2.2.2	UAF + U2F; DaD; L1+	

No.	Requirement	Security Measures
	<p>The security strength (see the relevant Allowed Deterministic Random Number Generator specification document cited in the “Allowed Cryptography List” [FIDOAllowedCrypto]) of any Authenticator’s Allowed Deterministic Random Number Generator shall be at least as large as the largest claimed cryptographic strength of any key generated or used.</p> <div data-bbox="256 373 1328 527" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="256 558 1328 680" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> the tester with documentation that specifies how the requirement above is met.</p> </div> <div data-bbox="256 711 1328 833" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="256 940 1328 1073" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div data-bbox="256 1073 678 1115" style="border: 1px solid #ccc; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-1, SM-26)</p>
<p><b>2.2.3</b></p>	<p>UAF + U2F; TVFR; L1+</p>	

No.	Requirement	Security Measures
	<p>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.</p> <p>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.</p> <div data-bbox="256 436 1328 590" style="border: 1px solid orange; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="256 621 1328 743" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="256 774 1328 896" style="border: 1px solid blue; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="256 928 1328 1050" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="256 1058 678 1094" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-16)
2.2.4	UAF; TVFR; L3+	

No.	Requirement	Security Measures												
	<p>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 <math>2^{-32}</math> after the maximum number of signatures allowed to be generated using that key.</p> <p>If a 16 byte Authenticator generated nonce value is added, no key use limit (see requirement 5.4) is required.</p> <p><b>NOTE</b></p> <p>This interacts with requirement 5.4, describing the maximum possible number of signatures.</p> <table border="1" data-bbox="256 680 1328 1062"> <thead> <tr> <th>Bytes in Nonce</th> <th>Log Base 2 of Allowed Operations</th> </tr> </thead> <tbody> <tr> <td>8</td> <td>16</td> </tr> <tr> <td>9</td> <td>20</td> </tr> <tr> <td>10</td> <td>24</td> </tr> <tr> <td>11</td> <td>28</td> </tr> <tr> <td>12</td> <td>32</td> </tr> </tbody> </table> <div data-bbox="256 1094 1328 1304" style="border: 1px solid orange; padding: 5px;"> <p>L3 Vendor Questionnaire</p> <p>Is this requirement applicable to the Authenticator? If <b>No</b>, then <i>describe</i> why.</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="256 1335 1328 1461" style="border: 1px solid blue; padding: 5px;"> <p>L3 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="256 1461 678 1499" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	Bytes in Nonce	Log Base 2 of Allowed Operations	8	16	9	20	10	24	11	28	12	32	(SM-8, SM-22)
Bytes in Nonce	Log Base 2 of Allowed Operations													
8	16													
9	20													
10	24													
11	28													
12	32													
2.2.5	UAF + U2F; L4+													

No.	Requirement	Security Measures
	<p>If the authenticator implements a Deterministic Random Number Generator, then Authenticator's Allowed Deterministic Random Number Generator shall be seeded using an Allowed Physical True Random Number Generator.</p> <p><b>NOTE</b></p> <p>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.</p> <p>VQ TP L1 L2 L3 L4 L5</p>	(SM-16)

### 2.2.3 Signature Counters

Support of Signature counters is optional.

**NOTE**

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

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

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

**NOTE**

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

No.	Requirement	Security Measures
2.3.1	UAF + U2F; DaD; L1+	

No.	Requirement	Security Measures
	<p>The vendor shall document whether the Authenticator supports Signature Counters and if they are supported, the vendor shall document whether one Signature Counter <i>per authentication key</i> is implemented or one (global) Signature Counter for all authentication keys.</p> <p>Authenticators not running in an <u>Allowed Restricted Operating Environment (AROE)</u> [<a href="#">FIDORestrictedOperatingEnv</a>], shall support signature counter(s).</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> the tester with documentation that specifies how the requirement above is met.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div style="display: flex; gap: 5px;"> <div style="border: 1px solid gray; padding: 2px;">VQ</div> <div style="border: 1px solid gray; padding: 2px;">TP</div> <div style="border: 1px solid gray; padding: 2px;">L1</div> <div style="border: 1px solid gray; padding: 2px;">L2</div> <div style="border: 1px solid gray; padding: 2px;">L3</div> <div style="border: 1px solid gray; padding: 2px;">L4</div> <div style="border: 1px solid gray; padding: 2px;">L5</div> </div>	(SM-15)
2.3.2	<p>UAF + U2F; GaVR-2; L1+</p> <p>If the Authenticator claims supporting signature counter(s), then the Authenticator shall ensure that the signature counter value <i>contained in FIDO signature assertions</i> related to one specific authentication key either</p> <ol style="list-style-type: none"> <li>1. is (a) greater than "0" and always has been greater than "0" for any previously generated FIDO signature assertion related to the same authentication key <i>and</i> is (b) greater than the signature counter value contained in any previously generated FIDO signature assertion related to the same authentication key, or</li> <li>2. is set to "0" indicating that the signature counter is not supported any longer (e.g. in the case of a counter error).</li> </ol> <div style="margin-top: 20px;"> <p style="color: green; font-weight: bold;">NOTE</p> <p>Once a signature counter value <i>contained in a FIDO signature assertion</i> for one specific authentication key has been set to "0" in must stay at such value for that specific authentication key (due to the requirement 1).</p> </div> <p>[<a href="#">U2FImplCons</a>], [Section 2.6] and [<a href="#">UAFAuthnrCommands</a>] [Section 6.3.4].</p>	(SM-15)

No.	Requirement	Security Measures
	<p>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 shall be incremented by a positive random number per signature operation (see [UAFAuthnrCommands] [Section A Security Guidelines, entry SignCounter]).</p> <div data-bbox="256 352 1328 562" style="border: 1px solid orange; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p>Is this requirement applicable to the Authenticator? If <b>No</b>, then <i>describe</i> why.</p> <p>If Yes, <i>provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="256 594 1328 888" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p>Is this requirement applicable to the Authenticator? If <b>No</b>, then <i>describe</i> why.</p> <p>If Yes, <i>provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div data-bbox="256 919 1328 1045" style="border: 1px solid blue; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="256 1077 1328 1234" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div data-bbox="256 1234 678 1276" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	

### 2.3 Authenticator's Test for User Presence and User Verification

No.	Requirement	Security Measures
3.1	UAF + U2F; TVFR; L1+	



No.	Requirement	Security Measures
	<p>The Authenticator shall provide a mechanism to establish if the user authorizes a given action. (For a U2F, this is the “Test for User Presence”. Generically, the term “User Verification” may also refer to this “Test for User Presence”.)</p> <p><b>NOTE</b></p> <p>This requirement prevents remote attacks. The user has to confirm an action by pressing a button or providing some other (physical) gesture.</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 10px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> <p>At L1, this requirement must be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.</p> </div> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 10px;"> <p>L1 Test Procedure</p> <p>{A0} The Security Secretariat shall <i>verify</i> the requirement during Interoperability Testing.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 10px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div style="display: flex; gap: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	<p>(SM-1, SM-5)</p>
<p><b>3.2</b></p>	<p>UAF + U2F; GaVR-2; L1+</p>	

No.	Requirement	Security Measures
	<p>The Authenticator shall not generate User Authentication Keys or produce signatures using such keys without first establishing that a user has requested this operation by verifying the user. [UAFAuthnrCommands], [section 6.2.4, 6.3.4]</p> <div data-bbox="237 338 1325 491" style="border: 1px solid orange; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="237 527 1325 730" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div data-bbox="237 766 1325 800" style="border: 1px solid blue; padding: 5px;"> <p>L1 Test Procedure</p> </div> <div data-bbox="237 867 1325 951" style="border: 1px solid blue; padding: 5px;"> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="237 982 1325 1136" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div data-bbox="237 1142 659 1178" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-1, SM-5)</p>
<p><b>3.3</b></p>	<p>U2F; TVFR; L1+</p>	

No.	Requirement	Security Measures
	<p>Once the Authenticator’s test for user presence is successful (and user presence is detected), the user shall be deemed “present” for no more than 10 seconds, or until the next operation which requires user presence is performed, whichever comes first.</p> <div data-bbox="237 338 1325 590" style="border: 1px solid orange; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> <p>At L1, this requirement must be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.</p> </div> <div data-bbox="237 621 1325 831" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator’s design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div data-bbox="237 863 1325 982" style="border: 1px solid blue; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A0} The Security Secretariat shall <i>verify</i> the requirement during Interoperability Testing.</p> </div> <div data-bbox="237 1014 1325 1136" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="237 1142 659 1178" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-5)
3.4	UAF; GaVR-1; L1+	

No.	Requirement	Security Measures
	<p>Once the Authenticator’s user verification is successful, the user shall be deemed “verified” for no more than 10 seconds, or until the next operation which requires user verification, whichever comes first. Any provided User Verification Token shall not be valid after this time period. [UAFAuthnrCommands], [Appendix A Security Guideleines]</p> <p><b>NOTE</b></p> <p>This security requirement helps mitigating timing attacks (e.g. cache-based timing attacks).</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> <p>At L1, this requirement must be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator’s design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A0} The Security Secretariat shall <i>verify</i> the requirement during Interoperability Testing.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="display: flex; gap: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-5)
3.5	UAF; GaVR-1; L1+	

No.	Requirement	Security Measures
	<p>The Authenticator shall not reveal the stored username(s) prior to verifying the user. [UAFAuthnrCommands], [Section 6.3.4]</p> <div data-bbox="237 268 1325 520" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> <p>At L1, this requirement must be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.</p> </div> <div data-bbox="237 552 1325 762" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div data-bbox="237 793 1325 919" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Test Procedure</p> <p>{A0} The Security Secretariat shall <i>verify</i> the requirement during Interoperability Testing.</p> </div> <div data-bbox="237 951 1325 1108" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div data-bbox="237 1108 659 1150" style="border: 1px solid #ccc; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-5, SM-10)</p>
<p><b>3.6</b></p>	<p>UAF; GaVR-1; L1+</p>	

No.	Requirement	Security Measures
	<p>The Authenticator shall not output unencrypted AppIDs or KeyIDs that are associated with a Key Handle prior to verifying the user.</p> <div data-bbox="237 268 1325 422" style="border: 1px solid orange; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="237 453 1325 541" style="border: 1px solid orange; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> </div> <div data-bbox="237 541 1325 663" style="border: 1px solid orange; padding: 5px;"> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div data-bbox="237 695 1325 816" style="border: 1px solid blue; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="237 848 1325 1003" style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div data-bbox="237 1003 659 1052" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-5, SM-23)</p>
<p><b>3.7</b></p>	<p>UAF + U2F; L3+</p>	

No.	Requirement	Security Measures
	<p>If the Authenticator accepts input directly from the user or provides outputs directly to the user, then this communication shall be protected from data injection, disclosure, modification or substitution through use of a Trusted Path. This Trusted Path shall allow a user to communicate directly with the Authenticator, shall only be able to be activated by the Authenticator or the user, and cannot be imitated by untrusted software.</p> <p>At L4+, the Authenticator shall implement protection measures for such trusted path against hardware based attacks.</p> <p><b>NOTE</b></p> <p>A Trusted Path is the means by which a user and a security functionality of the Authenticator can communicate with the necessary confidence. In other words, a Trusted Path allows users to perform functions through an assured direct interaction with the security functionality of the Authenticator. For instance, plaintext ASPs may be entered into or output from the Authenticator in an encrypted form (e.g. display text digitally signed).</p> <p>This means that if the Authenticator has a Transaction Confirmation Display, it shall be protected from a display overlay attack.</p> <div style="border: 1px solid orange; border-radius: 10px; padding: 5px; margin-top: 10px;"> <p>L3 Vendor Questionnaire</p> <p><i>Provide</i> documentation that specifies how the requirement above is met.</p> </div> <div style="display: flex; gap: 5px; margin-top: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	<p>(SM-5, SM-10, SM-29)</p>
<p><b>3.8</b></p>	<p>UAF + U2F; GaVR-3; L1+</p>	

No.	Requirement	Security Measures
	<p>The Authenticator shall protect against injection or replay of FIDO user verification data (e.g. user presence status, PIN, or biometric data).</p> <p>At L1, the Authenticator Application shall follow best security practices specific to the underlying operating environment for protecting against injection or replay of FIDO user verification data. This especially means that the <u>Authenticator Application</u> shall not provide any API for injecting FIDO user verification data.</p> <p>At L4+, the Authenticator shall implement protection measures against hardware based attacks of this kind.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-5, SM-31)</p>
<p><b>3.9</b></p>	<p>UAF + U2F; GaVR-3; L1+</p> <p>Authenticators implementing user verification methods other than user presence check [FIDOGlossary], shall rate-limit user verification attempts in order to prevent brute force attacks. [FIDOMETADATASTATEMENT], sections 3.1, 3.2, 3.3 and [UFAUTHNRCOMMANDS], Appendix A Security Guidelines, entry "Matcher".</p> <p>After the 5th (and subsequent) failed user verification attempts, the Authenticator shall enforce a delay of (at least) 30 seconds before accepting further user verification attempts.</p> <p>Counting failed attempts separately per user verification method is acceptable for no more than three different user verification methods (e.g. one counter for fingerprint, second counter for iris, third counter for PIN).</p> <p>The retry counter(s) shall be reset if and only if the user verification succeeds with some of the supported alternative user verification methods.</p>	<p>(SM-1, SM-5, SM-31)</p>



No.	Requirement	Security Measures							
	<p>This means that an Authenticator supporting only a single user verification method could only reset the retry counter if that user verification method succeeds.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• The rate limiting requirement applies to all user verification methods.</li> <li>• Implementing a more strict rate limiting method is allowed.</li> <li>• <i>We recommend</i> <ol style="list-style-type: none"> <li>1. an exponential increase of such delay, (e.g. 1 minute after the 6th+ false attempt, 2 minutes after the 7th+ false attempt, 4 minutes after the 8th+, etc.), or</li> <li>2. disabling biometric user verification after the 5th (and subsequent) failed attempt and falling back to an alternative knowledge based user verification method (e.g. PIN/Passcode/Pattern) if such alternative method is already implemented.</li> </ol> </li> <li>• We are considering making this recommendation mandatory in upcoming versions of these security requirements document.</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> <p>At L1, this requirement must be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>L1 Test Procedure</p> <p>{A0} The Security Secretariat shall <i>verify</i> the requirement during Interoperability Testing.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="margin-top: 10px;"> <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px 5px;">VQ</td> <td style="padding: 2px 5px;">TP</td> <td style="padding: 2px 5px;">L1</td> <td style="padding: 2px 5px;">L2</td> <td style="padding: 2px 5px;">L3</td> <td style="padding: 2px 5px;">L4</td> <td style="padding: 2px 5px;">L5</td> </tr> </table> </div>	VQ	TP	L1	L2	L3	L4	L5	
VQ	TP	L1	L2	L3	L4	L5			

## 2.4 Privacy

No.	Requirement	Security Measures
4.1	<p>UAF + U2F; GaVR-1; L1+</p> <p>An Authenticator shall not have any <b>Correlation Handle</b> that is visible across multiple Relying Parties.</p> <p>If the authenticator uses a shared attestation key (e.g. Full Basic Attestation), the minimum number of Authenticators sharing this key must be at least 100000.</p> <p><b>NOTE</b></p> <p>The goal of this requirement is that, for privacy reasons, the Authenticator must not leak information about the user across multiple Relying Parties by sharing a <u>Correlation Handle</u>.</p> <p>This requirement specifically applies to KeyIDs, KeyHandles etc.</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="display: flex; gap: 5px;"> <div style="border: 1px solid gray; padding: 2px;">VQ</div> <div style="border: 1px solid gray; padding: 2px;">TP</div> <div style="border: 1px solid gray; padding: 2px;">L1</div> <div style="border: 1px solid gray; padding: 2px;">L2</div> <div style="border: 1px solid gray; padding: 2px;">L3</div> <div style="border: 1px solid gray; padding: 2px;">L4</div> <div style="border: 1px solid gray; padding: 2px;">L5</div> </div>	(SM-23)
4.2	<p>UAF + U2F; GaVR-1; L1+</p>	

No.	Requirement	Security Measures
	<p>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.</p> <div data-bbox="237 270 1325 426" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="237 457 1325 541" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> </div> <div data-bbox="237 548 1325 667" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div data-bbox="237 695 1325 821" style="border: 1px solid #00aaff; padding: 5px; margin-bottom: 10px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="237 848 1325 1010" style="border: 1px solid #00aaff; padding: 5px; margin-bottom: 10px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div data-bbox="237 1010 659 1052" style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-23)
4.3	UAF; GaVR-1; L1+	

No.	Requirement	Security Measures
	<p>An external party with two (AAID, KeyID) tuples produced using the Authenticator shall not be able to establish that they were produced using the same Authenticator.</p> <div data-bbox="237 306 1325 459" style="border: 1px solid orange; padding: 5px; margin-bottom: 10px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="237 491 1325 699" style="border: 1px solid orange; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div data-bbox="237 730 1325 854" style="border: 1px solid blue; padding: 5px; margin-bottom: 10px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="237 886 1325 1041" style="border: 1px solid blue; padding: 5px; margin-bottom: 10px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div data-bbox="237 1045 660 1083" style="border: 1px solid gray; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-23)
4.4	UAF; GaVR-1; L1+	

No.	Requirement	Security Measures
	<p>The Authenticator's response to a "Deregister" command shall not reveal whether the provided KeyID was registered.</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> <p>At L1, this requirement must be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.</p> </div> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A0} The Security Secretariat shall <i>verify</i> the requirement during Interoperability Testing.</p> </div> <div style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="display: flex; gap: 5px; margin-top: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-23)

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

No.	Requirement	Security Measures
<b>5.1</b>	<p>UAF + U2F; DaD; L2+</p> <p>The vendor shall document the physical security and side channel attack protections used by the Authenticator.</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> the tester with documentation that specifies how the requirement above is met.</p> </div> <div style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div style="display: flex; gap: 5px; margin-top: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-1, SM-20, SM-24, SM-26, SM-33)
<b>5.2</b>	<p>UAF + U2F; L4+</p>	

No.	Requirement	Security Measures
	<p>The Authenticator shall provide evidence of physical tampering that allows the attacker to violate FIDO Security Goals or FIDO Authenticator Security Requirements.</p> <p><b>NOTE</b></p> <p>At L3 such evidence shall be visible to the user (and not necessarily to the RP). As a consequence, a level of cooperation from the user is expected to protect the RP.</p> <p>VQ TP L1 L2 L3 L4 L5</p>	(SM-20, SM-24, SM-26)
5.3	<p>UAF + U2F; L5+</p> <p>The Authenticator shall resist physical tampering that allows the attacker to violate FIDO Security Goals or FIDO Authenticator Security Requirements.</p> <p><b>NOTE</b></p> <p>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.</p> <p>VQ TP L1 L2 L3 L4 L5</p>	(SM-20, SM-24, SM-26)
5.4	<p>UAF + U2F; TVFR; L2+</p> <p>Each secret or private key that is an <u>Authenticator Security Parameter</u> shall have a key use limit establishing the maximal number of times that particular key can be used within a particular Authenticator.</p> <p>If the Authenticator adds a 16 byte nonce value (see requirement 2.2.4), no key use limit is required.</p> <p><b>NOTE</b></p> <p>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.</p> <p>This requirement interacts with requirements 2.3, 2.25, 5.5, 5.6.</p> <p>This is a requirement that provides flexibility in satisfying other requirements. The idea is that key use limit should be established such that the other requirements cited here are fulfilled (providing the vendor the ability to restrict the number of possible key uses rather than using longer nonces or better side-channel countermeasures), and additionally provides the option for the vendor to defend the Authenticator against attacks that are not yet known.</p>	(SM-24, SM-26)

No.		Security Measures
	<p>Both cryptographic and side-channel attacks on the Authenticator can be enabled by having access to information associated with distinct cryptographic operations under the same key, so the vendor may elect to impose a conservative key use limit in order to defend against such attacks, especially for attacks that are not yet known and thus cannot easily be otherwise defended against.</p> <p>Any limit that allows the Authenticator to fulfil the other related requirements is sufficient for compliance to the requirement set. Some examples follow:</p> <p>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 <math>(5 \times 365 + 1) \times 86400</math> (less than <math>2^{28}</math>) would be sufficient.</p> <p>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 <math>2^{24}</math>) 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.</p> <p>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.</p> <p>Some keys (e.g., the User Private Key, or the Attestation key) cannot be painlessly replaced within the FIDO protocol (this requires re-enrolling, or replacing the Authenticator, respectively), so a suitably large limit should be chosen to prevent usability problems.</p> <p>FIDO Authenticators typically require a user verification before using a private key. Such manual interaction requires a minimum amount of time.</p> <div data-bbox="240 1717 1325 1839" style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="240 1871 1325 1992" style="border: 1px solid blue; padding: 5px; margin-top: 10px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div>	

No.	Requirement	Security Measures
	<div style="display: flex; gap: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	
<b>5.5</b>	<p>UAF + U2F; L4+</p> <p>The Authenticator shall not leak <u>Secret Authenticator Security Parameter</u> data (e.g. due to power, near field, or radio leakage) at a rate that would allow an attacker to weaken the key below the claimed cryptographic strength of the key, even after an attacker has observed all allowed key uses.</p> <p><b>NOTE</b></p> <p>This interacts with requirement 5.4.</p> <div style="display: flex; gap: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-20)
<b>5.6</b>	<p>UAF + U2F; GaVR-3; L3+</p> <p>The variations in the amount of time required to perform a cryptographic algorithm shall not allow remote attackers to reduce the security of Authenticator Security Parameters which are secret or private keys below their claimed cryptographic strength.</p> <p><b>NOTE</b></p> <p>This requirement is mandatory for L3+ but it remains relevant for L2 as a developer guideline. It refers to all <u>Secret Authenticator Security Parameters</u>, 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.</p> <p>The defense against remote timing attacks requires securing the cryptographic operation implementations and/or hardening the <u>Allowed Restricted Operating Environment (AROE, see [FIDORestrictedOperatingEnv])</u> cache implementation:</p> <p><b>Securing cryptographic operations:</b> Concerning symmetric-key algorithms, It is recommended to use Hardware-based cryptographic algorithms replacing the software-based implementation and thus eliminating the side-channel information leaked from the execution of cryptographic operations. Otherwise, the software implementation must consider randomization of the control flow so that there is no fixed relation between the execution path and the cache set. Or, must enable using the same amount of cache independently from the keys used.</p> <p><b>AROE cache enhanced implementations:</b> 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 <u>AROE</u> cache memory. The implementation can also consider flushing sensitive secure cache to memory to eliminate the information on the table access.</p>	(SM-20, SM-33)



No.		Security Measures
	<p>For more details on how to implement adequate counter-measures please review the following research papers:</p> <ul style="list-style-type: none"> <li>• for <b>ECC, remote timing attack (protocol timing)</b> refer to <a href="https://eprint.iacr.org/2011/232">https://eprint.iacr.org/2011/232</a></li> <li>• for <b>ECC, local cache timing attack (local cache timing)</b> refer to <a href="http://eprint.iacr.org/2014/161">http://eprint.iacr.org/2014/161</a></li> <li>• for <b>RSA cache timing</b> refer to <a href="https://eprint.iacr.org/2015/898">https://eprint.iacr.org/2015/898</a></li> <li>• for <b>AES cache timing</b> refer to <a href="https://eprint.iacr.org/2014/435">https://eprint.iacr.org/2014/435</a></li> </ul> <p><b>NOTE</b></p> <p>This interacts with requirement 5.4.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>L3 Vendor Questionnaire</p> <p><i>Provide a rationale for how the requirement above is met.</i></p> <p><i>Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</i></p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>L3 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="display: flex; gap: 5px; margin-top: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	
5.7	<p>UAF + U2F; L4+</p> <p>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.</p> <p><b>NOTE</b></p> <p>No time variations are allowed in this requirement, in comparison to requirement 5.6, in which some time variations are allowed.</p> <div style="display: flex; gap: 5px; margin-top: 10px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-20, SM-33)
5.8	<p>UAF + U2F; GaVR-2; L2+</p>	

No.	Requirement	Security Measures
	<p>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.</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="display: flex; gap: 5px; margin-top: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-23, SM-26)
5.9	<p>UAF + U2F; L4+</p> <p>The Authenticator shall be resistant to induced fault attacks.</p> <div style="border-left: 3px solid green; padding-left: 10px; margin-top: 10px;"> <p><b>NOTE</b></p> <p>This requirement is mandatory for L4+ but it is still relevant for L2+ as a developer guideline. The developer shall take into account SW-based fault induction side channel attack and implement relevant countermeasures such as enabling memory error detection.</p> </div> <div style="display: flex; gap: 5px; margin-top: 10px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-32, SM-21)

## 2.6 Attestation

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

No.	Requirement	Security Measures
6.1	UAF + U2F; TVFR; L2+	

No.	Requirement	Security Measures
	<p>The vendor shall use attestation certificates / ECDAA Issuer public keys [FIDOEcdaaAlgorithm] dedicated to a single Authenticator model.</p> <div data-bbox="237 268 1325 394" style="border: 1px solid #ccc; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="237 422 1325 548" style="border: 1px solid #ccc; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="237 552 659 583" style="border: 1px solid #ccc; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-3)
6.2	<p>UAF + U2F; TVFR; L1+</p> <p>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.</p> <div data-bbox="237 831 1325 1083" style="border: 1px solid #ccc; padding: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> <p>At L1, this requirement must be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.</p> </div> <div data-bbox="237 1115 1325 1241" style="border: 1px solid #ccc; padding: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="237 1268 1325 1394" style="border: 1px solid #ccc; padding: 5px;"> <p>L1 Test Procedure</p> <p>{A0} The Security Secretariat shall <i>verify</i> the requirement during Interoperability Testing.</p> </div> <div data-bbox="237 1421 1325 1547" style="border: 1px solid #ccc; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="237 1551 659 1583" style="border: 1px solid #ccc; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-3)
6.3	<p>UAF + U2F; GaVR-1; L1+</p>	

No.	Requirement	Security Measures
	<p>The Authenticator shall accurately describe itself in its provided metadata, or alternately describe an Authenticator of lesser security. The vendor shall provide all mandatory Metadata Statement fields.</p> <div data-bbox="237 306 1325 558" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> <p>At L1, this requirement must be demonstrated to the Test Proctor during Interoperability Testing. Documentation is not required.</p> </div> <div data-bbox="237 625 1325 835" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div data-bbox="237 865 1325 991" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L1 Test Procedure</p> <p>{A0} The Security Secretariat shall <i>verify</i> the requirement during Interoperability Testing.</p> </div> <div data-bbox="237 1020 1325 1180" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div data-bbox="237 1180 659 1222" style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-3)
6.4	<p>UAF + U2F; DaD; L2+</p> <p>The vendor shall document whether the attestation root certificate is shared across multiple Authenticator models.</p> <p>In such case, the attestation certificate <b>MUST</b> contain an extension indicating the Authenticator model (e.g. AAID or AAGUID).</p> <div data-bbox="237 1495 1325 1621" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design document references.</p> </div> <div data-bbox="237 1650 1325 1734" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div data-bbox="237 1734 659 1776" style="border: 1px solid #ccc; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-3)
6.5	<p>UAF + FIDO2; DaD; L2+</p>	

No.	Requirement	Security Measures
	<p>The vendor shall document whether the attestation certificate includes the Authenticator model (e.g. AAID or AAGUID).</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> the tester with documentation that specifies how the requirement above is met.</p> </div> <div style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>verify</i> that the documentation meets the requirement.</p> </div> <div style="display: flex; gap: 5px; margin-top: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-3)

## 2.7 Operating Environment

### NOTE

At L1 we allow the Authenticator Application to run in any operating environment. For the levels L2-L5, the Authenticator Application needs to run in an Allowed Restricted Operating Environment [[FIDORestrictedOperatingEnv](#)].

No.	Requirement	Security Measures
7.1	<p>UAF + U2F; GaVR-1; L2+</p> <p>The Authenticator Application shall run in an Allowed Restricted Operating Environment (AROE)[<a href="#">FIDORestrictedOperatingEnv</a>].</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="display: flex; gap: 5px; margin-top: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-1)
7.2	<p>UAF + U2F; GaVR-3; L2+</p>	

No.	Requirement	Security Measures
	<p>The <u>operating environment</u> shall be configured so that all <u>operating environment security functions</u> used by the Authenticator are active and available for use to support the FIDO Authenticator Security Goals or FIDO Authenticator Security Requirements.</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator’s design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="display: flex; gap: 5px; margin-top: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-1)
7.3	<p>UAF + U2F; GaVR-3; L2+</p> <p>The <u>operating environment</u> shall prevent non-Authenticator processes from reading, writing and modifying running or stored Authenticator software and its associated memory.</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator’s design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div style="border: 1px solid blue; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="display: flex; gap: 5px; margin-top: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-1)
7.4	<p>UAF + U2F; GaVR-3; L2+</p>	

No.	Requirement	Security Measures
	<p>The <u>operating environment</u> shall not be able to be modified in a way that undermines the security of the Authenticator.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide a rationale for how the requirement above is met.</i></p> <p><i>Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</i></p> </div> <div style="border: 1px solid #ccc; padding: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="display: flex; gap: 5px; margin-top: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-1)
7.5	<p>UAF + U2F; GaVR-1; L2+</p> <p>The security configuration of the <u>operating environment</u> 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.</p> <div style="margin-top: 20px;"> <p><b>NOTE</b></p> <p>In some environments (e.g. PC), the user (i.e. anyone other than the Authenticator vendor or its delegates) might change the security configuration of the Authenticator. However, it is the responsibility of the Authenticator to detect potential changes in the Authenticator security configuration and provide the appropriate RP response through a FIDO assertion if the changed configuration still meets the expected security characteristics according to the Metadata Statement (or stop working and either protect the security parameters at the prior level or securely destroy them if it doesn't). The Authenticator certification must include all security configuration items available to the user.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide a rationale for how the requirement above is met.</i></p> <p><i>Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</i></p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="display: flex; gap: 5px; margin-top: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-1, SM-28)
7.6	<p>UAF + U2F; GaVR-1; L2+</p>	

No.	Requirement	Security Measures
	<p>The security characteristics of the Authenticator shall not be modifiable by anyone other than the Authenticator device vendor or its delegates.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Provide a rationale for how the requirement above is met.</i></p> <p><i>Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</i></p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="display: flex; gap: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-1, SM-28)

## 2.8 Self-Tests and Firmware Updates

No.	Requirement	Security Measures
8.1	<p>UAF + U2F; GaVR-2; L2+</p> <p>An Authenticator shall either (a) be resistant to induced fault analysis (requirement 5.7) 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.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p>Is this requirement applicable to the Authenticator? If <b>No</b>, then <i>describe</i> why.</p> <p><i>Provide a rationale for how the requirement above is met.</i></p> <p><i>Provide a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</i></p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this are consistent with the vendor's provided rationale.</p> </div> <div style="display: flex; gap: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-21, SM-24)
8.2	<p>UAF + U2F; TVFR; L1+</p>	



No.	Requirement	Security Measures
	<p>If the Authenticator mediates the update of its software, then the Authenticator shall use an Allowed Data Authentication or Signature Cryptographic Function 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.</p> <p>At L1, if the Authenticator Application mediates its own update, then it shall use an Allowed Data Authentication or Signature Cryptographic Function 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.</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p>Is this requirement applicable to the Authenticator? If <b>No</b>, then <i>describe</i> why.</p> <p>If Yes, <i>provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p>Is this requirement applicable to the Authenticator? If <b>No</b>, then <i>describe</i> why.</p> <p>If Yes, <i>provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	<p>(SM-16, SM-26, SM-24)</p>
<p><b>8.3</b></p>	<p>UAF + U2F; TVFR; L2+</p>	

No.	Requirement	Security Measures
	<p>An Authenticator shall either (a) be resistant to induced fault analysis (requirement 5.7) 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.</p> <div style="border: 1px solid orange; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p>Is this requirement applicable to the Authenticator? If <b>No</b>, then <i>describe</i> why.</p> <p><i>Provide</i> a rationale for how the requirement above is met.</p> <p><i>Provide</i> a documentation review procedure to confirm that the Authenticator's design is consistent with the provided rationale. Please provide explicit design document references.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div style="display: flex; gap: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-21)
<b>8.4</b>	<p>UAF + U2F; L3+</p> <p>An Authenticator shall either be resistant to induced fault analysis (requirement 5.7) or the Authenticator shall verify that any produced signature is valid prior to outputting the signature.</p> <div style="display: flex; gap: 5px;"> <span>VQ</span> <span>TP</span> <span>L1</span> <span>L2</span> <span>L3</span> <span>L4</span> <span>L5</span> </div>	(SM-21)

## 2.9 Manufacturing and Development

### NOTE

At L1, the creation of the final Authenticator Application is considered the Authenticator manufacturing.

No.	Requirement	Security Measures
<b>9.1</b>	<p>UAF + U2F; TVFR; L1+</p>	

No.	Requirement	Security Measures
	<p>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.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p>Is this requirement applicable to the Authenticator? If <b>No</b>, then <i>describe</i> why.</p> <p>If Yes, <i>provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p>Is this requirement applicable to the Authenticator? If <b>No</b>, then <i>describe</i> why.</p> <p>If Yes, <i>describe</i> how this requirement can be verified through documentation review. Please provide explicit design documentation references.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div style="display: flex; gap: 5px;"> <div style="border: 1px solid #ccc; padding: 2px;">VQ</div> <div style="border: 1px solid #ccc; padding: 2px;">TP</div> <div style="border: 1px solid #ccc; padding: 2px;">L1</div> <div style="border: 1px solid #ccc; padding: 2px;">L2</div> <div style="border: 1px solid #ccc; padding: 2px;">L3</div> <div style="border: 1px solid #ccc; padding: 2px;">L4</div> <div style="border: 1px solid #ccc; padding: 2px;">L5</div> </div>	(SM-28)
9.2	<p>UAF + U2F; TVFR; L2+</p> <p>Access to the private component of any Authenticator's attestation key shall be restricted to security-qualified authorized factory personnel.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design documentation references.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div style="display: flex; gap: 5px;"> <div style="border: 1px solid #ccc; padding: 2px;">VQ</div> <div style="border: 1px solid #ccc; padding: 2px;">TP</div> <div style="border: 1px solid #ccc; padding: 2px;">L1</div> <div style="border: 1px solid #ccc; padding: 2px;">L2</div> <div style="border: 1px solid #ccc; padding: 2px;">L3</div> <div style="border: 1px solid #ccc; padding: 2px;">L4</div> <div style="border: 1px solid #ccc; padding: 2px;">L5</div> </div>	(SM-28)
9.3	<p>UAF + U2F; TVFR; L2+</p>	

No.	Requirement	Security Measures
	<p>The manufacturing environment used to provision Authenticators with Authenticator Security Parameters which are keys shall be secured against electronic attacks aimed at capturing keying material.</p> <div data-bbox="237 306 1325 430" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design documentation references.</p> </div> <div data-bbox="237 459 1325 583" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="237 583 659 625" style="border: 1px solid #ccc; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-28)
9.4	<p>UAF + U2F; TVFR; L1+</p> <p>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.</p> <p>At L1, the use of a revision control system shall only be proven for the <u>Authenticator Application</u>.</p> <div data-bbox="237 1003 1325 1150" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="237 1180 1325 1306" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design documentation references.</p> </div> <div data-bbox="237 1335 1325 1461" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="237 1491 1325 1617" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="237 1617 659 1659" style="border: 1px solid #ccc; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-28)
9.5	<p>UAF + U2F; TVFR; L1+</p>	

No.	Requirement	Security Measures
	<p>Each version of each configuration item that comprises the Authenticator and associated documentation shall be assigned a unique identification.</p> <p>At L1, the configuration items comprising the <u>Authenticator Application</u> are relevant.</p> <p><b>NOTE</b></p> <p>"Configuration item" stands for all the objects managed by the configuration management system during the product development. These may be either parts of the product (e.g. source code) or objects related to the development of the product like guidance documents, development tools, tests results, etc.)</p> <div data-bbox="237 789 1325 940" style="border: 1px solid #f4a460; padding: 5px; margin-bottom: 5px;"> <p>L1 Vendor Questionnaire</p> <p><i>Provide</i> the Security Secretariat with a <u>rationale</u> of how the requirement above is met.</p> </div> <div data-bbox="237 974 1325 1096" style="border: 1px solid #f4a460; padding: 5px; margin-bottom: 5px;"> <p>L2 Vendor Questionnaire</p> <p><i>Describe</i> how this requirement can be verified through documentation review. Please provide explicit design documentation references.</p> </div> <div data-bbox="237 1129 1325 1251" style="border: 1px solid #4a90e2; padding: 5px; margin-bottom: 5px;"> <p>L1 Test Procedure</p> <p>{A1} The Security Secretariat shall <i>review</i> the provided rationale to verify the requirement is met.</p> </div> <div data-bbox="237 1285 1325 1407" style="border: 1px solid #4a90e2; padding: 5px; margin-bottom: 5px;"> <p>L2 Test Procedure</p> <p>{A2} The tester shall <i>conduct</i> the documentation review described by the vendor, and confirm that all the results of this review meet the requirement.</p> </div> <div data-bbox="237 1411 659 1444" style="border: 1px solid #ccc; padding: 2px;"> <p>VQ TP L1 L2 L3 L4 L5</p> </div>	(SM-28)

## A. References

### A.1 Normative references

#### [FIDOAllowedCrypto]

Dr. Joshua E. Hill; Douglas Biggs. [FIDO Authenticator Allowed Cryptography List](https://github.com/fido-alliance/security-requirements/blob/master/fido-authenticator-allowed-cryptography-list.html). August 2016. Draft. URL: <https://github.com/fido-alliance/security-requirements/blob/master/fido-authenticator-allowed-cryptography-list.html>

#### [FIDOEcdaaAlgorithm]

R. Lindemann; J. Camenisch; M. Drijvers; A. Edgington; A. Lehmann; R. Urian. [FIDO ECDA Algorithm](https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-ecdaa-v1.1-id-20170202.html). Implementation Draft. URL: <https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-ecdaa-v1.1-id-20170202.html>

#### [FIDOMetadataStatement]

B. Hill; D. Baghdasaryan; J. Kemp. *FIDO Metadata Statements v1.0*. Implementation Draft. URL: <https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-metadata-statement-v1.1-id-20170202.html>

**[FIDORestrictedOperatingEnv]**

Laurence Lundblade; Meagan Karlsson. *FIDO Authenticator Allowed Restricted Operating Environments List*. August 2016. Draft. URL: <https://github.com/fido-alliance/security-requirements/blob/master/fido-authenticator-allowed-restricted-operating-environments-list.html>

**[U2FImpICons]**

D. Balfanz. *FIDO U2F Implementation Considerations v1.0*. Draft. URL: <http://fidoalliance.org/specs/fido-u2f-implementation-considerations-v1.0-rd-20140209.pdf>

**[U2FRawMsgs]**

D. Balfanz. *FIDO U2F Raw Message Formats v1.0*. Draft. URL: <http://fidoalliance.org/specs/fido-u2f-raw-message-formats-v1.0-rd-20140209.pdf>

**[UAFAuthnrCommands]**

D. Baghdasaryan; J. Kemp; R. Lindemann; R. Sasson; B. Hill. *FIDO UAF Authenticator Commands v1.0*. Implementation Draft. URL: <https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-uaf-authnr-cmds-v1.1-id-20170202.html>

**[UAFProtocol]**

R. Lindemann; D. Baghdasaryan; E. Tiffany; D. Balfanz; B. Hill; J. Hodges. *FIDO UAF Protocol Specification v1.0*. Proposed Standard. URL: <https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-uaf-protocol-v1.1-id-20170202.html>

## A.2 Informative references

**[FIDOGlossary]**

R. Lindemann; D. Baghdasaryan; B. Hill; J. Hodges. *FIDO Technical Glossary*. Implementation Draft. URL: <https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-glossary-v1.1-id-20170202.html>

**[FIDOSecRef]**

R. Lindemann; D. Baghdasaryan; B. Hill. *FIDO Security Reference*. Implementation Draft. URL: <https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-security-ref-v1.1-id-20170202.html>

**[RFC2119]**

S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. March 1997. Best Current Practice. URL: <https://tools.ietf.org/html/rfc2119>

**[SP800-132]**

Meltem Sönmez Turan; Elaine Barker; William Burr; Lily Chen. *NIST Special Publication 800-132: Transitions: Recommendation for Password-Based Key Derivation*. December 2010. URL: <http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf>