IMPLEMENTATION DRAFT

FIDO UAF Errata

FIDO Alliance Implementation Draft 02 February 2017

This version:
https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-uaf-errata-v1.1-id-20170202.html
Previous version:
https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-errata-v1.0-ps-20141208.html

Editor:
Dr. Rolf Lindemann, Nok Nok Labs, Inc.

Copyright © 2013-2017 FIDO Alliance All Rights Reserved.

Abstract

This document defines the errata of the FIDO UAF specifications.

Status of This Document

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

This document was published by the FIDO Alliance as a Implementation Draft. This document is intended to become a FIDO Alliance Proposed Standard. If you wish to make comments regarding this document, please Contact Us. All comments are welcome.

This Implementation Draft Specification has been prapared by FIDO Alliance, Inc. Permission is hereby granted to use the Specification solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works of this Specification. Entities seeking permission to reproduce portions of this Specification for other uses must contact the FIDO Alliance to determine whether an appropriate license for such use is available.

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

Type names, attribute names and element names are written as `code`.

String literals are enclosed in “”, e.g. “UAF-TLV”.

In formulas we use “|” to denote byte wise concatenation operations.

UAF specific terminology used in this document is defined in [FIDOGlossary].

All diagrams, examples, notes in this specification are non-normative.

1.1 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].

2. FIDO UAF v1.1 Errata

This section is normative.

2.1 FIDO UAF Registry

Section 5.2 Android Key Attestation

See [UAFRegistry], step 2 in Server Processing currently states:

"it must verify the syntax of the key attestation extension and it must perform RFC5280 compliant chain validation of the entries in the array to one attestationRootCertificate specified in the Metadata Statement."

This step needs to be corrected into:

"it must verify the syntax of the key attestation extension and it must perform RFC5280 compliant chain validation of the entries in the array to one attestationRootCertificate specified in the Metadata Statement - **accepting that that the keyCertSign bit in the key usage extension of the certificate issuing the leaf certificate is NOT set (which is a deviation from RFC5280)."**

A. References

A.1 Normative 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

[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

[UAFRegistry]

R. Lindemann; D. Baghdasaryan; B. Hill. *FIDO UAF Registry of Predefined Values*. Proposed Standard. URL: https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-uaf-reg-v1.1-id-20170202.html