FIDO Authenticator Metadata Requirements

FIDO Alliance Final Requirements Document 02 November 2020

This version:
https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-metadata-requirements-v1.2-fd-20201102.html
Previous version:
https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-metadata-requirements-v1.1-fd-20180629.html
Editors:
Meagan Karlsson, FIDO Alliance
Roland Atoui, FIDO Alliance

Abstract

This document supports the FIDO Authenticator Certification program.

The fields in the Authenticator Metadata will be the primary method of communicating Authenticator Certification status and details about implementations to Relying Parties (RPs).

Status of This Document

This section describes the status of this document at the time of its publication. Other documents may supersede this document. The most recent version of this document can be found on the FIDO Alliance Website at https://fidoalliance.org.

This document was published by the FIDO Alliance as a Final Requirements Document. If you wish to

make comments regarding this document, please Contact Us. All comments are welcome.

Table of Contents

- 1. Notation
  - 1.1 Version
- 2. Introduction
- 3. Security Metadata Fields
- 4. Biometric Metadata Fields
- 5. Use of Metadata Service 1.1 Status Dictionary
- A. References
  - A.1 Normative references

1. Notation

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

1.1 Version

This document specifies version 1.1.0 of the metadata requirements.

2. Introduction

This document reflects the Metadata Requirements for Authenticator Certification.

Mandatory fields are required to be evaluated by the FIDO Security Secretariat (Level 1), or the FIDO Accredited Security Laboratory (Level 2 and above) and submitted to FIDO Security Secretariat as part of the Certification Request. Submitted metadata will be verified to be an accurate representation of the implementation.

Submission of Metadata to the FIDO Metadata Service (MDS) is optional, and can be done after recieving FIDO Authenticator Certification. If Metadata is submitted to MDS, the elements marked herin

as Mandatory (and applicable to the product type under certification) must be submitted and must match the Metadata submitted to FIDO during Authenticator Certification.

For each field listed in this document an Application Note is provided. All these fields are described in [FIDOMetadataStatement] and/or [FIDOMetadataService] document.

Functional Metadata Fields

The following Functional Metadata Fields are Mandatory for Authenticator Certification when applicable.

Field	Application Note
VerificationMethodDescriptor	Applicable to all.
verificationMethodANDCombination	Applicable to all.
AAID	Applicable to FIDO UAF.
AAGUID	Applicable to FIDO 2.0.
attestationCertificateKeyIdentifiers	Applicable to all.
description	Applicable to all.
authenticatorVersion	Applicable to all.
protocolFamily	Applicable to all.
upv	Applicable to all.
userVerificationDetails	Applicable to all.
attachmentHint	Applicable to all.
isSecondFactorOnly	Applicable to all.
tcDisplay	Applicable to all.
tcDisplayContentType	Applicable to all.

3. Security Metadata Fields

The following Security-related Metadata Fields are Mandatory for Authenticator Certification when applicable.

Field	Application Note
CodeAccuracyDescriptor	Applicable to all.
PatternAccuracyDescriptor	Applicable to all.
EcdaaTrustAnchor	Applicable in the case of ECDAA attestation

attestationRootCertificate	Applicable in the case of ECDAA attestation
assertionScheme	Applicable to all.
authenticationAlgorithm	Applicable to all.
publicKeyAlgAndEncoding	Applicable to all.
attestationTypes	Applicable to all.
keyProtection	Applicable to all.
matcherProtection	Applicable to all.
isKeyRestricted	Applicable to all.
isFreshUserVerificationRequired	Applicable to all.
certificationDescriptor	Applicable to all.
certificateNumber	Applicable to all.
certificationRequirementsVersion	Applicable to all.
cryptoStrength	Applicable to Authenticators certified at L2 or above
operatingEnv	Applicable to Authenticators certified at L2 or above

4. Biometric Metadata Fields

Providing the biometry related Metadata Statement field [FIDOMetadataStatement] is not mandatory for passing FIDO Authenticator Certification at L2 and below.

Field	Application Note
BiometricAccuracyDescriptor	Applicable to the FIDO Biometrics Component
selfAttestedFRR	Applicable to the FIDO Biometrics Component
selfAttestedFAR	Applicable to the FIDO Biometrics Component
maxTemplates	Applicable to the FIDO Biometrics Component
maxRetries	Applicable to the FIDO Biometrics Component
blockSlowdown	Applicable to the FIDO Biometrics Component

5. Use of Metadata Service 1.1 Status Dictionary

SRWG recommends the use of the Status Dictionary to report the issue dates of Certifications within the array of status report entries. Default status to as “not FIDO Certified” and status is updated to include

Certifications as they are achieved. Each Certification would have a separate entry.

A. References

A.1 Normative references

[FIDOMetadataService]
R. Lindemann; B. Hill; D. Baghdasaryan. *FIDO Metadata Service*. Implementation Draft. URL: https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-metadata-service-v2.0-id-20180227.html

[FIDOMetadataStatement]
B. Hill; D. Baghdasaryan; J. Kemp. *FIDO Metadata Statements*. Implementation Draft. URL: https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-metadata-statement-v2.0-id-20180227.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