FIDO Metadata Statements

FIDO Alliance Review Draft 02 July 2018

This version:  

Previous version:  

Editors:  
Rolf Lindemann, Nok Nok Labs, Inc.  
John Kemp, FIDO Alliance

Contributors:  
Brad Hill, PayPal, Inc.  
Davit Baghdasaryan, Nok Nok Labs, Inc.

Copyright © 2013-2018 FIDO Alliance. All Rights Reserved.

Abstract

FIDO authenticators may have many different form factors, characteristics and capabilities. This document defines a standard means to describe the relevant pieces of information about an authenticator in order to interoperate with it, or to make risk-based policy decisions about transactions involving a particular authenticator.

Status of This Document

This section describes the status of this document at the time of its publication. Other documents may supersede this document. 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 Review 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 is a Review Draft Specification and is not intended to be a basis for any implementations as the Specification may change. Permission is hereby granted to use the Specification solely for the purpose of reviewing 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,
Table of Contents

1. Notation
   1.1 Conformance

2. Overview
   2.1 Scope
   2.2 Audience
   2.3 Architecture

3. Types
   3.1 Authenticator Attestation GUID (AAGUID) typedef
   3.2 CodeAccuracyDescriptor dictionary
      ■ 3.2.1 Dictionary CodeAccuracyDescriptor Members
   3.3 BiometricAccuracyDescriptor dictionary
      ■ 3.3.1 Dictionary BiometricAccuracyDescriptor Members
   3.4 PatternAccuracyDescriptor dictionary
      ■ 3.4.1 Dictionary PatternAccuracyDescriptor Members
   3.5 VerificationMethodDescriptor dictionary
      ■ 3.5.1 Dictionary VerificationMethodDescriptor Members
   3.6 verificationMethodANDCombinations typedef
   3.7 rgbPaletteEntry dictionary
      ■ 3.7.1 Dictionary rgbPaletteEntry Members
   3.8 DisplayPNGCharacteristicsDescriptor dictionary
      ■ 3.8.1 Dictionary DisplayPNGCharacteristicsDescriptor Members
   3.9 EcdaaTrustAnchor dictionary
      ■ 3.9.1 Dictionary EcdaaTrustAnchor Members
   3.10 ExtensionDescriptor dictionary
      ■ 3.10.1 Dictionary ExtensionDescriptor Members
   3.11 AlternativeDescriptions dictionary
      ■ 3.11.1 Dictionary AlternativeDescriptions Members

4. Metadata Keys
   4.1 Dictionary MetadataStatement Members

5. Metadata Statement Format
   5.1 UAF Example
   5.2 U2F Example
   5.3 FIDO2 Example

6. Additional Considerations
   6.1 Field updates and metadata

A. References
   A.1 Normative references
   A.2 Informative references

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.

DOM APIs are described using the ECMAScript ECMA-262 bindings for WebIDL [WebIDL-ED].
Following [WebIDL-ED], dictionary members are optional unless they are explicitly marked as required.

WebIDL dictionary members **MUST NOT** have a value of null.

Unless otherwise specified, if a WebIDL dictionary member is DOMString, it **MUST NOT** be empty.

Unless otherwise specified, if a WebIDL dictionary member is a List, it **MUST NOT** be an empty list.

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

**NOTE**

Note: Certain dictionary members need to be present in order to comply with FIDO requirements. Such members are marked in the WebIDL definitions found in this document, as **required**. The keyword **required** has been introduced by [WebIDL-ED], which is a work-in-progress. If you are using a WebIDL parser which implements [WebIDL], then you may remove the keyword **required** from your WebIDL and use other means to ensure those fields are present.

1.1 Conformance

As well as sections marked as non-normative, all authoring guidelines, diagrams, examples, and notes in this specification are non-normative. Everything else in this specification is normative.

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

2. Overview

*This section is non-normative.*

The FIDO family of protocols enable simpler and more secure online authentication utilizing a wide variety of different devices in a competitive marketplace. Much of the complexity behind this variety is hidden from Relying Party applications, but in order to accomplish the goals of FIDO, Relying Parties must have some means of discovering and verifying various characteristics of authenticators. Relying Parties can learn a subset of verifiable information for authenticators certified by the FIDO Alliance with an Authenticator Metadata statement. The URL to access that Metadata statement is provided by the Metadata TOC file accessible through the Metadata Service [FIDOMetadataService].

For definitions of terms, please refer to the FIDO Glossary [FIDO Glossary].

2.1 Scope

This document describes the format of and information contained in Authenticator Metadata statements. For a definitive list of possible values for the various types of information, refer to the FIDO Registry of Predefined Values [FIDO Registry].

The description of the processes and methods by which authenticator metadata statements are distributed and the methods how these statements can be verified are described in the Metadata Service Specification [FIDOMetadataService].

2.2 Audience

The intended audience for this document includes:

- FIDO authenticator vendors who wish to produce metadata statements for their products.
- FIDO server implementers who need to consume metadata statements to verify characteristics of authenticators and attestation statements, make proper algorithm choices for protocol messages, create policy statements or tailor various other modes of operation to authenticator-specific characteristics.
- FIDO relying parties who wish to
  - create custom policy statements about which authenticators they will accept
  - risk score authenticators based on their characteristics
  - verify attested authenticator IDs for cross-referencing with third party metadata

2.3 Architecture
Authenticator metadata statements are used directly by the FIDO server at a relying party, but the information contained in the authoritative statement is used in several other places. How a server obtains these metadata statements is described in [FIDOMetadataService].

The workflow around an authenticator metadata statement is as follows:

1. The authenticator vendor produces a metadata statement, that is UTF-8 encoded, describing the characteristics of an authenticator.
2. The metadata statement is submitted to the FIDO Alliance as part of the FIDO certification process. The FIDO Alliance distributes the metadata as described in [FIDOMetadataService].
3. A FIDO relying party configures its registration policy to allow authenticators matching certain characteristics to be registered.
4. The FIDO server sends a registration challenge message. This message can contain such policy statement.
5. Depending on the FIDO protocol being used, either the relying party application or the FIDO UAF Client receives the policy statement as part of the challenge message and processes it. It queries available authenticators for their self-reported characteristics and (with the user’s input) selects an authenticator that matches the policy, to be registered.
6. The client processes and sends a registration response message to the server. This message contains a reference to the authenticator model and, optionally, a signature made with the private key corresponding to the public key in the authenticator’s attestation certificate.
7. The FIDO Server looks up the metadata statement for the particular authenticator model. If the metadata statement lists an attestation certificate(s), it verifies that an attestation signature is present, and made with the private key corresponding to either (a) one of the certificates listed in this metadata statement or (b) corresponding to the public key in a certificate that chains to one of the issuer certificates listed in the authenticator’s metadata statement.
8. The FIDO Server next verifies that the authenticator meets the originally supplied registration policy based on its authoritative metadata statement. This prevents the registration of unexpected authenticator models.
9. Optionally, a FIDO Server may, with input from the Relying Party, assign a risk or trust score to the authenticator, based on its metadata, including elements not selected for by the stated policy.
10. Optionally, a FIDO Server may cross-reference the attested authenticator model with other metadata databases.
published by third parties. Such third-party metadata might, for example, inform the FIDO Server if an authenticator has achieved certifications relevant to certain markets or industry verticals, or whether it meets application-specific regulatory requirements.

3. Types

*This section is normative.*

3.1 Authenticator Attestation GUID (AAGUID) typedef

```webidl
typedef DOMString AAGUID;
```

Some authenticators have an AAGUID, which is a 128-bit identifier that indicates the type (e.g. make and model) of the authenticator. The AAGUID **MUST** be chosen by the manufacturer to be identical across all substantially identical authenticators made by that manufacturer, and different (with probability $1 - 2^{-128}$ or greater) from the AAGUIDs of all other types of authenticators.

The AAGUID is represented as a string (e.g. "7a98c250-6808-11cf-b73b-00aa00b677a7") consisting of 5 hex strings separated by a dash ("-"). see [RFC4122].

3.2 CodeAccuracyDescriptor dictionary

The **CodeAccuracyDescriptor** describes the relevant accuracy/complexity aspects of passcode user verification methods.

**NOTE**

One example of such a method is the use of 4 digit PIN codes for mobile phone SIM card unlock.

We are using the numeral system base (radix) and minLen, instead of the number of potential combinations since there is sufficient evidence [iPhonePasscodes] [MoreTopWorstPasswords] that users don't select their code evenly distributed at random. So software might take into account the various probability distributions for different bases. This essentially means that in practice, passcodes are not as secure as they could be if randomly chosen.

```webidl
dictionary CodeAccuracyDescriptor {
    required unsigned short base;
    required unsigned short minLength;
    unsigned short maxRetries;
    unsigned short blockSlowdown;
};
```

3.2.1 Dictionary **CodeAccuracyDescriptor** Members

- **base** of type required unsigned short
  
  The numeric system base (radix) of the code, e.g. 10 in the case of decimal digits.

- **minLength** of type required unsigned short
  
  The minimum number of digits of the given base required for that code, e.g. 4 in the case of 4 digits.

- **maxRetries** of type unsigned short
  
  Maximum number of false attempts before the authenticator will block this method (at least for some time). 0 means it will never block.

- **blockSlowdown** of type unsigned short
  
  Enforced minimum number of seconds wait time after blocking (e.g. due to forced reboot or similar). 0 means this user verification method will be blocked, either permanently or until an alternative user verification method method succeeded. All alternative user verification methods **MUST** be specified appropriately in the Metadata in userVerificationDetails.

3.3 BiometricAccuracyDescriptor dictionary
The BiometricAccuracyDescriptor describes relevant accuracy/complexity aspects in the case of a biometric user verification method, see [FIDOBiometricsRequirements].

At least one of the values MUST be set. If the vendor doesn't want to specify such values, then VerificationMethodDescriptor.baDesc MUST be omitted.

NOTE

Typical fingerprint sensor characteristics can be found in Google Android 6.0 Compatibility Definition and Apple iOS Security Guide.

WebIDL

dictionary BiometricAccuracyDescriptor {
    double selfAttestedFRR;
    double selfAttestedFAR;
    unsigned short maxTemplates;
    unsigned short maxRetries;
    unsigned short blockSlowdown;
};

3.3.1 Dictionary BiometricAccuracyDescriptor Members

selfAttestedFRR of type double

The false rejection rate [ISO19795-1] for a single template, i.e. the percentage of verification transactions with truthful claims of identity that are incorrectly denied. For example a FRR of 10% would be encoded as 0.1.

This value is self attested and, if the authenticator passed biometric certification, the data is an independently verified FRR as measured when meeting the FRR target specified in the biometric certification requirements [FIDOBiometricsRequirements] for the indicated biometric certification level (see certLevel in related biometricStatusReport as specified in [FIDOMetadataService]).

NOTE

The false rejection rate is relevant for user convenience. Lower false rejection rates mean better convenience.

selfAttestedFAR of type double

The false acceptance rate [ISO19795-1] for a single template, i.e. the percentage of verification transactions with wrongful claims of identity that are incorrectly confirmed. For example a FAR of 0.002% would be encoded as 0.00002.

This value is self attested and, if the authenticator passed biometric certification, the data is an independently verified FAR specified in the biometric certification requirements [FIDOBiometricsRequirements] for the indicated biometric certification level (see certLevel in related biometricStatusReport as specified in [FIDOMetadataService]).

NOTE

The resulting FAR when all templates are used is approx. maxTemplates * FAR.

The false acceptance rate is relevant for the security. Lower false acceptance rates mean better security.

Only the live captured subjects are covered by this value - not the presentation of artefacts.

maxTemplates of type unsigned short

Maximum number of alternative templates from different fingers allowed (for other modalities, multiple parts of the body that can be used interchangeably), e.g. 3 if the user is allowed to enroll up to 3 different fingers to a fingerprint based authenticator.

If the authenticator passed biometric certification this value defaults to 1. For maxTemplates greater than one, it SHALL be independently verified to ensure FAR meets biometric performance requirements of certLevel (of the related biometricStatusReport as specified in [FIDOMetadataService]).
If the authenticator did not pass biometric certification, vendor can submit any number, but this number has not been validated for biometric performance requirements.

- **maxRetries** of type unsigned short
  Maximum number of false attempts before the authenticator will block this method (at least for some time). 0 means it will never block.

- **blockSlowdown** of type unsigned short
  Enforced minimum number of seconds wait time after blocking (e.g. due to forced reboot or similar). 0 means that this user verification method will be blocked either permanently or until an alternative user verification method succeeded. All alternative user verification methods **must** be specified appropriately in the metadata in `userVerificationDetails`.

### 3.4 PatternAccuracyDescriptor dictionary

The **PatternAccuracyDescriptor** describes relevant accuracy/complexity aspects in the case that a pattern is used as the user verification method.

**NOTE**

One example of such a pattern is the 3x3 dot matrix as used in Android [AndroidUnlockPattern] screen unlock. The `minComplexity` would be 1624 in that case, based on the user choosing a 4-digit PIN, the minimum allowed for this mechanism.

**WebIDL**

```webidl
dictionary PatternAccuracyDescriptor {
  required unsigned long minComplexity;
  unsigned short maxRetries;
  unsigned short blockSlowdown;
};
```

#### 3.4.1 Dictionary PatternAccuracyDescriptor Members

- **minComplexity** of type required unsigned long
  Number of possible patterns (having the minimum length) out of which exactly one would be the right one, i.e. 1/probability in the case of equal distribution.

- **maxRetries** of type unsigned short
  Maximum number of false attempts before the authenticator will block authentication using this method (at least temporarily). 0 means it will never block.

- **blockSlowdown** of type unsigned short
  Enforced minimum number of seconds wait time after blocking (due to forced reboot or similar mechanism). 0 means this user verification method will be blocked, either permanently or until an alternative user verification method method succeeded. All alternative user verification methods **must** be specified appropriately in the metadata under `userVerificationDetails`.

### 3.5 VerificationMethodDescriptor dictionary

A descriptor for a specific base user verification method as implemented by the authenticator.

A base user verification method must be chosen from the list of those described in [FIDORegistry]

**NOTE**

In reality, several of the methods described above might be combined. For example, a fingerprint based user verification can be combined with an alternative password.

The specification of the related AccuracyDescriptor is optional, but recommended.

**WebIDL**

```webidl
dictionary VerificationMethodDescriptor {
```
3.5.1 Dictionary VerificationMethodDescriptor Members

- **userVerification** of type required unsigned long
  a single USER_VERIFY constant (see [FIDORegistry]), not a bit flag combination. This value MUST be non-zero.

- **caDesc** of type CodeAccuracyDescriptor
  May optionally be used in the case of method USER_VERIFY_PASSCODE.

- **baDesc** of type BiometricAccuracyDescriptor
  May optionally be used in the case of method USER_VERIFY_FINGERPRINT, USER_VERIFY_VOICEPRINT, USER_VERIFY_FACEPRINT, USER_VERIFY_EYEPRINT, or USER_VERIFY_HANDPRINT.

- **paDesc** of type PatternAccuracyDescriptor
  May optionally be used in case of method USER_VERIFY_PATTERN.

3.6 verificationMethodANDCombinations typedef

```
WebIDL
typedef VerificationMethodDescriptor[] VerificationMethodANDCombinations;
```

VerificationMethodANDCombinations MUST be non-empty. It is a list containing the base user verification methods which must be passed as part of a successful user verification.

This list will contain only a single entry if using a single user verification method is sufficient.

If this list contains multiple entries, then all of the listed user verification methods MUST be passed as part of the user verification process.

3.7 rgbPaletteEntry dictionary

The rgbPaletteEntry is an RGB three-sample tuple palette entry

```
WebIDL
dictionary rgbPaletteEntry { 
  required unsigned short r;
  required unsigned short g;
  required unsigned short b;
};
```

3.7.1 Dictionary rgbPaletteEntry Members

- **r** of type required unsigned short
  Red channel sample value

- **g** of type required unsigned short
  Green channel sample value

- **b** of type required unsigned short
  Blue channel sample value

3.8 DisplayPNGCharacteristicsDescriptor dictionary

The DisplayPNGCharacteristicsDescriptor describes a PNG image characteristics as defined in the PNG [PNG] spec for IHDR (image header) and PLTE (palette table)

```
WebIDL
dictionary DisplayPNGCharacteristicsDescriptor { 
  required unsigned long width;
  required unsigned long height;
  required octet bitDepth;
};
```
3.8.1 Dictionary `DisplayPNGCharacteristicsDescriptor` Members

- **width** of type `required unsigned long`
  - image width

- **height** of type `required unsigned long`
  - image height

- **bitDepth** of type `required octet`
  - Bit depth - bits per sample or per palette index.

- **colorType** of type `required octet`
  - Color type defines the PNG image type.

- **compression** of type `required octet`
  - Compression method used to compress the image data.

- **filter** of type `required octet`
  - Filter method is the preprocessing method applied to the image data before compression.

- **interlace** of type `required octet`
  - Interlace method is the transmission order of the image data.

- **plte** of type array of `rgbPaletteEntry`
  - 1 to 256 palette entries

3.9 EcdaaTrustAnchor dictionary

In the case of ECDAA attestation, the ECDAA-Issuer’s trust anchor **MUST** be specified in this field.

<table>
<thead>
<tr>
<th>WebIDL</th>
</tr>
</thead>
</table>
| `dictionary EcdaaTrustAnchor {`
| `  required DOMString X;`
| `  required DOMString Y;`
| `  required DOMString c;`
| `  required DOMString sx;`
| `  required DOMString sy;`
| `  required DOMString G1Curve;`
| `};` |

3.9.1 Dictionary `EcdaaTrustAnchor` Members

- **X** of type `required DOMString`
  - base64url encoding of the result of `ECPoint2ToB` of the `ECPoint2 X = P_X`. See [FIDOEcdaaAlgorithm] for the definition of `ECPoint2ToB`.

- **Y** of type `required DOMString`
  - base64url encoding of the result of `ECPoint2ToB` of the `ECPoint2 Y = P_Y`. See [FIDOEcdaaAlgorithm] for the definition of `ECPoint2ToB`.

- **c** of type `required DOMString`
  - base64url encoding of the result of `BigNumberToB(c)`. See section “Issuer Specific ECDAA Parameters” in [FIDOEcdaaAlgorithm] for an explanation of c. See [FIDOEcdaaAlgorithm] for the definition of `BigNumberToB`.

- **sx** of type `required DOMString`
  - base64url encoding of the result of `BigNumberToB(sx)`. See section “Issuer Specific ECDAA Parameters” in [FIDOEcdaaAlgorithm] for an explanation of sx. See [FIDOEcdaaAlgorithm] for the definition of `BigNumberToB`.

- **sy** of type `required DOMString`
  - base64url encoding of the result of `BigNumberToB(sy)`. See section “Issuer Specific ECDAA Parameters” in [FIDOEcdaaAlgorithm] for an explanation of sy.
[FIDOEcdaaAlgorithm] for an explanation of $s_y$. See [FIDOEcdaaAlgorithm] for the definition of BigNumberToB.

**G1Curve** of type required DOMString

**NOTE**
Whenever a party uses this trust anchor for the first time, it must first verify that it was correctly generated by verifying $s$, $s_x$, $s_y$. See [FIDOEcdaaAlgorithm] for details.

3.10 ExtensionDescriptor dictionary
This descriptor contains an extension supported by the authenticator.

```webidl
dictionary ExtensionDescriptor {
  required DOMString id;
  unsigned short tag;
  DOMString data;
  required boolean fail_if_unknown;
};
```

3.10.1 Dictionary ExtensionDescriptor Members

- **id** of type required DOMString
  Identifies the extension.

- **tag** of type unsigned short
  The TAG of the extension if this was assigned. TAGs are assigned to extensions if they could appear in an assertion.

- **data** of type DOMString
  Contains arbitrary data further describing the extension and/or data needed to correctly process the extension.

  This field **MAY** be missing or it **MAY** be empty.

- **fail_if_unknown** of type required boolean
  Indicates whether unknown extensions must be ignored (false) or must lead to an error (true) when the extension is to be processed by the FIDO Server, FIDO Client, ASM, or FIDO Authenticator.

  - A value of false indicates that unknown extensions **MUST** be ignored
  - A value of true indicates that unknown extensions **MUST** result in an error.

3.11 AlternativeDescriptions dictionary
This descriptor contains description in alternative languages.

```webidl
dictionary AlternativeDescriptions {
  DOMString *IETFLanguageCodes-members...;
};
```

3.11.1 Dictionary AlternativeDescriptions Members

- ***IETFLanguageCodes-members...** of type DOMString
  IETF language codes ([RFC5646]), defined by a primary language subtag, followed by a region subtag based on a two-letter country code from [ISO3166] alpha-2 (usually written in upper case), e.g: Austrian-German - “de-AT”. In case of absence of the specific territorial language definition, vendor should fallback to the more general language option, e.g: If "de" is given, but "de-AT" is missing, the use "de" entry instead.
Description values can contain any UTF-8 characters.

For example: { "ru-RU": "Пример U2F аутентификатора от FIDO Alliance", "fr-FR": "Exemple U2F authenticator de FIDO Alliance" }

Each description SHALL NOT exceed a maximum length of 200 characters.

4. Metadata Keys

This section is normative.

```webidl
dictionary MetadataStatement {
    DOMString legalHeader;
    AAID aaid;
    AAGUID aaguid;
    DOMString[] attestationCertificateKeyIdentifiers;
    required DOMString description;
    required Version[] upv;
    required DOMString assertionScheme;
    required DOMString publicKeyAlgAndEncoding;
    required DOMString publicKeyAlgAndEncodings;
    required DOMString attestationTypes;
    required Version[] usv;
    required boolean isSecondFactorOnly;
    required DOMString tcDisplay;
    DOMString tcDisplayContentType;
    DisplayPNGCharacteristicsDescriptor[] tcDisplayPNGCharacteristics;
    required DOMString[] attestationRootCertificates;
    EcdaaTrustAnchor[] ecdaaTrustAnchors;
    required DOMString icon;
    ExtensionDescriptor[] supportedExtensions;
};
```

4.1 Dictionary MetadataStatement Members

**legalHeader** of type DOMString

The legalHeader, if present, contains a legal guide for accessing and using metadata, which itself MAY contain URL(s) pointing to further information, such as a full Terms and Conditions statement.

**aaid** of type AAID

The Authenticator Attestation ID. See [UAFProtocol] for the definition of the AAID structure. This field MUST be set if the authenticator implements FIDO UAF.

**NOTE**

FIDO UAF Authenticators support AAID, but they don't support AAGUID.

It is always expected that the UAF Authenticator (or at least the UAF ASM) knows and provides the correct AAID.

**aaguid** of type AAGUID

The Authenticator Attestation GUID. See [FIDOKeyAttestation] for the definition of the AAGUID structure. This field MUST be set if the authenticator implements FIDO 2.

**NOTE**

FIDO 2 Authenticators support AAGUID, but they don't support AAID.
attestationCertificateKeyIdentifiers of type array of DOMString
A list of the attestation certificate public key identifiers encoded as hex string. This value **MUST** be calculated according to method 1 for computing the keyIdentifier as defined in [RFC5280] section 4.2.1.2. The hex string **MUST NOT** contain any non-hex characters (e.g. spaces). All hex letters **MUST** be lower case. This field **MUST** be set if neither aaid nor aaguid are set. Setting this field implies that the attestation certificate(s) are dedicated to a single authenticator model.

All attestationCertificateKeyIdentifier values should be unique within the scope of the Metadata Service.

**NOTE**
FIDO U2F Authenticators typically do not support AAID nor AAGUID, but they use attestation certificates dedicated to a single authenticator model.

description of type required DOMString
A human-readable, short description of the authenticator, in English.

**NOTE**
This description should help an administrator configuring authenticator policies. This description might deviate from the description returned by the ASM for that authenticator.

This description **SHALL NOT** exceed a maximum length of 200 characters.

alternativeDescriptions of type AlternativeDescriptions
A list of human-readable short descriptions of the authenticator in different languages.

authenticatorVersion of type required unsigned short
Earliest (i.e. lowest) trustworthy authenticatorVersion meeting the requirements specified in this metadata statement.

Adding new StatusReport entries with status UPDATE_AVAILABLE to the metadata TOC object [FIDOMetadataService] **MUST** also change this authenticatorVersion if the update fixes severe security issues, e.g. the ones reported by preceding StatusReport entries with status code USER_VERIFICATION_BYPASS, ATTESTATION_KEY_COMPROMISE, USER_KEY_REMOTE_COMPROMISE, USER_KEY_PHYSICAL_COMPROMISE, REVOKED.

It is **RECOMMENDED** to assume increased risk if this version is higher (newer) than the firmware version present in an authenticator. For example, if a StatusReport entry with status USER_VERIFICATION_BYPASS or USER_KEY_REMOTE_COMPROMISE precedes the UPDATE_AVAILABLE entry, than any firmware version lower (older) than the one specified in the metadata statement is assumed to be vulnerable.

protocolFamily of type DOMString
The FIDO protocol family. The values "uaf", "u2f", and "fido2" are supported. If this field is missing, the assumed protocol family is "uaf". Metadata Statements for U2F authenticators **MUST** set the value of protocolFamily to "u2f" and FIDO 2.0/WebAuthentication Authenticator implementations **MUST** set the value of protocolFamily to "fido2".

upv of type array of required Version
The FIDO unified protocol version(s) (related to the specific protocol family) supported by this authenticator. See [UAFProtocol] for the definition of the Version structure.

assertionScheme of type required DOMString
The assertion scheme supported by the authenticator. Must be set to one of the enumerated strings defined in the FIDO UAF Registry of Predefined Values [UAFRegistry], or to "U2FV1BIN" in the case of the U2F raw message format, or to "FIDOV2" in the case of the FIDO 2/WebAuthentication assertion scheme.

authenticationAlgorithm of type required unsigned short
The preferred authentication algorithm supported by the authenticator. Must be set to one of the ALG_ constants defined in the FIDO Registry of Predefined Values [FIDORegistry]. This value **MUST** be non-zero.

authenticationAlgorithms of type array of unsigned short
The list of authentication algorithms supported by the authenticator. Must be set to the complete list of the
supported ALG constants defined in the FIDO Registry of Predefined Values [FIDORegistry] if the authenticator supports multiple algorithms. Each value MUST be non-zero.

### NOTE

FIDO UAF Authenticators
For verification purposes, the field `SignatureAlgAndEncoding` in the FIDO UAF authentication assertion [UAFAuthnrCommands] should be used to determine the actual signature algorithm and encoding.

FIDO U2F Authenticators
FIDO U2F only supports one signature algorithm and encoding:
**ALG_SIGN_SECP256R1_ECDSA_SHA256_RAW** [FIDORegistry].

### publicKeyAlgAndEncoding of type required unsigned short

The preferred public key format used by the authenticator during registration operations. Must be set to one of the **ALG_KEY** constants defined in the FIDO Registry of Predefined Values [FIDORegistry]. Because this information is not present in APIs related to authenticator discovery or policy, a FIDO server MUST be prepared to accept and process any and all key representations defined for any public key algorithm it supports. This value MUST be non-zero.

### publicKeyAlgAndEncodings of type array of unsigned short

The list of public key formats supported by the authenticator during registration operations. Must be set to the complete list of the supported **ALG_KEY** constants defined in the FIDO Registry of Predefined Values [FIDORegistry] if the authenticator model supports multiple encodings. Because this information is not present in APIs related to authenticator discovery or policy, a FIDO server MUST be prepared to accept and process any and all key representations defined for any public key algorithm it supports. Each value MUST be non-zero.

### NOTE

FIDO UAF Authenticators
For verification purposes, the field `PublicKeyAlgAndEncoding` in the FIDO UAF registration assertion [UAFAuthnrCommands] should be used to determine the actual encoding of the public key.

FIDO U2F Authenticators
FIDO U2F only supports one public key encoding: **ALG_KEY_ECC_X962_RAW** [FIDORegistry].

### attestationTypes of type array of required unsigned short

The supported attestation type(s). (e.g. **ATTESTATION_BASIC_FULL(0x3E07)**, **ATTESTATION_BASIC_SURROGATE(0x3E08)**).

See section 3.6.3 of FIDO Registry [FIDORegistry] for all available attestation formats

### userVerificationDetails of type array of required VerificationMethodANDCombinations

A list of alternative VerificationMethodANDCombinations. Each of these entries is one alternative user verification method. Each of these alternative user verification methods might itself be an "AND" combination of multiple modalities.

All effectively available alternative user verification methods MUST be properly specified here. A user verification method is considered effectively available if this method can be used to either:

- enroll new verification reference data to one of the user verification methods

  or

- unlock the UAuth key directly after successful user verification

### keyProtection of type required unsigned short

A 16-bit number representing the bit fields defined by the **KEY_PROTECTION** constants in the FIDO Registry of Predefined Values [FIDORegistry].

This value MUST be non-zero.

### NOTE
The keyProtection specified here denotes the effective security of the attestation key and Uauth private key and the effective trustworthiness of the attested attributes in the “sign assertion”. Effective security means that key extraction or injecting malicious attested attributes is only possible if the specified protection method is compromised. For example, if keyProtection=TEE is stated, it shall be impossible to extract the attestation key or the Uauth private key or to inject any malicious attested attributes without breaking the TEE.

**isKeyRestricted** of type boolean

This entry is set to **true**, if the Uauth private key is restricted by the authenticator to only sign valid FIDO signature assertions.

This entry is set to **false**, if the authenticator doesn't restrict the Uauth key to only sign valid FIDO signature assertions. In this case, the calling application could potentially get any hash value signed by the authenticator.

If this field is missing, the assumed value is isKeyRestricted=**true**.

**NOTE**

Note that only in the case of isKeyRestricted=**true**, the FIDO server can trust a signature counter or transaction text to have been correctly processed/controlled by the authenticator.

**isFreshUserVerificationRequired** of type boolean

This entry is set to **true**, if Uauth key usage always requires a fresh user verification.

If this field is missing, the assumed value is isFreshUserVerificationRequired=**true**.

This entry is set to **false**, if the Uauth key can be used without requiring a fresh user verification, e.g. without any additional user interaction, if the user was verified a (potentially configurable) caching time ago.

In the case of isFreshUserVerificationRequired=**false**, the FIDO server **MUST** verify the registration response and/or authentication response and verify that the (maximum) caching time (sometimes also called "authTimeout") is acceptable.

This entry solely refers to the user verification. In the case of transaction confirmation, the authenticator **MUST** always ask the user to authorize the specific transaction.

**NOTE**

Note that in the case of isFreshUserVerificationRequired=**false**, the calling App could trigger use of the key without user involvement. In this case it is the responsibility of the App to ask for user consent.

**matcherProtection** of type required unsigned short

A 16-bit number representing the bit fields defined by the MATCHER_PROTECTION constants in the FIDO Registry of Predefined Values [FIDORegistry].

This value **MUST** be non-zero.

**NOTE**

If multiple matchers are implemented, then this value must reflect the weakest implementation of all matchers.

The matcherProtection specified here denotes the effective security of the FIDO authenticator’s user verification. This means that a false positive user verification implies breach of the stated method. For example, if matcherProtection=TEE is stated, it shall be impossible to trigger use of the Uauth private key when bypassing the user verification without breaking the TEE.

**cryptoStrength** of type unsigned short

The keyProtection specified here denotes the effective security of the attestation key and Uauth private key and the effective trustworthiness of the attested attributes in the “sign assertion”. Effective security means that key extraction or injecting malicious attested attributes is only possible if the specified protection method is compromised. For example, if keyProtection=TEE is stated, it shall be impossible to extract the attestation key or the Uauth private key or to inject any malicious attested attributes without breaking the TEE.
The authenticator’s overall claimed cryptographic strength in bits (sometimes also called security strength or security level). This is the minimum of the cryptographic strength of all involved cryptographic methods (e.g. RNG, underlying hash, key wrapping algorithm, signing algorithm, attestation algorithm), e.g. see [FIPS180-4], [FIPS186-4], [FIPS198-1], [SP800-38B], [SP800-38C], [SP800-38D], [SP800-38F], [SP800-90C], [SP800-90ar1], [FIPS140-2] etc.

If this value is absent, the cryptographic strength is unknown. If the cryptographic strength of one of the involved cryptographic methods is unknown the overall claimed cryptographic strength is also unknown.

**operatingEnv** of type DOMString
Description of the particular operating environment that is used for the Authenticator. These are specified in [FIDORestrictedOperatingEnv].

**attachmentHint** of type required unsigned long
A 32-bit number representing the bit fields defined by the ATTACHMENT_HINT constants in the FIDO Registry of Predefined Values [FIDORegistry].

**NOTE**
The connection state and topology of an authenticator may be transient and cannot be relied on as authoritative by a relying party, but the metadata field should have all the bit flags set for the topologies possible for the authenticator. For example, an authenticator instantiated as a single-purpose hardware token that can communicate over bluetooth should set ATTACHMENT_HINT_EXTERNAL but not ATTACHMENT_HINT_INTERNAL.

**isSecondFactorOnly** of type required boolean
Indicates if the authenticator is designed to be used only as a second factor, i.e. requiring some other authentication method as a first factor (e.g. username+password).

**tcDisplay** of type required unsigned short
A 16-bit number representing a combination of the bit flags defined by the TRANSACTION_CONFIRMATION_DISPLAY constants in the FIDO Registry of Predefined Values [FIDORegistry].

This value **MUST** be 0, if transaction confirmation is not supported by the authenticator.

**NOTE**
The tcDisplay specified here denotes the effective security of the authenticator’s transaction confirmation display. This means that only a breach of the stated method allows an attacker to inject transaction text to be included in the signature assertion which hasn’t been displayed and confirmed by the user.

**tcDisplayContentType** of type DOMString
Supported MIME content type [RFC2049] for the transaction confirmation display, such as text/plain or image/png.

This value **MUST** be present if transaction confirmation is supported, i.e. tcDisplay is non-zero.

**tcDisplayPNGCharacteristics** of type array of DisplayPNGCharacteristicsDescriptor
A list of alternative DisplayPNGCharacteristicsDescriptor. Each of these entries is one alternative of supported image characteristics for displaying a PNG image.

This list **MUST** be present if PNG-image based transaction confirmation is supported, i.e. tcDisplay is non-zero and tcDisplayContentType is image/png.

**attestationRootCertificates** of type array of required DOMString
Each element of this array represents a PKIX [RFC5280] X.509 certificate that is a valid trust anchor for this authenticator model. Multiple certificates might be used for different batches of the same model. The array does not represent a certificate chain, but only the trust anchor of that chain. A trust anchor can be a root certificate, an intermediate CA certificate or even the attestation certificate itself.

Each array element is a base64-encoded (section 4 of [RFC4648]), DER-encoded [ITU-X690-2008] PKIX certificate value. Each element **MUST** be dedicated for authenticator attestation.

**NOTE**
Either

1. the manufacturer attestation trust anchor

    or

2. the trust anchor dedicated to a specific authenticator model

    MUST be specified.

In the case (1), the trust anchor certificate might cover multiple authenticator models. In this case, it must be possible to uniquely derive the authenticator model from the Attestation Certificate. When using AAID or AAGUID, this can be achieved by either specifying the AAID or AAGUID in the attestation certificate using the extension id-fido-gen-ce-aaid { 1 3 6 1 4 1 45724 1 1 1 } or id-fido-gen-ce-aaguid { 1 3 6 1 4 1 45724 1 1 4 } or - when neither AAID nor AAGUID are defined - by using the attestationCertificateKeyIdentifier method.

In the case (2) this is not required as the trust anchor only covers a single authenticator model.

When supporting surrogate basic attestation only (see [UAFProtocol], section “Surrogate Basic Attestation”), no attestation trust anchor is required/used. So this array MUST be empty in that case.

ecdaaTrustAnchors of type array of EcdaaTrustAnchor

A list of trust anchors used for ECDAA attestation. This entry MUST be present if and only if attestationType includes ATTESTATION_ECDAA. The entries in attestationRootCertificates have no relevance for ECDAA attestation. Each ecdaaTrustAnchor MUST be dedicated to a single authenticator model (e.g as identified by its AAID/AAGUID).

icon of type DOMString


supportedExtensions[] of type ExtensionDescriptor

List of extensions supported by the authenticator.

5. Metadata Statement Format

This section is non-normative.

NORMATIVE

A FIDO Authenticator Metadata Statement is a document containing a JSON encoded dictionary MetadataStatement.

5.1 UAF Example

Example of the metadata statement for an UAF authenticator with:

- authenticatorVersion 2.
- Fingerprint based user verification allowing up to 5 registered fingers, with false acceptance rate of 0.002% and rate limiting attempts for 30 seconds after 5 false trials.
- Authenticator is embedded with the FIDO User device.
- The authentication keys are protected by TEE and are restricted to sign valid FIDO sign assertions only.
- The (fingerprint) matcher is implemented in TEE.
- The Transaction Confirmation Display is implemented in a TEE.
- The Transaction Confirmation Display supports display of “image/png” objects only.
- Display has a width of 320 and a height of 480 pixel. A bit depth of 16 bits per pixel offering True Color (=Color Type 2). The zlib compression method (0). It doesn't support filtering (i.e. filter type of=0) and no interlacing support.
The Authenticator can act as first factor or as second factor, i.e. isSecondFactorOnly = false.

It supports the "UAFV1TLV" assertion scheme.

It uses the [ALG_SIGN_SECP256R1_ECDSA_SHA256_RAW](#) authentication algorithm.

It uses the [ALG_KEY_ECC_X962_RAW](#) public key format (0x100=256 decimal).

It only implements the [ATTESTATION_BASIC_FULL](#) method (0x3E07=15879 decimal).

It implements UAF protocol version (upv) 1.0 and 1.1.

---

**EXAMPLE 1: MetadataStatement for UAF Authenticator**

```json
{
  "description": "FIDO Alliance Sample UAF Authenticator",
  "aaid": "1234#5678",
  "alternativeDescriptions": {
    "ru-RU": "Пример UAF аутентификатора от FIDO Alliance",
    "fr-FR": "Exemple UAF authenticateur de FIDO Alliance"
  },
  "authenticatorVersion": 2,
  "upv": [
    { "major": 1, "minor": 0 },
    { "major": 1, "minor": 1 }
  ],
  "assertionScheme": "UAFV1TLV",
  "authenticationAlgorithm": 1,
  "publicKeyAlgAndEncoding": 256,
  "attestationTypes": [15879],
  "userVerificationDetails": {
    "userVerification": 2,
    "baDesc": {
      "selfAttestedFAR": 0.00002,
      "maxRetries": 5,
      "blockSlowdown": 30,
      "maxTemplates": 5
    }
  },
  "keyProtection": 6,
  "isKeyRestricted": true,
  "matcherProtection": 2,
  "cryptoStrength": 128,
  "operatingEnv": "TEEs based on ARM TrustZone HW",
  "attachmentHint": "Y",
  "tcDisplay": 5,
  "tcDisplayContentType": "image/png",
  "tcDisplayPNGCharacteristics": {
    "width": 320,
    "height": 480,
    "bitDepth": 16,
    "colorType": 2,
    "compression": 0,
    "filter": 0,
    "interlace": 0
  },
  "attachmentRootCertificates": [
    "MIICPTCCAcAgAwIBAgUAOuevU3Oy2wMAoGCCqGSM49BAMCMxIDAeBgNVBAMMD1NhbXBlZnBo
    HlRvIB3oBsb290MRywFAYDVQQKDA1GSURpIIEFabGi8mbmNl
    MREwDwYDVQQDAhVQUYgVFdHLEsMBAGA1UEBwQwJYQgMBAGA1UEChRBQXV0aDBETQIB
    DAJDBMTQ5MBMGJ1UdIQAQQwEAoGCygGCSqGCCqGSM49AgEoBQcQBgNVBAM[MhBh
    d1Yp
    "iVBORw0KGgoAAAANSUhEUgAAAE8AAAAYCAYAAAAwHh/1CGgAAAAASUVORK5CYII="
  }
}
```
Example of an **User Verification Methods** entry for an authenticator with:

- Fingerprint based user verification method, with:
  - the ability for the user to enroll up to 5 fingers (reference data sets) with a false acceptance rate of 1 in 50000 (0.002%) per finger. This results in a FAR of 0.01% (0.0001).
  - The fingerprint verification will be blocked after 5 unsuccessful attempts.
- A PIN code with a minimum length of 4 decimal digits has to be set-up as alternative verification method.
  - Entering the PIN into the authenticator will be required to re-activate fingerprint based user verification after it has been blocked.

**5.2 U2F Example**

Example of the metadata statement for an U2F authenticator with:

- authenticatorVersion 2.
- Touch based user presence check.
- Authenticator is a USB pluggable hardware token.
- The authentication keys are protected by a secure element.
- The user presence check is implemented in the chip.
- The Authenticator is a pure second factor authenticator.
- It supports the "U2FV1BIN" assertion scheme.
- It uses the **ALG_SIGN_SECP256R1_ECDSA_SHA256_RAW** authentication algorithm.
- It implements the **ATTESTATION_BASIC_FULL** method (0x3E07=15879 decimal).
- It implements U2F protocol version 1.0 only.

```json
884zu9NdlnOTZJP2n3oN+++r893h3veBxB+xPcZjIkTUVbBmplUdWbVbTlmpcCZsVzLXd9X905s1k9vbb5af59g9++er541q7aPl1Vv95lyVuNI8ilid5kGTe30nFv7a9in7QZP7nvdby4s2er1U2XMQ
Udy8+xZaaNmGimEbyXN3RUDzat1an180f7uovz+0C7TaW2dpw2v+jom1bEvey6c4i5p UMGMVEw0e50q2q7
dtuW1lfub4eW0yPfFNhlow1751mN2LyP3hWVzf66Lilq817FR9YFSx5smSeb6ooeOGByY7
MNUocGp8z2mNe9f9UaaV+VJX99sdzDCSypkZHMtZg9x7bLHcMnThb16euj+mViQqfyaUAZGNg64i
Xz-0/k6iuOZF0OoTatdWKXnRQ99981R5OFInkJn0tUqI03qNnI+Ml+98bk6B77W7wZpcPc+
0zg4YlYrUd6E6eGdBjUmbVpccsearligYGRkbin2zVR+jChzioL7550jedLExopWoAp2U2XJu
e7JLrVsvQsU81zk0PFeemMRyVvXuQx7PbDQ5YsJvsoNf1+IVYH6lxts3loh0b+jmRyq6ouaYVe
rW/WYjpcbcwMmE82twqWf1rA4j+SH131FY4osZmXspq7rDx1QhxkJK+iRsWk1dg7Tu6v
8tJUmbWlpFkrw1UG05q13zlewmB8zQc17+B8aw7K8IEK5q5zYeark6A87P93GZCdk++nd3DQow+6UC
85SVN92u38t7MnT0xV1CvBqRgw4psmbd3b2uDe7Yr4BxQqfvpvqUfJQFNTQ22fDvUVT6bT
JKF5dSmruLdagdqm4S9pmsD1Jr3G6ToH0w9aV7LWLHYXkIITD0LTAltYlaamp1QjOw++uyGUXV
djDNvXsXm+b1Qripl84d4bX1LP1Od169tsodv5shGre9x980+plLr1chGHNT6D57C9KMWXeJdO
Z94bb9c9c1RoN57tT1HmMqv1bo3gG9dDvYkv3WQBBh2zK35YKNd0c08a366DZFGkXaLsEjP5
rdPib98p8Cis/m'TvuS0r9GQ4n6kPoZn3UJu0mzZ2yP1fmUX+o5Gq6qbV+1mz+SuYNVq77
WbdI6lVvjiLopCpXLP+2QtvQ7vIL1vmlS5dbG2so5y6q76Tdj+jqzpaV9BQcee*NJy6v6tK
9cw1LoST7TF1hD3M3b92y7h3Tnx5oz6969lLPYWuAwq5n62q7cecbfeYYaRePe3F1Ubj1knSw
ZXHmMcNYqOaGu7U0ISCM5opqQ2HFXPF7eXaX5yY911Y1eCep4m0zoh+11G3sD4T17x8wyj8nw
btev26V0Gbd7+7H4zXKudAH537FjpyozOhdj1nEuzmXwJrOObvMNvWn9hwy xs2aVsWtC8+48aLeap
E7p5wKzi0A2Q9R5n4R4e+uJc+b61kApo9nBxgmd/4V5QP/mt18HDC7ssHftmee5lhimhV0m/ALX2
3b2q46F1nx7v1Cw2UfOlB8QqemxmUji9Quyjupd3YD6abWBBBMrh+apNbOKrNF1+uagCa4ri
XGlwMPPrVaihUyMQMAANuUbIR70L70YoSeOaOdE88ApsXFg3f30nyUjMc1U6NV9EzgvpvHBFUy
lvarePiwJ3sd5F5ZTz7nEnE9g95NuU2uJ2Wpr4omnkn4X4zhFtVod8vNhznqOgldilGvAS6Du
eZeW078AAQ06cE6x+nv5VijqyvQNYDPOOLUwIakShnxAXLkH4yr4yGIMYDc1wF5Ta3h19OJOCuhr
UJ1J6in6e8eYd4Bpocr+-yj61G1HNPlM4D5jU+SfG6HrRDSBnAYLgMuYMszKpb70kncPIPO8
H9wPlLZ1N5kX4c1wQDUmzXYeZ6hczkYtVrYEB4YQDZrYclurmlmpHekk72zaFKyQAZhGQu1
z+85NFpWXPDr3xv10XqgpQ6BezNBoBk6n5k4nbebRh+k1hwXTFD0D1EyWUsn5vdgQpXazcuCe00i
sHIO2NQ8a0omxX12La3m609w9k+wLNTMY86PM0y9jisO5m76PWqOg9+DZuKynA56msZf5WWSy
5qVA1rwUyQjXalznkia/9hHS7D7KykYhogAAAABJRUS3Ejkjggg="}
```
EXAMPLE 3: MetadataStatement for U2F Authenticator

```json
{
   "description": "FIDO Alliance Sample U2F Authenticator",
   "alternativeDescriptions": {
      "ru-RU": "Пример U2F аутентификатор от FIDO Alliance",
      "fr-FR": "Exemple U2F authenticator de FIDO Alliance",
      "zh-CN": "FIDO Alliance U2F"
   },
   "attestationCertificateKeyIdentifiers": ["7c0903708b87115b0b422def3138c3b64e44573"],
   "protocolFamily": "u2f",
   "authenticatorVersion": 2,
   "upv": [2]
}
```

---

**Key Protection:** 10

**Matcher Protection:** 4

**OperatingEnv:** "Secure Element (SE)"

**Attachment Hint:** 2

**Is SecondFactorOnly:** true

**TC Display:** 0

**Attestation Root Certificates:**

```
MIICPTCCAeOgAwIBAgIJAOuexvU3Oy2wMAoGCCqGSM49BAMCMHsxIDAeBgNVBAMM
F1NhXbveZS5BbHdlcicRsdHGiVtbbsb9290MYFyAYFDVQDKDA1GSPUIR/EBwvHGihbmi
NMEwDyYXDSDQALVQ5Y/UFW/dHESMBAGA1UEBwwFZGmybGhvbmd1MCMGgGCSqGSG
1w0dDQQDAjTElMAkGBnVtMVh0dC1T/1/1IcGRkQg07v0A1/9R2n7C7Lb899yX
w7BMT3wAsM4wQDXXV4s03X0s7y/P0LqKt73lW68Z6QYXfAMrH3/2277/0w/s3
MaZ3h3n1US8b8HYQdb8B5pxpQJ/URyX/0NQME4wHQYDVR0DBBEFo4oH3CLcXhF
C01t7z8w8d51aEM/BG7A1UiqDYMBAFPo4oH3CLcXhFbC01t7z8w8d51aEM/BG7A1
A1UdEwQFMFMAABAgwCgYKoZiZoJ0AeA0EIAWTh0QigJ0AeA0EIAWTh0QigJ0AeA0EIA
IQ==
```

**Icon:** data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAE8AAAAvCAYAAACiwJfcAAAAAXNSR0IArs4c6QAAAARnQU1BAACxjwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAAahSURBVGhD7Zr5bxRlGMf9KzTB8AM/YEhE2W7pQZcWKKSbC5HATIELARE7kNECA3KkcK0KSKCKSFSkBvCDVQDNEdsliYdwygjjBriRMCnFc/4wy8

---

**Icon Data:** image/png

---

**Icon Data:** image/png
5.3 FIDO2 Example

Example of the metadata statement for an FIDO2 authenticator with:

- AAGUID is set to 0132d110-bf4e-4208-a403-ab4f5f12efe5.
- authenticatorVersion is set to 2.
- Touch based user presence check.
- Authenticator is a USB pluggable hardware token.
- The authentication keys are protected by a secure element.
- The user presence check is implemented in the chip.
- It supports the "FIDO2" assertion scheme.
- It uses the ALG_SIGN_SECP256R1_ECDSA_SHA256_RAW authentication algorithm.
- It uses the ALG_KEY_COSE public key format (0x104=260 decimal).
- It only implements the ATTESTATION_BASIC_FULL method (0x3E07=15879 decimal).
- It implements FIDO2 protocol version 1.0.
6. Additional Considerations

This section is non-normative.

6.1 Field updates and metadata

Metadata statements are intended to be stable once they have been published. When authenticators are updated in the field, such updates are expected to improve the authenticator security (for example, improve FRR or FAR).

The authenticatorVersion must be updated if firmware updates fixing severe security issues (e.g. as reported previously) are available.

NOTE
The metadata statement is assumed to relate to all authenticators having the same authenticator model identifier (AAID/AAGUID/attestationCertificateKeyIdentifiers).

NOTE
The FIDO Server is recommended to assume increased risk if the authenticatorVersion specified in the metadata statement is newer (higher) than the one present in the authenticator.

NORMATIVE
Significant changes in authenticator functionality are not anticipated in firmware updates. For example, if an authenticator vendor wants to modify a PIN-based authenticator to use “Speaker Recognition” as a user verification method, the vendor MUST assign a new authenticator model identifier (AAID/AAGUID/attestationCertificateKeyIdentifiers) to this authenticator.

NORMATIVE
A single authenticator implementation could report itself as two “virtual” authenticators using different authenticator model identifiers. Such implementations MUST properly (i.e. according to the security characteristics claimed in the metadata) protect UAuth keys and other sensitive data from the other “virtual” authenticator - just as a normal authenticator would do.

NOTE
Authentication keys (UAuth.pub) registered for one authenticator model (e.g. as identified by 0zg4tLrYlUc86E6eGDjIMubVpcusearfgIYGRk6brhZVr/JcHzooul5750jedLExopWcApi2ZUqhu7JLvrVsQU81zkOPeemMRVuyuXq7X7FbpDQ5JvZonfK+1VY8Hluu9530h100b+jmRYg6ouaYVvEe 8nWlWYip8cbWm8M682tWqFw1R4j25SH13lRJU14moZvXpSqd7dxOQxKaPK31+Bwks1K1dTgLhu6V8tqc3Jw8kx4FQO501r3e2vmBZcZq177+BBaw7k8KEK5qzkYeark9A86p7P3GQkD+xnd3DOQw+6UC8SVN8U2uv38im7NtaXVCvRgv4ypsmbdl3bu2De7YfBxXcogpsyPurUFQGTQu2ifDJVT68rTSJKF5dnSmjUjddgq4mSS9pmsdRJ3G6H0H9aW9ALWLYXkilletD0LTLakYlaamp1QVv++uyuGjUV vJ0JDNVXs0+m148xP8ld4tXL1IPOIe08tsoo0v5hGr4ex9ux0o+IplR1coHNTD6Z51C0MWKxeluoZcZ4kbbboqo1fOnS7qT7ZhimMqDvu03gDdDvYKWQ8H2z0fS35XNk0hC03ac861D2FgKaxLsEpj5fdrPgs98LC0s/m7Tv0kx240bKoPo3z0JUoOn22zyP1fmenu+055qSgebVt+1zsuYNxH7qT WdBViLJvplloECLP+2gtQGILr/1vm1s8D8tzsCgZfyu6Tqj+jxyspasV98CQeeyNjvy6kIc 0wicui/S7TH1DPoM8529y7h73Ttx5ozK6HHLPYWuAwaq55c6270e06beYvaReP31FU8zj1knSw ZKHHmmCjY0Ogalo7UQISCM3qQrQr2H/XFP7seXxu45y91ByeCep4m0zoH+i1f3x9241T7x8kwyw8nw b9ev26V8b6d+7H4kXkUnAh537FjyzyOHdJnHEuzmXgyWjxObvNMv27hnywsx2aVexWtCB+48aLeaP E75p5wKz0A0AQ5v5nr4E+u+j0+b6lAqplinxBgmd4/V5Q5pmt18HDC7sFHtmeu5imhV0m/ALX2 32bo4B6Fd7xV11cW52u10bB47qexmnuJj9OtyJupd3YD6abWBBMrh+apnbOKrNF1+uyAC4r XiGmWMPRiavlh5YJOMDAKnUbsR07L0yOSeOadeE88apsXFIfi36nyughUg5I1U0vBNbEzgrnpvHBFUj yVraepxiw5rF0DF2Z7m0EmENe08KJUd2oL2Jwp4Ocmnk/N4x42HfVC OgYDH8vNzuuhNq0dd0u46ADu eZWo78Aa0CMc6Eki+n5vCyCvqNPDypootUawklnXxUlkH4yUgYIMYDtc10WFS5ta13h1POcUhr UJ:JL1IN6C6IerRyDbo0++yJx6b11GINFrM4MD5rJ13F30GHJnD5BarnYUgLMLyMsZkpb70XppoHlsP8 h3W1pLz7NhN1k54XXC1wDGUmYzXYeh6z/cklVtm4EBka9VQGD2rY3rLMpRHEkikk7zaFKYQA2hGQU1 z+z5NFwpXDrk3xv10GpxQ6BeNboB6kn8k4n4ebxrh+k1HwxFt0DF1EYWUs5v+dgQqKaxzudCediO sHI0H2q8ah0mx12A3l309fwi9lwh+wLNTMY/86MOp8y31OxhmT6PWqQ9+DZukYna56sm5s35fWWSy 5q1VAYhlyJqXalmkzkaigHSD7FrtTyilhogAAABJRU5ErkJgg=="}
A References

A.1 Normative references

[ECMA-262]

[FIDOBiometricsRequirements]

[FIDOMetadataService]
R. Lindemann; B. Hill; D. Baghdasaryan. FIDO Metadata Service v1.0 Implementation Draft. URL: https://fidoalliance.org/specs/fido-v2.0-rd-20180702/fido-metadata-service-v2.0-rd-20180702.html

[FIDOREgistry]
R. Lindemann; D. Baghdasaryan; B. Hill. FIDO Registry of Predefined Values Implementation Draft. URL: https://fidoalliance.org/specs/fido-v2.0-rd-20180702/fido-registry-v2.0-rd-20180702.html

[FIDORestrictedOperatingEnv]

[ISO19795-1]

[RFC2049]

[RFC2119]

[RFC2397]

[RFC4122]

[UAFProtocol]

[WebIDL-ED]

A.2 Informative references

[AndroidUnlockPattern]
Android Unlock Pattern Security Analysis. Published. URL: http://www.sinustrom.info/2012/05/21/android-unlock-pattern-security-analysis/

[FIDOEdcdaaAlgorithm]

[FIDOglossary]

[FIDOKeyAttestation]
FIDO 2.0: Key attestation format. URL: https://fidoalliance.org/specs/fido-v2.0-ps-20150904/fido-key-attestation-v2.0-ps-20150904.html

[FIPS140-2]

[FIPS180-4]