FIDO U2F Authenticator Transports Extension

FIDO Alliance Proposed Standard 11 April 2017

This version:
> https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-authenticator-transports-v1.1-v1.2-ps-20170411.html

Editors:
> Juan Lang, Google, Inc.
> Robin Bertels, STMicroelectronics
> Alexei Czeskis, Google, Inc.

The English version of this specification is the only normative version. Non-normative translations may also be available.

Abstract

FIDO-compliant relying parties may wish to offer tailored user interfaces based on the transports a FIDO U2F authenticator supports. This standard describes one way relying parties may learn which transports an authenticator supports, by allowing authenticator vendors to embed hardware features as an optional extension in the authenticator's attestation certificate.

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 Proposed Standard. 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.

This document has been reviewed by FIDO Aliance Members and is endorsed as a Proposed Standard. It is a stable document and may be used as reference material or cited from another document. FIDO Alliance's role in making the Recommendation is to draw attention to the specification and to promote its widespread deployment.

Table of Contents

1. Document Information

1.1 Notation

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

1.1.1 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. Attestation certificates

Attestation certificates are X.509 certificates. Transports supported by an authenticator can be embedded as an extension in the authenticator's attestation certificate. As certificate extensions are only available since [X509V3], the attestation certificate's version must be v3.

As such, this specification is a profile of [RFC5280] which is itself a profile of the ISO/IEC/ITU-T [X509V3] specifications for public key certificates. All syntax and semantics are inherited from those specifications unless explicitly documented otherwise. In this document, all fields are defined in ASN.1 and must be DER-encoded ([X690]).

3. FIDO U2F extensions

3.1 FIDO U2F OID arc

The FIDO OID arc and its FIDO U2F OID subarc are defined as:

```
-- FIDO Alliance's OID
id-fido OBJECT IDENTIFIER ::= 1.3.6.1.4.1.45724

-- FIDO U2F protocol OID
id-fido-u2f OBJECT IDENTIFIER ::= { id-fido 2 }
```

3.2 FIDO U2F certificate extensions

The FIDO U2F certificate extensions arc is defined as:

```
-- FIDO U2F certificate extensions arc
id-fido-u2f-ce OBJECT IDENTIFIER ::= { id-fido-u2f 1 }
```

3.2.1 FIDO U2F certificate transports extension

This extension is identified by `id-fido-u2f-ce-transports` and specifies the transports supported by the authenticator. It's a non-critical extension and therefore FIDO clients and relying parties may ignore it, if present.

The FIDO U2F certificate transports extension is defined as:

```
-- FIDO U2F certificate extensions
id-fido-u2f-ce-transports OBJECT IDENTIFIER ::= { id-fido-u2f-ce 1 }

fidoU2FTransports EXTENSION ::= {
  WITH SYNTAX FIDOU2FTransports
  ID id-fido-u2f-ce-transports
}

FIDOU2FTransports ::= BIT STRING {
  bluetoothRadio(0), -- Bluetooth Classic
  bluetoothLowEnergyRadio(1),
  uSB(2),
  nFC(3),
  uSBInternal(4)
}
```

3.3 Examples

3.3.1 BT classic authenticator

EXAMPLE 1

```
SEQUENCE                                    30 13
  OBJECT IDENTIFIER                           06 0B
    value: id-fido-u2f-ce-transports            2B 06 01 04 01 82 E5 1C 02 01 01
  OCTET STRING                                04 04
    BIT STRING                                  03 02
      unused bits: 7                              07
      value: 0x80                                 80
```

3.3.2 USB + NFC authenticator

EXAMPLE 2

```
SEQUENCE                                    30 13
  OBJECT IDENTIFIER                           06 0B
    value: id-fido-u2f-ce-transports            2B 06 01 04 01 82 E5 1C 02 01 01
```

```
      OCTET STRING                          04 04
        BIT STRING                            03 02
          unused bits: 4                         04
          value: 0x30                            30
```

A. References

A.1 Normative references

[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

[RFC5280]
D. Cooper; S. Santesson; S. Farrell; S. Boeyen; R. Housley; W. Polk.*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. May 2008. Proposed Standard. URL: https://tools.ietf.org/html/rfc5280

[X509V3]
ITU-T Recommendation X.509 version 3 (1997). "Information Technology - Open Systems Interconnection - The Directory Authentication Framework" ISO/IEC 9594-8:1997.. URL:undefined

[X690]
Recommendation X.690 — Information Technology — ASN.1 Encoding Rules — Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER), and Distinguished Encoding Rules (DER). URL:https://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf