Abstract

The FIDO U2F framework was designed to be able to support multiple authenticator form factors. This document describes the communication protocol with authenticators over Near Field Communication (NFC).

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.
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].

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

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. Protocol

The general protocol between a FIDO client and authenticator over NFC is as follows:

1. Client sends an applet selection command
2. Authenticator replies with success
3. Client sends a command for an operation (register / authenticate)
4. Authenticator replies with response data or error

The Authenticator must reply to all commands within 800ms.

3. Framing

The NFC protocol shall not use any additional framing (unlike the USB HID protocol, for
example). Instead, messages sent to an NFC authenticator shall follow the U2F raw message format as defined in [U2FRawMsgs] in the bibliography. In the NFC protocol, either short or extended length APDU encoding is allowed.

4. APDU Length

Some responses may not fit into a short APDU response. For this reason, U2F authenticators must respond in the following way:

- If the request was encoded using extended length APDU encoding, the authenticator must respond using the extended length APDU response format.
- If the request was encoded using short APDU encoding, the authenticator must respond using ISO 7816-4 APDU chaining (see Section A.4). See below for an example:

  Authenticator
  
  | CL IN P1 P2 Lc | Le |
  | 00 01 03 00 40 | [payload] 00 |

  Partial Response 1
  
  | CL IN P1 P2 Le |
  | 00 c0 00 00 00 |

  DATA | S1 S2 |
  [256 bytes data] 61 00

  Partial Response 2
  
  | CL IN P1 P2 Le |
  | 00 c0 00 00 AC |

  DATA | S1 S2 |
  [256 bytes data] 61 AC

  Final Response
  
  | CL IN P1 P2 Le |
  | 00 c0 00 00 AC |

  DATA | S1 S2 |
  [172 bytes data] 90 00

  Register Request
  
  | GET Response for 256 bytes |
  
  | GET Response for 172 bytes |

5. Applet selection

A FIDO client shall always send an applet selection command to begin interaction with a FIDO authenticator via NFC. The structure of the applection command shall follow the same APDU structure as in the raw message format mentioned above.

The FIDO U2F AID consists of the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RID</td>
<td>0xA000000647</td>
</tr>
<tr>
<td>AC</td>
<td>0x2F</td>
</tr>
<tr>
<td>AX</td>
<td>0x0001</td>
</tr>
</tbody>
</table>

As a result, the command for selecting the applet using the FIDO U2F AID is:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLA</td>
<td>0x00</td>
</tr>
<tr>
<td>INS</td>
<td>0xA4</td>
</tr>
<tr>
<td>P1</td>
<td>0x04</td>
</tr>
</tbody>
</table>
In response to the applet selection command, the FIDO authenticator shall reply with its version string in the successful response. In this writing, the version string is "U2F_V2", hence a successful response to the applet selection command would consist of the following bytes:

0x5532465F56329000

Note, future versions may respond with other version string values.

6. Implementation Considerations

Correct and reliable functioning of the NFC U2F authenticator requires a reliable contactless communication between the NFC U2F authenticator and the contactless reader device. However, there are currently several relevant specifications describing the contactless proximity interface often summarized under the term “NFC”.

In order to guarantee interoperability, the contactless interface of the NFC U2F authenticators and the various implementations of contactless readers should follow one of the following standards:

a. NFC U2F authenticators should be designed according to ISO/IEC 14443 or ISO/IEC 18092. These standards are commonly used for FIDO authenticators, eID, passports, public transport fare media etc. It is highly recommended to test and certify the conformance of the authenticator to ISO/IEC 14443 or ISO/IEC 18092 by an independent party.

b. For mobile use of FIDO authentication, the reader functionality of NFC-enabled mobile devices will typically be used for NFC U2F authenticators. Mobile devices should be designed according to NFC Forum Analog specification v2.0 or later. NFC Forum also offers testing and certification.

The testing and certification for the above listed specifications will ensure interoperability of NFC U2F authenticators and NFC mobile devices. Generally, all reader devices that may be used with unspecific types of NFC U2F authenticators (see a.) should be conformant to NFC Forum analog specification.

A. References

A.1 Normative references

[ECMA-262]  

[FIDOglossary]  
PDF: https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-glossary-v1.2-ps-20170411.pdf

[RFC2119]  

[U2FRawMsgs]  
D. Balfanz, FIDO U2F Raw Message Formats v1.0 FIDO Alliance Review Draft (Work
in progress.) URL: https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-
raw-message-formats-v1.2-ps-20170411.pdf

[WebIDL]
Cameron McCormack; Boris Zbarsky; Tobie Langel. Web IDL. 15 December 2016.
W3C Editor's Draft. URL: https://heycam.github.io/webidl/