



IMPLEMENTATION DRAFT

FIDO NFC Protocol Specification v1.0

FIDO Alliance Implementation Draft 14 May 2015

This version:

<https://fidoalliance.org/specs/fido-undefined-undefined-id-20150514/fido-u2f-nfc-protocol-v1.0-undefined-id-20150514.html>

Editors:

Alexei Czeskis, [Google, Inc.](#)
Juan Lang, [Google, Inc.](#)

Copyright © 2014-2015 [FIDO Alliance](#) All Rights Reserved.

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 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 prepared 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](#)
 - 1.1 [Key Words](#)
- 2. [Protocol](#)
- 3. [Framing](#)
- 4. [APDU Length](#)
- 5. [Applet selection](#)
- 6. [Implementation Considerations](#)
- 7. [Bibliography](#)
- A. [References](#)
 - A.1 [Normative 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](#)].

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

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

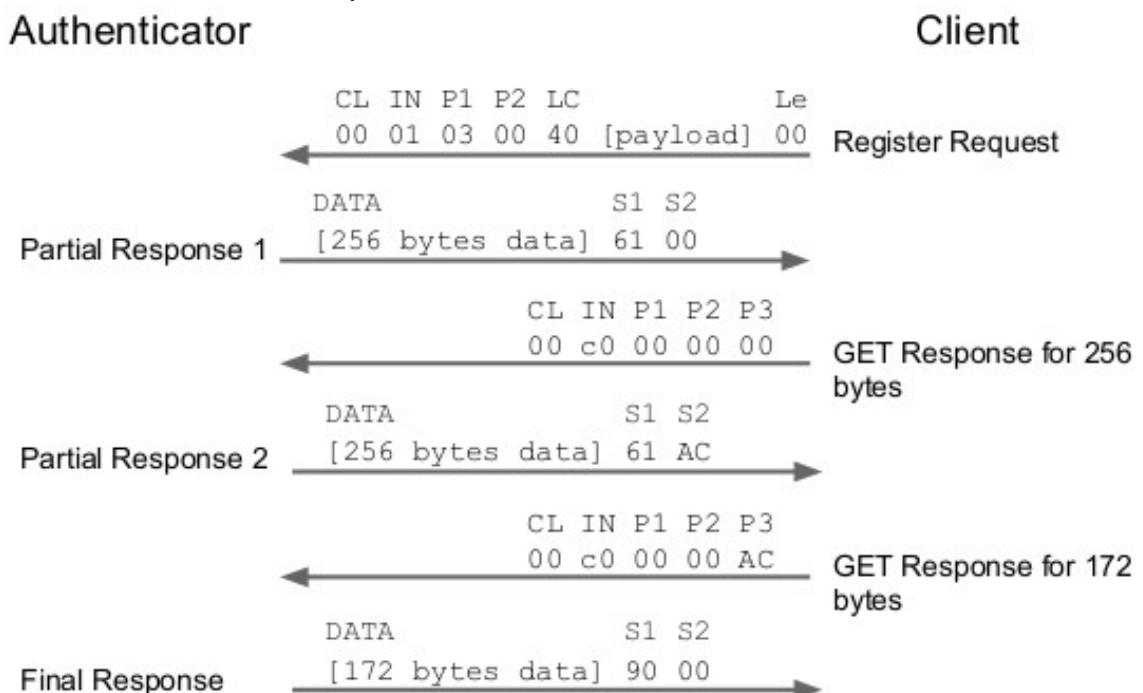
3. Framing

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 [U2FRAWMESSAGES] in the bibliography.

4. APDU Length

Some responses may not fit into a short APDU, for this reason U2F authenticators **MUST** respond in the following way:

- If the request was of extended length (*i.e.*, had 3 length bytes), the authenticator **MUST** respond using the extended length APDU format.
- If the request was not of extended length (*i.e.*, had 1 length byte), the authenticator **MUST** respond using ISO 7816-4 APDU chaining (see Section A.4). See below for an example:



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 applet selection command **SHALL** follow the same APDU structure as in the raw message format mentioned above.

The FIDO U2F AID consists of the following fields:

Field	Value
RID	0xA000000647
AC	0x2F
AX	0x0001

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

Field	Value
CLA	0x00
INS	0xA4
P1	0x04
P2	0x00
LEN	0x08
DATA	0xA0000006472F0001

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

6. Implementation Considerations

Some NFC authenticators may be passively powered -- drawing all of their power from the NFC field. If the authenticator does not power up quick enough or has insufficient power, a poor user experience is likely to occur.

7. Bibliography

[U2FRAWMESSAGES] Dirk Balfanz, Jakob Ehrensvard. FIDO U2F Raw Message Formats, Aug 2014

A. References

A.1 Normative references

[ECMA-262]

ECMAScript Language Specification, Edition 5.1. June 2011. URL:
<http://www.ecma-international.org/publications/standards/Ecma-262.htm>

[FIDO Glossary]

R. Lindemann, D. Baghdasaryan, B. Hill, J. Hodges, *FIDO Technical Glossary*.
FIDO Alliance Proposed Standard. URLs:
HTML: <fido-glossary.html>
PDF: <fido-glossary.pdf>

[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>

[WebIDL]

Cameron McCormack. *Web IDL*. 19 April 2012. W3C Candidate
Recommendation. URL: <http://www.w3.org/TR/WebIDL/>