FIDO NFC Protocol Specification v1.0

FIDO Alliance Review Draft 15 September 2016

This version:
https://fidoalliance.org/specs/fido-u2f-v1.1-rd-20160915/fido-u2f-nfc-protocol-v1.1-v1.1-rd-20160915.html

Editors:
Alexei Czeskis, Google, Inc.
Juan Lang, Google, Inc.

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 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.

Table of Contents

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 "l" 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

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:
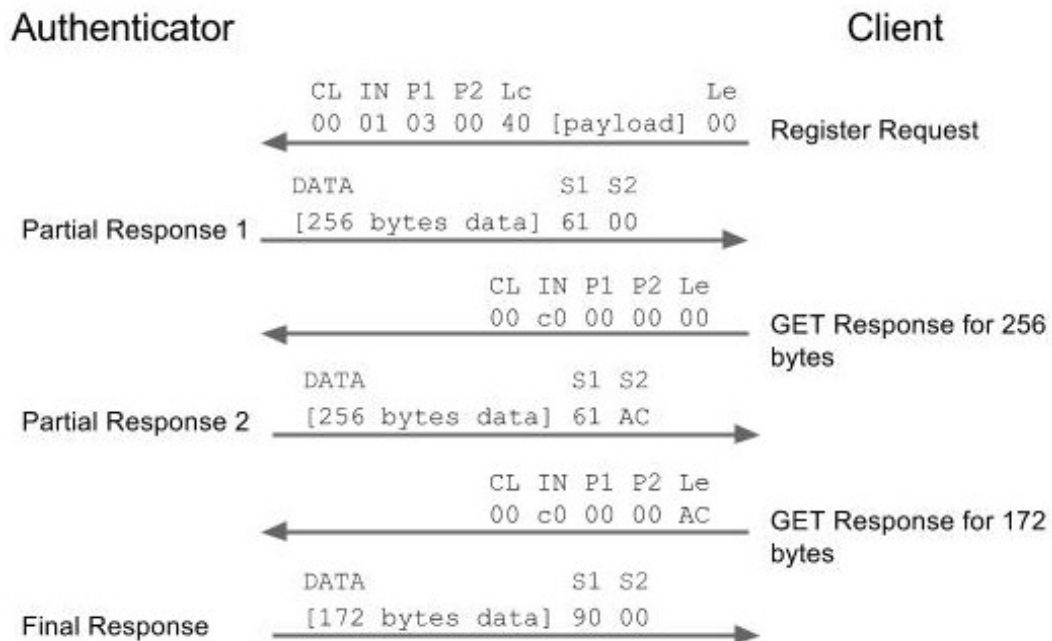
5. Applet selection

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:

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

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]
    ECMAScript Language Specification. URL: https://tc39.github.io/ecma262/
[FIDOGlossary]
    R. Lindemann, D. Baghdasaryan, B. Hill, J. Hodges, *FIDO Technical Glossary*. FIDO Alliance Proposed Standard. URLs:
    HTML: fido-glossary-v1.1-rd-20160915.html
    PDF: fido-glossary-v1.1-rd-20160915.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
[U2FRawMsgs]
    D. Balfanz, *FIDO U2F Raw Message Formats v1.0*. FIDO Alliance Review Draft (Work in progress.) URL: ./fido-u2f-raw-message-formats-v1.1-rd-20160915.pdf
[WebIDL]
    Cameron McCormack; Boris Zbarsky. *WebIDL Level 1*. 15 September 2016. W3C Proposed Recommendation. URL: https://www.w3.org/TR/WebIDL-1/