CTAP 2.1 Errata

Final Document, June 21, 2022

This version:
https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-errata-20220621.html

Issue Tracking:
GitHub

Editor:
FIDO Alliance

Copyright © 2022 FIDO Alliance. All Rights Reserved.

Abstract

The errata document for FIDO Client to Authenticator Protocol v2.1.

Table of Contents

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 an errata to a Proposed Standard Specification.

If you wish to make comments regarding this document, please Contact Us. All comments are welcome.

Implementation of certain elements of the related Specification, including when updated by this errata, 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 this errata and the related 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 ERRATA AND THE RELATED PROPOSED STANDARD FIDO ALLIANCE SPECIFICATION ARE 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.

1. Introduction§

This document contains errata to FIDO Client to Authenticator Protocol v2.1.

2. Section 5. Terminology§

See https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html#sctn-terminology

The definition for NFC under Evidence of user interaction did not sufficienty define a specific error for User Interaction when using an NFC transport.

Original Text

Upon the platform subsequently invoking either authenticatorMakeCredential or authenticatorGetAssertion (e.g., with the "up" option key set to 'true'):

1. If evidence of user interaction is requested then:
    1. If the NFC userPresent flag’s value is `true`, then consider the user as having granted permission, and set the NFC userPresent flag to `false`.
    2. Otherwise, do not consider the user as having granted permission.

Upon expiry of the NFC user presence maximum time limit, the NFC userPresent flag is set to `false` if it is not already `false`.

Corrected Text

Upon the platform subsequently invoking either authenticatorMakeCredential or authenticatorGetAssertion (e.g., with the "up" option key set to 'true'):

1. If evidence of user interaction is requested then:

    1. If the platform sends a zero length pinUvAuthParam then return either CTAP2_ERR_PIN_NOT_SET if PIN is not set or CTAP2_ERR_PIN_INVALID if PIN has been set.

        > Note: This is done for backwards compatibility with CTAP2.0 platforms in the case where multiple authenticators are attached to the platform. In this case the authenticator must not consume the NFC userPresent flag or it will prevent authentication with some CTAP2.0 platforms.

    2. If the NFC userPresent flag's value is `true`, then consider the user as having granted permission, and set the NFC userPresent flag to `false`.
    3. Otherwise, do not consider the user as having granted permission. End the operation by returning CTAP2_ERR_UP_REQUIRED.

Upon expiry of the NFC user presence maximum time limit, the NFC userPresent flag is set to `false` if it is not already `false`.

3. Section 6.4. authenticatorGetInfo (0x04)§

See https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html#authenticatorGetInfo

The text and links for userVerificationMgmtPreview were incorrect.

Original Text

user verification: Indicates that the authenticator supports a built-in user verification method. For example, devices with UI, biometrics fall into this category. If present and set to true, it indicates that the device is capable of built-in user verification and its user verification feature is presently configured.	Not Supported

uv	If present and set to false, it indicates that the authenticator is capable of built-in user verification and its user verification feature is not presently configured. For example, an authenticator featuring a built-in biometric user verification feature that is not presently configured will return this "uv" option id set to false. If absent, it indicates that the authenticator does not have a built-in user verification capability. A device that can only do Client PIN will not return the "uv" option id. If a device is capable of both built-in user verification and Client PIN, the authenticator will return both the "uv" and the "clientPin" option ids.	

Corrected Text

uv	user verification: Indicates that the authenticator supports a built-in user verification method. For example, devices with UI, biometrics fall into this category. If present and set to true, it indicates that the device is capable of built-in user verification and its user verification feature is presently configured. If present and set to false, it indicates that the authenticator is capable of built-in user verification and its user verification feature is not presently configured. For example, an authenticator featuring a built-in biometric user verification feature that is not presently configured will return this "uv" option id set to false. If absent, it indicates that the authenticator does not have a built-in user verification capability. A device that can only do Client PIN will not return the "uv" option id. If a device is capable of both built-in user verification and Client PIN, the authenticator will return both the "uv" and the "clientPin" option ids.	Not Supported

4. Section 6.5.8. PRF values used§

See https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-

20210615.html#prfValues

The description of `authenticatorClientPIN` was removed and new values were added to `authenticatorBioEnrollment` and `authenticatorCredentialManagement`

Original Text

Context	Pattern of PRF argument
authenticatorMakeCredential	32 arbitrary bytes
authenticatorGetAssertion	32 arbitrary bytes
authenticatorClientPIN	32×0xff || `0608` || 32-bit value || CBOR array
authenticatorBioEnrollment	`0101` || CBOR map `0102` || CBOR map `0104` `0105` || CBOR map

authenticatorCredentialManagement	`01`
	`02`
	`04` || CBOR map
	`06` || CBOR map

authenticatorLargeBlobs	32×0xff || `0c00` || 32-bit value || SHA-256(contents of `set` byte string, i.e. *not* including an outer CBOR tag with major type two)
authenticatorConfig	32×0xff || `0d` || 8-bit value || CBOR map

Index§

Terms defined by this specification§