CTAP 2.1 Errata

Final Document, June 21, 2022

This version:

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

1  Introduction

2  Section 5. Terminology

3  Section 6.4. authenticatorGetInfo (0x04)

4  Section 6.5.8. PRF values used

Index
Terms defined by this specification

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
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 sufficiently 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**

<table>
<thead>
<tr>
<th>user verification: Indicates that the authenticator supports a <strong>built-in user verification method</strong>. For example, devices with UI, biometrics fall into this category.</th>
<th>Not Supported</th>
</tr>
</thead>
</table>
| 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.

**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.

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

### Original Text

<table>
<thead>
<tr>
<th>Context</th>
<th>Pattern of PRF argument</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>authenticatorMakeCredential</code></td>
<td>32 arbitrary bytes</td>
</tr>
<tr>
<td><code>authenticatorGetAssertion</code></td>
<td>32 arbitrary bytes</td>
</tr>
<tr>
<td><code>authenticatorClientPIN</code></td>
<td>`32×0xff</td>
</tr>
<tr>
<td><code>authenticatorBioEnrollment</code></td>
<td>`\x0101</td>
</tr>
<tr>
<td></td>
<td>`\x0102</td>
</tr>
<tr>
<td></td>
<td><code>\x0104</code></td>
</tr>
<tr>
<td></td>
<td>`\x0105</td>
</tr>
<tr>
<td><code>authenticatorCredentialManagement</code></td>
<td><code>\x01</code></td>
</tr>
<tr>
<td></td>
<td><code>\x02</code></td>
</tr>
<tr>
<td></td>
<td>`\x04</td>
</tr>
<tr>
<td></td>
<td>`\x06</td>
</tr>
<tr>
<td><code>authenticatorLargeBlobs</code></td>
<td>`32×0xff</td>
</tr>
<tr>
<td><code>authenticatorConfig</code></td>
<td>`32×0xff</td>
</tr>
</tbody>
</table>

### Index

**Terms defined by this specification**

- `uv`
  - _dfn for `getInfo`, in §3_
  - _dfn for `getInfo-old`, in §3_