FIDO U2F Implementation Considerations

FIDO Alliance Proposed Standard 14 May 2015

This version:
https://fidoalliance.org/specs/fido-undefined-undefined-ps-20150514/fido-u2f-implementation-considerations-v1.0-undefined-ps-20150514.html
Previous version:
https://fidoalliance.org/specs/fido-u2f-implementation-considerations-v1.0-RD-20140209.html
Editor:
Dirk Balfanz, Google, Inc.

The English version of this specification is the only normative version. Non-normative translations may also be available.

Abstract

This document lists a number of considerations for U2F implementers.

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.

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.

This document has been reviewed by FIDO Aliance Members and is endorsed as a Proposed Standard. It is a stable document and may be used as reference material or cited from another document. FIDO Alliance's role in making the Recommendation is to draw attention to the specification and to promote its widespread deployment.

Table of Contents

1. Notation
    1.1 Key Words
2. Implementation Considerations
    2.1 Timing Considerations
    2.2 Generation of Key Handles
    2.3 Secure Key Generation
    2.4 Challenge Parameters
    2.5 Revocation of Tokens
    2.6 Token Counters
    2.7 Key Usage
    2.8 UI Considerations for FIDO Clients

A. References
    A.1 Normative references
    A.2 Informative 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].

U2F 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. Implementation Considerations

Note: Reading the 'FIDO U2F Overview' (see [U2FOverview] in bibliography) is recommended as a background for this document.

2.1 Timing Considerations

U2F Tokens should respond to authentication and registration request as soon as possible to ensure a responsive user interface. In particular, they should not wait for user presence if the request message requires it. Usually, this means that U2F tokens should respond within 500ms to requests. (FIDO clients, on the other hand, should be coded more defensively, and should wait for at least 3 seconds before giving up on a U2F token.)

Once user presence is detected, U2F tokens should persist the user presence' state for 10 seconds or until an operation which requires user presence is performed, whichever comes first.

2.2 Generation of Key Handles

U2F tokens might not store private key material, and instead might export a wrapped private key as part of the key handle. If a U2F token chooses to do this, then the following must be taken into consideration:

The U2F token should employ a cipher that offers the best possible security on the given hardware. Sometimes, hardware offers better protections against certain attacks for 'weak' ciphers (e.g., 3DES) than against 'strong' ciphers (e.g., AES). Implementers should carefully weigh the pros and cons of different ciphers on the hardware platform that they're implementing on.

Given a particular U2F token and a relying party, the relying party should not be able to tell the difference between a key handle that was issued for a different token, and a key handle that was issued for a different relying party. (The concern is that a site, evil.com, might want to find out whether a given token has been registered for a site embarrassing.com, and would be able to do so if it had key handles from

embarrassing.com if it could tell the difference.) The two error conditions ('wrong key handle' and 'wrong origin (but correct key handle)') should not be distinguishable to the relying party, through careful timings or otherwise.

2.3 Secure Key Generation

U2F tokens should follow best practices when generating private keys (i.e., use a recommended PRNG) and use a good source of entropy (which usually serves as input to the PRNG). If no good source of entropy is available on the token, the token should combine whatever entropy there is with the challenge parameter from the request as input into the PRNG.

2.4 Challenge Parameters

The registration and authentication operations require the relying party to pass a challenge parameter to the Javascript API (as part of the SignData and EnrollData parameters -- (see [U2FJSAPI] in bibliography). This parameter is the base64-encoding of a byte array chosen by the relying party.

Relying parties should ensure that the challenge parameter has sufficient entropy. In particular, it is recommended that the challenge parameter contains at least 8 random bytes, following the requirements in [SP800-63-1].

2.5 Revocation of Tokens

Since U2F tokens don't have device identifiers, U2F does not prescribe a way to revoke tokens (through a revocation list or similar mechanism). Instead, it is up to individual relying parties to stop honoring authentication responses that come from certain tokens.

Relying parties should give users a mechanism to report lost or stolen tokens. If the token is lost or stolen, then the relying party should stop honoring authentication responses from the token.

2.6 Token Counters

A U2F token must increase a counter each time it performs an authentication operation. This counter may be 'global' (i.e., the same counter is incremented regardless of the application parameter in Authentication Request message), or per-application (i.e., one counter for each value of application parameter in the Authentication Request message).

U2F token counters should start at 0.

The counter allows relying parties to detect token cloning in certain situations. Relying parties should implement their own remediation strategies if they suspect token cloning due to non-increasing counter values.

2.7 Key Usage

Keys generated during a U2F registration must not be used for any purpose other than U2F authentications. Implementers of hardware and/or software that serves other purposes beyond U2F need to ensure that U2F keys are not used for such other purposes.

2.8 UI Considerations for FIDO Clients

FIDO Clients should implement a user interface that allows the user to get a clear indication of which relying parties are using the FIDO U2F APIs. Such APIs allow relying parties that are in possession of the user's public key to confirm the identity of the user, even if the user has removed their cookies, is using anonymizing onion routing networks, etc. In the case where the FIDO Client is a web browser, the web browser should indicate to the user which page or web origin is creating or exercising U2F keys for the user. The FIDO client might also give the user the ability to allow or deny the use of the U2F APIs for relying parties.

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

[FIDOGlossary]
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

[U2FJSAPI]
D. Balfanz, A. Birgisson, J. Lang, *FIDO U2F Javascript API v1.0*. FIDO Alliance Review Draft (Work in progress.) URL: http://fidoalliance.org/specs/fido-u2f-javascript-api-v1.0-rd-20140209.pdf

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

A.2 Informative references

[SP800-63-1]
W. Burr, D. Dodson, E. Newton, R. Perlner, W.T. Polk, S. Gupta and E. Nabbus, *NIST Special Publication 800-63-1: Electronic Authentication Guideline*. National Institute of Standards and Technology, December 2011, URL: http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf