FIDO U2F Authenticator

A FIDO U2F (Fast IDentity Online, Universal 2nd Factor) Authenticator is a hardware device that provides an additional layer of security during the authentication process, commonly used to implement two-factor authentication (2FA). It usually takes the form of a USB dongle, but it can also come in other formats like NFC (Near Field Communication) or Bluetooth devices. When a user attempts to log in to a service that supports U2F, the service prompts the user to activate their U2F authenticator, usually by inserting it into a USB port and pressing a button on the device.

Purpose of U2f Attestation Statement

The U2F Attestation Statement serves as a secure method for confirming the legitimacy of FIDO U2F authenticators, which are hardware devices that provide an additional layer of security for online accounts. This statement helps websites and online services trust that the authenticator is valid and that the security features are intact.

Key Components

Attestation Statement Format Identifier

- Identifier
- :fido-u2f
-

Supported Attestation Types

- Types
- : Basic, AttCA
-

Syntax

The syntax for a FIDO U2F attestation statement is formally defined as follows:

```

Copy plaintextCopy codeattStmtType //= ( fmt: "fido-u2f", attStmt: u2fStmtFormat )

u2fStmtFormat = { x5c: [ attestnCert: bytes ], sig: bytes }

```

Field Definitions

fmt

- Type
- : String
- Description
- : The attestation format identifier, set to "fido-u2f".
-

attStmt

- Type
- : Object (u2fStmtFormat
-)
- Description
- : The actual attestation statement, structured according tou2fStmtFormat
- .
-

x5c

- Type
- : Array of bytes (single element)
- Description
- : Contains the attestation certificate in X.509 format. This certificate is used to verify the origin and characteristics of the authenticator device.
-

sig

- Type
- : Bytes
- Description
- : This is the attestation signature. It is calculated over the raw U2F registration response message received by the client from the authenticator. This serves as cryptographic proof that the attestation certificate and the public key belong together and originate from the authenticator.
-

U2F Attestation Statement Verification

1. Format and Syntax Check
2. : Verify that the Attestation Statement (attStmt
3.) follows the correct format (CBOR syntax) and decode it to extract key fields.
4. Public Key Verification
5. : Confirm that thex5c
6. field contains an appropriate Elliptic Curve (EC) public key over the P-256 curve. This step assures the device's legitimacy.
7. Data Extraction and Conversion
8. : Retrieve essential data (rpIdHash
9. ,credentialId
10. ,credentialPublicKey
11.) fromauthenticatorData
12. and convert the public key to a standard format.
13. Coordinate Validation
14. : Check the size of the x and y coordinates incredentialPublicKey
15. to confirm they are each 32 bytes.
16. Signature Check and Attestation
17. : Create a combined data string (verificationData
18.) and validate the device's digital signature (sig
19.). Optionally, identify the attestation type (Basic or AttCA) based on external information.
20.

Previous Windows Next WebAuthn Attestation Last updated6 months ago On this page *Purpose of U2f Attestation Statement * Key Components * U2F Attestation Statement Verification

Was this helpful?