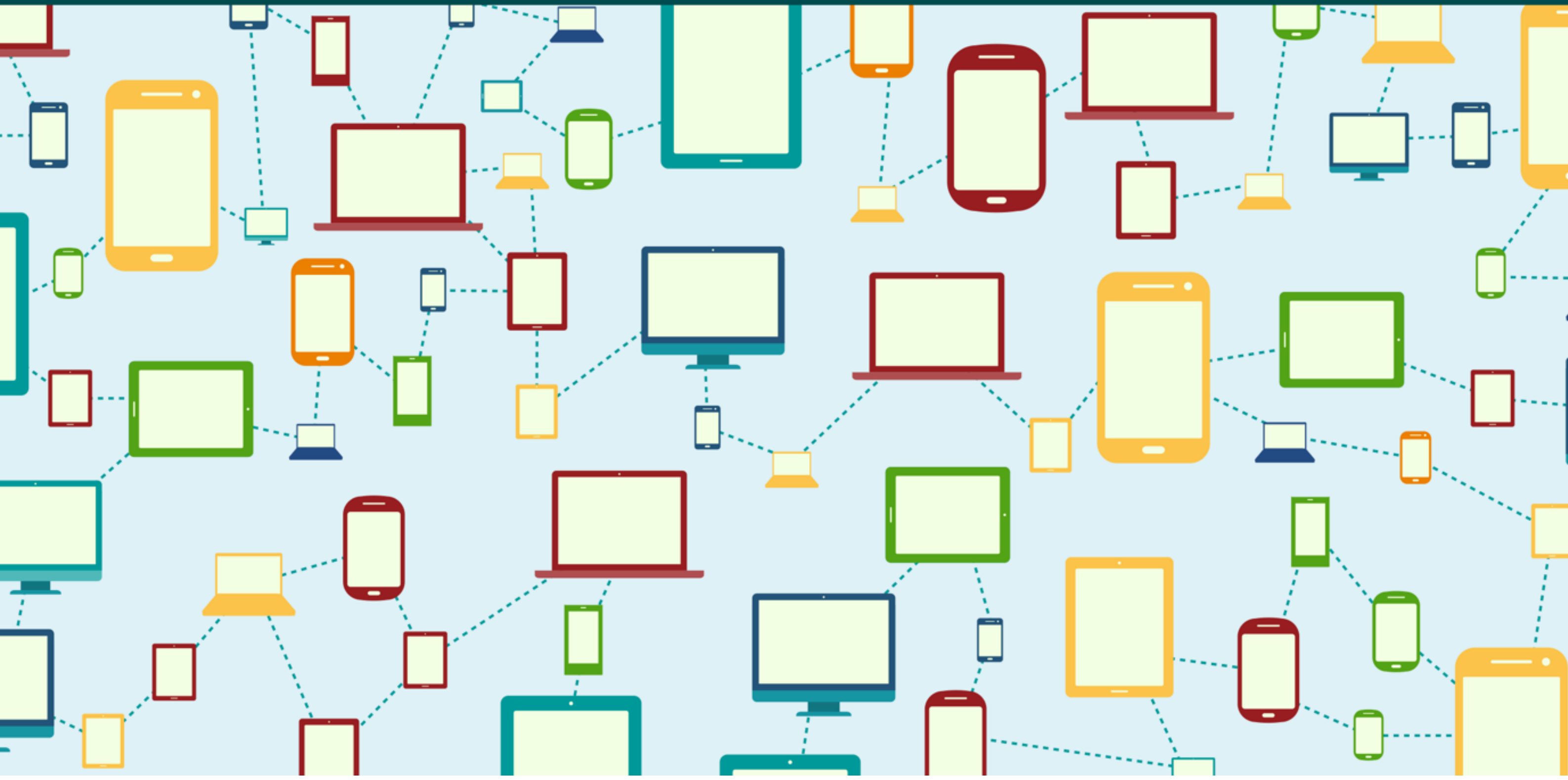


The FIDO UAF Metadata Service White Paper

January 2016

Introduction to FIDO 1.0 Protocols

The Fast IDentity Online (FIDO) Alliance is an industry consortium created to address the authentication problems faced by today's applications. The FIDO Alliance specifies protocols and interfaces that allows member companies to build the next generation of authentication products that make authentication more secure and user friendly. FIDO specifications allow vendors to incorporate FIDO into their devices, authenticators and servers in an interoperable manner.

UAF

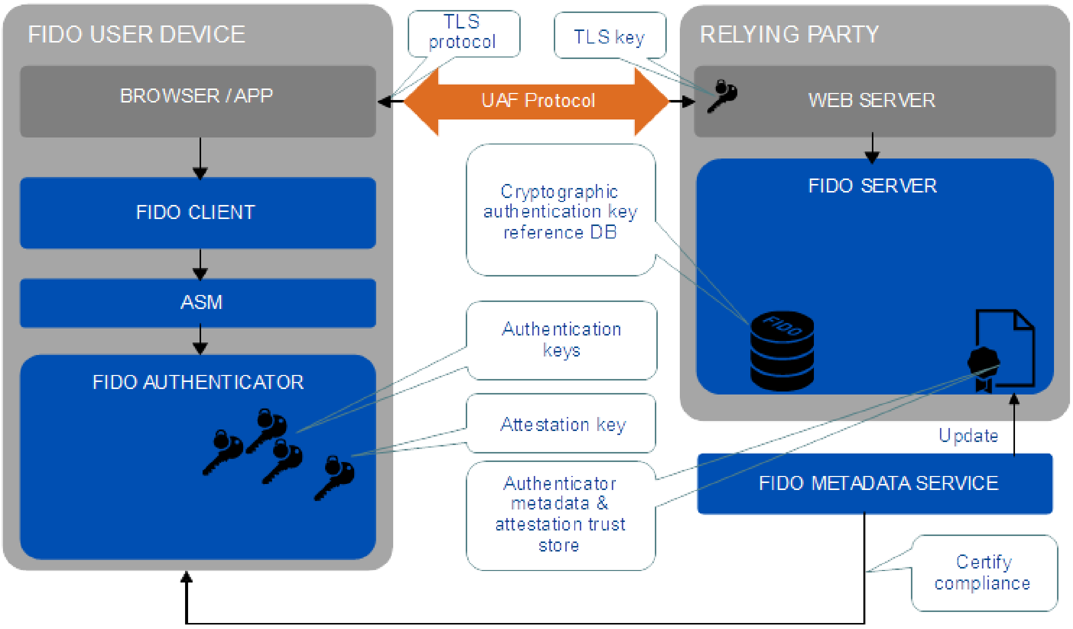
The Universal Authentication Framework (UAF) is an authentication protocol developed by the Alliance that allows users to authenticate to online applications using the native capabilities of the devices that they carry. The UAF protocol can plug in virtually any authenticator present on the device such as a fingerprint biometrics, a secure element-based PIN, face biometrics and many others. UAF uses a public key cryptography-based challenge response model to protect against many known authentication attacks. The white paper currently addresses UAF only.

U2F

The Universal 2nd Factor (U2F) is a protocol created by the FIDO Alliance that uses public key cryptography to provide users with a strong second factor to secure authentication to online services. A U2F authenticator can take a number of form factors, including both hardware and software only. For computers with a USB interface, the user presents the second factor by inserting a device and pressing its button. For mobile devices, U2F can be used in the form of a software client downloaded on a phone, a Bluetooth authenticator triggered by a click, or tapping with a device that supports Near Field Communication (NFC). The FIDO Alliance U2F Working Group is creating a specification for the Metadata Service to address U2F attestation. (See Appendix).

Architectural Overview of FIDO-UAF

It is useful for purposes of this paper to have an orientation into the FIDO-UAF architecture and terms. The key entities in the FIDO-UAF architecture are outlined in the diagram below.



Note that the architectural elements labeled in blue are abstractions (logical rather than physical entities) for purposes of the protocol design. For example, a FIDO Fingerprint Authenticator is a logical entity that encompasses the physical biometric sensor with its biometric matching software when they are combined with the cryptographic operations related to the FIDO protocol, the Authentication and the Attestation keys. The implementation of this authenticator may result in specific configurations to achieve security and performance goals.

In practice, an authenticator may be created by a single vendor as the prime or from contributions from multiple suppliers to a prime who assembles and delivers the complete solution for use by the end-user. For the sake of simplicity, this paper refers to such a prime as the “authenticator vendor”. Authenticators may be external to the user’s computing device e.g. a USB key or a wearable and presented to the device for authentication to a PC. Authenticators can also be built into the computing device e.g. A fingerprint sensor built into a phone. When authenticators are embedded in a device, it is possible that the device vendor is also the authenticator vendor.

For a complete overview of the FIDO-UAF protocol, its most current published specification and a technical glossary of terms can be found on the FIDO Alliance website in the specifications section.

Verification of UAF Authenticators

Each UAF authenticator may have different characteristics. For example, a fingerprint authenticator may protect the authentication keys using a Trusted Execution Environment and may use a secure display to show transactions. The trust that an application places on a UAF authentication may depend on the particular authenticator used. For this purpose, the application must be able to:

- Securely verify the authenticator employed on the user’s device.
- Determine the characteristics of that authenticator.

To enable the verification of authenticators by applications, UAF includes a cryptographic mechanism called attestation. Each UAF authenticator embeds an attestation private key that is used to sign UAF responses that it creates. UAF servers contain a database of attestation certificates of all known UAF authenticators that they use to cryptographically verify that a UAF response is actually from a specific authenticator. UAF servers also include a metadata database that contains the characteristics of each known UAF authenticator known as metadata statements. This information may be used for various purposes by the application such as input to a risk engine or for invoking application-specific actions such as limiting a transaction or require an additional authentication step.

Metadata Statements

The metadata statement is a JSON file that is produced by the authenticator vendor and consumed by UAF servers. The structure of the metadata statements is defined by the FIDO Alliance. The metadata statement contains information about the authenticator such as:

- Authenticator Version
- Authenticator ID (AAID)
- Attestation Certificate
- User verification method such as fingerprint biometrics
- Whether keys are protected by Trusted Execution Environment (TEE) or Secure Element (SE)
- Whether biometrics are protected by TEE

The metadata statement is also used in the authenticator attestation process. For a particular authentication event, an application can specify policies on which authenticators it is willing to accept to a UAF server. When a registration response is sent from an authenticator supporting attestation, it is signed using the authenticator’s attestation key. The server looks up the metadata statement corresponding to the authenticator’s (Authenticator Attestation ID) AAID and verifies that the signature is genuine using the authenticator’s public key from the attestation certificate in the metadata statement.

The FIDO MetaData Service

The universe of UAF authenticators is dynamic. Vendors are constantly updating their authenticators and introducing new ones. In addition, vulnerabilities may be discovered in existing authenticators, requiring that their use be limited or phased out. An organization deploying UAF must keep its metadata database up-to-date to both take advantage of new authenticators and protect itself against vulnerabilities in the authenticators it is allowing. To facilitate this process, the FIDO Alliance provides a MetaData Service (MDS) that allows UAF servers to automatically update their metadata database at frequent intervals. MDS is a web-based tool developed to facilitate authenticator vendors to publish metadata statements and for deployed UAF servers to download them (Figure 1).

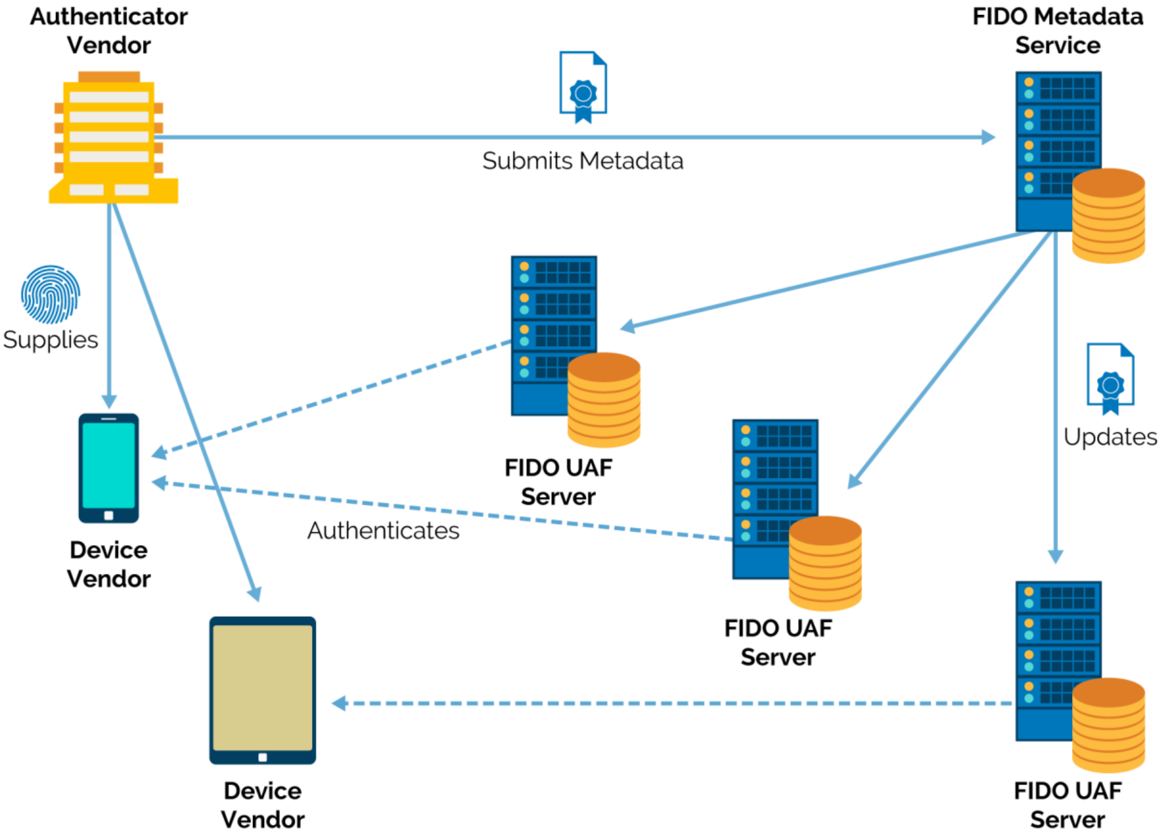
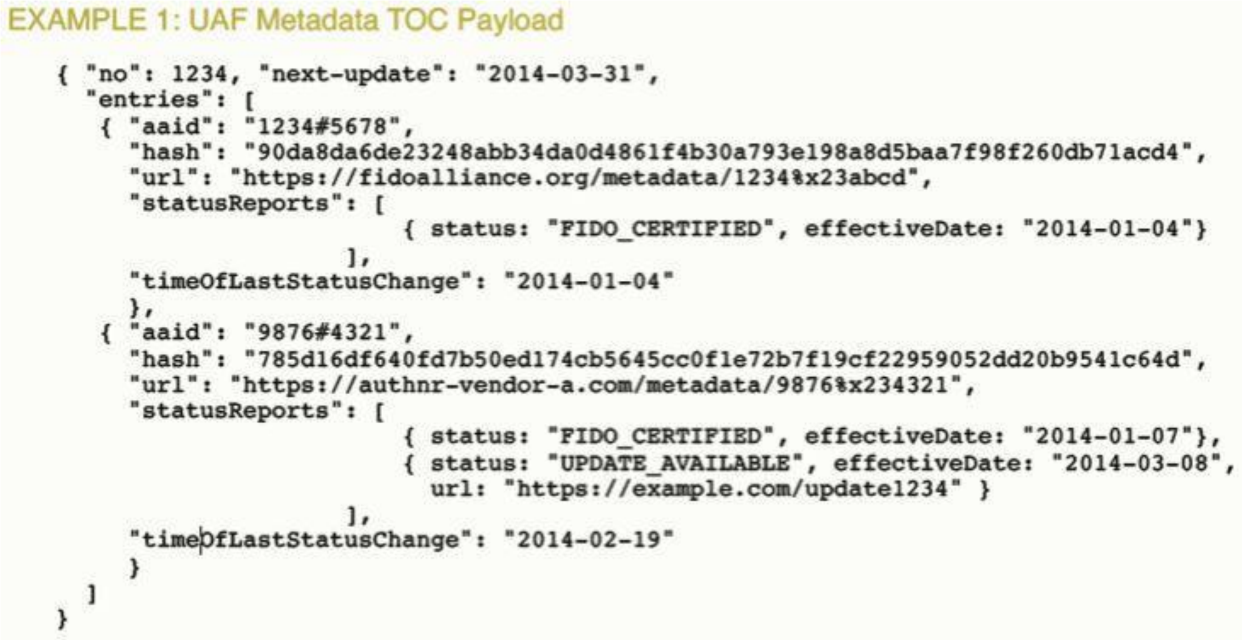


Figure 1

Metadata TOC

The MetaData Service (MDS) publishes a digitally signed document known as the metadata Table of Contents. The metadata Table of Contents (TOC) is a file that points to all the approved individual metadata statements submitted by authenticator vendors. The actual metadata statement is not contained in the TOC but rather the TOC contains URLs pointing to the statements.

The TOC is published in Javascript Web Token form at https://mds.fidoalliance.org. It has three components – a header (containing the algorithm used for the hash and signature generation), a payload, and the signature generated over the header and payload. Figure 2 shows a sample TOC.



EXAMPLE 1: UAF Metadata TOC Payload

```
{ "no": 1234, "next-update": "2014-03-31",
  "entries": [
   { "aaid": "1234#5678",
     "hash": "90da8da6de23248abb34da0d4861f4b30a793e198a8d5baa7f98f260db71acd4",
     "url": "https://fidoalliance.org/metadata/1234%x23abcd",
     "statusReports": [
                          { status: "FIDO_CERTIFIED", effectiveDate: "2014-01-04"}
                      ],
     "timeOfLastStatusChange": "2014-01-04"
     },
   { "aaid": "9876#4321",
     "hash": "785d16df640fd7b50ed174cb5645cc0f1e72b7f19cf22959052dd20b9541c64d",
     "url": "https://authnr-vendor-a.com/metadata/9876%x234321",
     "statusReports": [
                          { status: "FIDO_CERTIFIED", effectiveDate: "2014-01-07"},
                          { status: "UPDATE_AVAILABLE", effectiveDate: "2014-03-08",
                            url: "https://example.com/update1234" }
                      ],
     "timeOfLastStatusChange": "2014-02-19"
     }
  ]
}
```

Figure 2

The TOC document contains information such as the hash to verify data integrity of an individual metadata statement along with the URL from where the statement can be downloaded. The TOC also contains a list of status reports for each authenticator which indicates if the authenticator has gone through FIDO Certification or has been revoked.

The UAF server is expected to download the digitally signed TOC and verify its signature to check the integrity of the TOC. After the verification is successful, the UAF server can update its metadata database by fetching the metadata statements for relevant authenticators using the URLs specified for the corresponding entries in the TOC. If the UAF server is not interested in a particular authenticator, the server can choose to ignore the metadata statement for it. Thus, the server can obtain the security profile of an authenticator and accordingly choose to include it in their policy evaluation.

Publishing a Metadata Statement

To publish a metadata statement, a vendor must first apply for an account with the FIDO Alliance at https://mymds.fidoalliance.org. Once an account has been set up, the vendor can then create and submit a metadata statement according to the FIDO Authenticator Metadata specification. The metadata statement can either be hosted by the vendor on their chosen web site or submitted directly to the MDS for publishing. If the statement is self hosted, the authenticator vendor submits the URL of its location to the MDS.

Once a vendor submits a metadata statement, a series of actions are undertaken by the MDS before publishing. These actions are undertaken in two steps by two different individuals to maintain a segregation of duties.

Step 1

Each submission to the MDS is verified for syntactic correctness and validity. The following are validated in the submitted metadata statement:

- The identity of the submitter and his affiliation with the authenticator vendor company.
- The certification status of the authenticator and fill out the associated fields in the metadata statement.
- The AAID for which the statement was submitted belongs to the submitter's company.

Once the submission has been verified, the metadata TOC is prepared as follows:

- The hash value of the metadata statement is computed.
- The metadata TOC sequence number is created.
- Any status updates on the authenticator are added (such as when the authenticator was certified).
- The nextUpdate date of the metadata TOC file which also indicates the expiration date of the current submission is added.

If the metadata statement is to be hosted by the MDS, a URL where it is hosted is also created. This updated TOC data is then digitally signed using designated signing keys on behalf of the FIDO Alliance in a secure facility.

Step 2

The newly signed TOC data is re-verified for the updated content and then it is published to the designated web location (https://mds.fidoalliance.org). Finally, all the affected vendors of this publication are notified of the publication event.

Security Precautions for Signature Generation

For signature computation, several security processes and precautions are taken (Figure 3). The signature is not generated on the system where the MDS is running. Rather, a stand-alone (not connected to internet) system is used for this step. The signature is performed using a private key that is kept in a secure hardware token. A FIPS 140 hardware token is used for key generation and signing of the TOC.

The root and issuing CA's are managed in a secure facility by a third-party public CA. Any and all access to the token and the computing environment are logged and audited.

All access to the systems are authenticated. Segregation of duties is maintained between Step 1 (Signing) and Step 2 (Publishing) of the metadata TOC and statement. Controls are in place to preserve data integrity of the submitted metadata at every step of the process and the metadata TOC is verified again before the final publishing step.

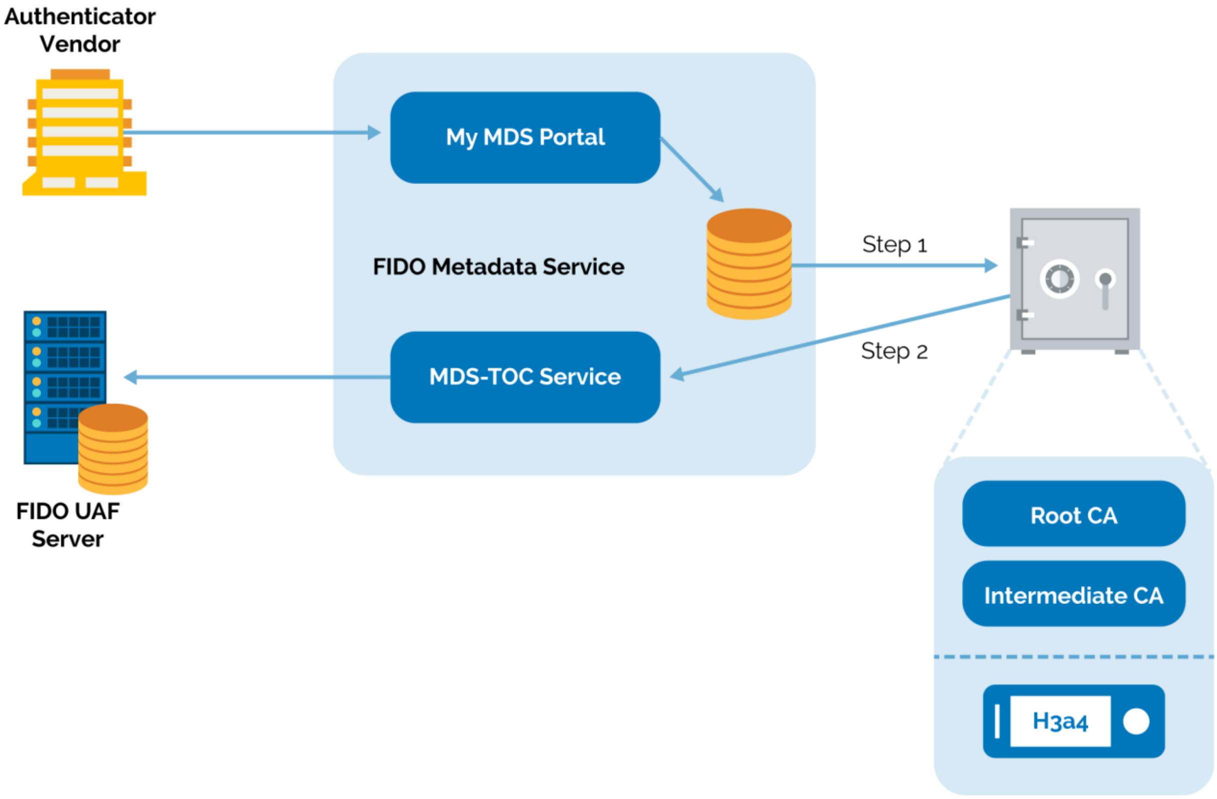


Figure 3

The metadata TOC has a maximum lifetime. Therefore, the ToC is updated frequently. Revocation check for TOC signing certificates is Certificate Revocation List (CRL) based. The CRL also has a maximum lifetime and is published at a fixed frequency.

Conclusion

The Universal Authentication Framework (UAF) protocol is an extensible authentication protocol that allows different authentications to be plugged into it. UAF includes an attestation mechanism that allows UAF servers to cryptographically verify the authenticator used in a UAF operation. In conjunction with attestation, UAF servers maintain a database of authenticator metadata statements that allow the application to determine the characteristics of the authenticator. The FIDO Alliance provides a MetaData Service (MDS) that allows organizations deploying UAF servers to easily keep the UAF servers up-to-date. UAF servers periodically download a metadata Table of Contents (TOC) file which contains URLs from which individual metadata statements can be downloaded. Authenticator vendors create and submit metadata statements to the MDS for publishing.

The FIDO Alliance takes several security measures to protect the integrity of the metadata service. The signing and publishing of metadata is separated into two steps and handled by segregated roles. Submissions to the MDS go through several verifications and checks before publishing. Signing is performed using a standalone system using a hardware protected key.

Appendix

The FIDO UAF Metadata Service is a full-featured centralized utility with the flexibility to include services for FIDO 1.0, such as attestation for U2F devices, and the forthcoming FIDO 2.0 protocol. The FIDO Alliance U2F Working Group is currently creating a specification to support a U2F attestation extension.

Verification of U2F Authenticators

Work is underway within the FIDO Alliance U2F Working Group for adding U2F attestation in the unified Metadata Service. This extension uses a subset of the Metadata Services to allow U2F authenticators to make claims to a Relying Party. In the U2F model, just as with the UAF model, the Metadata Service is provided by the FIDO Alliance to the marketplace as an optional utility for Relying Parties who would like additional assurances as to the authenticity and capabilities of the FIDO Authenticators that register with their system. In the U2F model, Relying Parties can obtain device metadata from attributes in the attestation certificate once the certificates have been deemed trustworthy.