**METADATA:**

- Relying Parties must have some means of discovering and verifying various characteristics of authenticators.

- Relying Parties can learn a subset of verifiable information for authenticators certified by the FIDO Alliance with an Authenticator Metadata statement.

- The URL to access that Metadata statement is provided by the Metadata TOC file accessible through the Metadata Service. [See document: FIDO UAF Authenticator Metadata Service v1.0]

- Authenticator metadata statements are used directly by the FIDO server at a relying party, but the information contained in the authoritative statement is used in several other places. How a server obtains these metadata statements is described in document: [FIDO UAF Authenticator Metadata Service v1.0]

- The workflow around an authenticator metadata statement is as follows:

* *The authenticator vendor (the authenticator) produces a metadata statement (JSON for metadata) describing the characteristics (aaid, etc) of an authenticator.*
* *The metadata statement is submitted to the FIDO Alliance as part of the FIDO certification process. The FIDO Alliance distributes the metadata as described in document: [FIDO UAF Authenticator Metadata Service v1.0].*
* *A FIDO relying party configures its registration policy to allow authenticators matching certain characteristics to be registered. (Means RP has its own policy created with certain conditions and characteristics and authenticators that match these characteristics are allowed to be registered with RP).*
* *The FIDO server sends a registration challenge message containing this policy statement. (That is the regRequest API, which stats the policy of the RP).*
* *The FIDO UAF Client receives the policy statement as part of the challenge message. It queries available authenticators for their self-reported characteristics and (with the user's input) selects an authenticator that matches the policy, to be registered. (Means user gets the policy on his mobile and checks for authenticators that match the policy and chooses one only on user's consent).*
* *The client (mobile) processes and sends a registration response message to the server. This message contains the AAID for the authenticator and, optionally, a signature made with the private key corresponding to the public key in the authenticator's attestation certificate. (That is the regResponse API, which contains aaid and attestation details).*
* *The FIDO Server looks up the metadata statement for the authenticator using the authenticator's AAID. If the metadata statement lists an attestation certificate(s), it verifies that an attestation signature is present, and made with the private key corresponding to either (a) one of the certificates listed in this metadata statement or (b) corresponding to the public key in a certificate that chains to one of the issuer certificates listed in the authenticator's metadata statement. (Means it checks if metadata exists for passed aaid in regResponse for that given authenticator, and if yes, checks if attestation signature is there and verifies it either using public key stored on metadata side or using one of the certificates stored for that authenticator on metadata side).*
* *The FIDO Server next verifies that the authenticator meets the originally supplied registration policy based on its authoritative metadata statement. This prevents a faulty, modified, or compromised FIDO UAF Client from registering authenticators that are out of policy. (Means it checks the metadata statement fetched for the given aaid of the authenticator with that stored for the same authenticator aaid in metadata service just to confirm that this is really the registered authenticator present in metadata and not some duplicate authenticator trying to register itself with modified data to match the policy).*
* *Optionally, a FIDO Server may, with input from the Relying Party, assign a risk or trust score to the authenticator, based on its metadata, including elements not selected for by the stated policy. (Means Fido server, along with RP, can additionally provide a kind of a trust store to maintain details about authenticator which are not selected by the stated policy and this depends on the authenticator's metadata).*
* *Optionally, a FIDO Server may cross-reference the attested AAID of the authenticator with other metadata databases published by third parties. Such third-party metadata might, for example, inform the FIDO Server if an authenticator has achieved certifications relevant to certain markets or industry verticals, or whether it meets application-specific regulatory requirements. (Means FIDO server can check the given aaid of authenticator in other 3rd party metadata databases, to check if this authenticator is already registered with some other certifications or markets or is it only related to Fido alliance certificate, etc).*