fidoalliance.org

FIDO TechNotes: The Truth about Attestation - FIDO Alliance

8-10 minutes

Adam Powers, FIDO Alliance Technical Director

There is a frequently mentioned but little understood term in FIDO: attestation. Even engineers implementing FIDO products are often confused with how attestation works or why it is needed. This Tech Note is an attempt to clarify attestation and its role in FIDO transactions; the post is largely for the technical community, but hopefully it is clear enough to the lay-person with a basic understanding of FIDO as well.

To start with, every time a user registers with a new service (Google, Facebook, PayPal, GitHub, etc.) the FIDO authenticator generates a new key pair for that service. The keys are necessarily unique to that service and aren't shared across services. This is the keypair most commonly associated with FIDO, and it is referred to as the "credential key pair" or just "the key pair". When a user registers with a service a new key pair is generated, and the public key is sent to the service to be stored and used in the future to authenticate the user. That key pair is not the attestation key pair, and to confuse things further that key pair gets used for an operation called "assertion" (the signing of a challenge during authentication). The terms “assertion” and “attestation” are frequently confused – assertion occurs when authenticating; attestation occurs during registration.

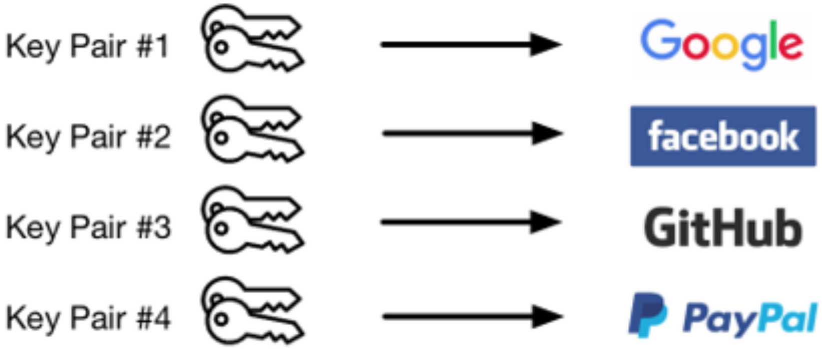

***Figure 1**: A new “credential key pair” is generated for each service that a user registers with.*

With that context in mind, what is attestation? It is a key pair that is burned into the device during manufacturing time that is specific to a device model. For example, all YubiKey 4 devices would have the same attestation certificate; or all Samsung Galaxy S8’s would have the same attestation certificate. The attestation is specific to a device model and can be used to cryptographically prove that a user has a specific model of device when they register. When a user creates the new “credential key pair” mentioned above, the public key that is sent to the service is signed with the attestation private key. The service that is creating the new account for the user can verify that the “attestation signature” on the newly created public key came from the device.

Generally speaking, attestation keys have associated attestation certificates, and those certificates chain to a root certificate that the service trusts. This is how the service establishes its trust in the authenticator’s attestation key.

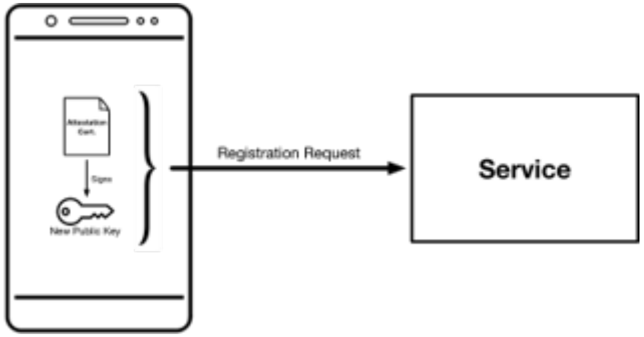

Figure 2*: During registration, a new public key is created and signed by an attestation private key that was created with the device when it was manufactured.*

Attestation accomplishes two things: 1) if an attacker intercepts a registration message with their own, they would not be able to swap out the new public key with their own since the attestation signature wouldn't match; and 2) it allows the service to trust that it knows the provenance of the authenticator being used.

At first glance, it might seem like preventing an attacker from replacing the public key with their own is the more important aspect of attestation. However, registration for FIDO typically requires that a user already have an authenticated session and communications are TLS protected, so there isn't much opportunity for malicious behavior. For this reason, many services will not reject an authenticator if it is using "self attestation". Self attestation (also called surrogate attestation) is when an authenticator uses a self-signed certificate instead of an attestation certificate that chains back to some root certificate.

Some services though, such as those in the financial industry or the public sector, may be required to know more about the devices that are accessing their services. They must guarantee that encryption keys are secure, biometrics are of a certain level of accuracy, etc. This is where the second aspect of attestation comes in, which is enabling the service to trust that the registration request is coming from a specific model of FIDO authenticator.

During registration the unique model number of the device is sent to the service along with the newly created public key. The unique model number is an “Authenticator Attestation ID” (AAID) in UAF; an “Authenticator Attestation Globally Unique ID” (AAGUID) in FIDO2; or a “Attestation Certificate Key Identifier” in U2F. Upon receiving a new public key from a user during registration, this unique identifier can be used to look up a metadata statement in a service such as the FIDO Metadata Service (MDS). Each record in the MDS has an AAID, AAGUID or Attestation Certificate Key Identifier that corresponds to the device.

Once the right record is found, the record has two essential kinds of information: 1) an “attestation root certificate”; and 2) the metadata about the device. We previously mentioned “self (or surrogate) attestation”, but devices can also use “full basic attestation” where the attestation certificate chains up to some well-known attestation root certificate. Assuming that the attestation signature over the public key is correct and the certificate chain is validated to root certificate, a service can then trust the other metadata about the device, such as the security and biometric characteristics of the device.

(Note: the FIDO authenticator certification program tests for and ensures that keys and other secrets are protected against external threats. FIDO will soon be launching a biometric certification program that ensures biometrics correctly verify users. Both certifications show up as metadata about the authenticator, providing more information to enable services to establish stronger trust in the authenticators.)

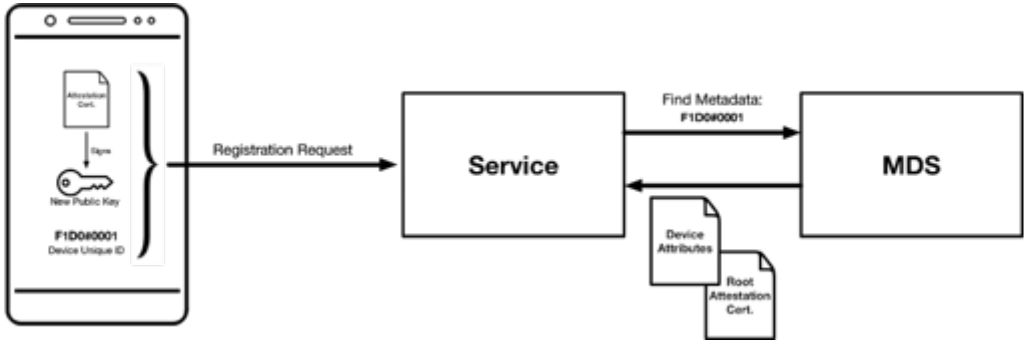

***Figure 3**: During registration, a service can use a device's unique identifier to look up the "root attestation certificate" and attributes about the device from a Metadata Service (MDS).*

For UAF and U2F, each has its own attestation format. UAF has a custom "tag length value" (TLV) structure that contains more information than just the attestation signature, and the U2F protocol simply has an attestation certificate and an attestation signature. As FIDO2 and WebAuthn are rolling out, more and more platforms are including attestation as a service that is built into the platform. Android has both SafetyNet and Android key attestation. Most modern PCs have TPM attestation, and more attestation formats are expected in the future as platforms evolve. For that reason, WebAuthn defines multiple attestation formats and allows new ones to be added in the future.

Hopefully that helps clarify what attestation is and how it is used, but there is just one more point to make – and this is really the reason I am writing this article. Please note that attestation is supposed to be unique to a device model, not an individual device.

One of the key attributes of attestation, as with all FIDO operations, is that it must preserve the privacy of the user. The reason that attestation keys are common to a model of device rather than each individual device having its own keys is so that attestation can't be used as a way of identifying and tracking users. During a recent FIDO interop, I had the pleasure of working with some incredibly smart, well-educated engineers that had fantastic implementations of FIDO; however, they didn't understand that they shouldn't create a new attestation certificate for every instance of a device. This is potentially problematic – if everyone buying a model of phone or security key gets the same model of the device, but has a different attestation certificate, that attestation certificate can be used to track and identify the individual across services. FIDO is founded on a principle of strong privacy, and using attestation to track users would violate FIDO's privacy principles. Making sure that attestation certificates are used across large batches of authenticators of the same model (100,000+) ensures that users can't be tracked based on their attestation certificate. My hope is that this blog post helps ensure that we are all using attestation certificates correctly and protecting the privacy of users.

MORE Buying, Building & Partnering