FIDO Attestation

Enhancing Trust, Privacy, and Interoperability in Passwordless Authentication

May 2024

Editors:

Khaled Zaky, Amazon Web Services
Monty Wiseman, Beyond Identity
Sean Miller, RSA Security
Eric Le Saint, Visa

Abstract

This document intends to provide a comprehensive understanding of attestation's role in enhancing and advancing the digital security landscape, specifically with respect to authentication. It focuses on the core function of attestation: verifying the origin and integrity of user devices and their authentication materials. FIDO credentials are discussed with a focus on how they offer more secure alternatives than traditional password-based systems and how FIDO attestation enhances authentication security for both Relying Parties (RPs) and end-users. In this document, RPs are those entities that provide websites, applications and online services that require the need for secure user access by confirming the identity of users or other entities. FIDO Alliance's historical journey is presented with practical analogies for understanding FIDO attestation, its enterprise-specific technical solutions, and privacy aspects involved in the attestation process.

Audience

Targeted for CISOs, security engineers, architects, and identity engineers, this white paper serves as a guide for professionals considering the adoption of FIDO within their enterprise ecosystem. Readers should possess a baseline understanding of FIDO technologies, the meaning of attestation, and have a desire to understand why and how to implement attestation.

Contents

1. Introduction 5
   1.1 Real-World Analogies for FIDO Attestation 5
2. Practical Implications and Use-Cases of FIDO Attestation 6
   2.1 From the Perspective of a Relying Party 6
   2.2 From the Perspective of the End-User 6
3. FIDO Attestation Explained 6
   3.1 What is FIDO Attestation? 6
   3.2 Types of FIDO Attestation 7
   3.3 Using AAGUID 7
4. Technical Solutions 8
   4.1 Authentication vs. Attestation Keys 8
   4.2 Trust in the Attestation Key - Trust Chain 8
   4.3 FIDO Attestation Sequence 8
   4.4 A General Description of the Attestation Lifecycle 9
   4.5 Enterprise Attestation 10
      4.5.1 Use Cases 10
      4.5.2 Process 11
         4.5.2.1 Provisioning 11
         4.5.2.2 User Registration with Enterprise Attestation 11
5. Privacy Implications and Considerations 12
6. Adoption and Deployment Considerations 12
7. Conclusion 12
8. Acknowledgments 13
9. Appendix 13
   9.1 Attestation Object 13
   9.2 Example Attestation Object 14
10. References 15

Figures

Figure 1 - New User Registration Sequence with Attestation 9
Figure 2 - Registration Sequence with Enterprise Attestation 11

1. Introduction

While authentication is widely understood, attestation may be less familiar to many practitioners in the information technology field. Attestation, as understood within the FIDO protocols, confirms a set of properties or characteristics of the authenticator. In the physical world, we can rely on examining an object to inspect its properties and verify its authenticity. In the interconnected digital world, physical inspection is not practical. Devices used for FIDO authentication should be carefully checked before use, especially if their source or contents are uncertain. Certain transactions, especially those related to government, healthcare, or financial institutions, demand higher assurance, and it is vital that the Relying Party (RP) confirms the authenticator's legitimacy in these cases. To ensure that high-assurance transactions are legitimate, RPs can employ attestation to verify the authenticity and properties of the authenticator.

> *A note on terminology: The term "key" and "key pair" is common to several types of keys described in this paper. To alleviate this confusion the term "passkey" will always be used when referring to a key used to authenticate a user. Use of other instances of the term 'key' will be specific by either the context or a modifier such as Attestation Key.*

In traditional password-based systems, it may be assumed that users and RPs keep passwords confidential. Because this assumption is not consistently enforced, breaches can occur. Using passkeys instead of passwords is a significant improvement, but some RPs may need more stringent policies to verify the authenticity of the authenticator and its properties.

Unlike passwords, passkeys use securely generated key material allowing access to websites and apps. Users and RPs rely on the authenticator for storage and management of this key material and therefore share the responsibility for secure handling of passkeys. All actors and components of the FIDO solution, including the authenticator, RP, and the passkey provider (when applicable), together ensure a robust security framework. This is in contrast to passwords, where the secure handling of passwords depends primarily on the user's memory, behavior, the RP, and password managers (if used). RPs can leverage attestations to verify that passkeys are securely handled within properly implemented FIDO certified devices.

Attestation provides RPs with information about the authenticator protecting the user's passkeys. This provides a means for the RP to enforce security policies for FIDO authentication. In the following sections, we delve deeper into the concept of attestation, its purpose, real-life scenario comparisons, and the problems attestation solves.

1.1 Real-World Analogies for FIDO Attestation

Drawing parallels with everyday security protocols offers significant insights. Both digital and physical environments demand rigorous checks and balances to validate identities and fortify trust. FIDO Attestation reflects the trust and verification processes familiar in the physical world.

To understand the pivotal role of FIDO attestation, consider its application in real-world identification and verification practices. These analogies underscore its integral function and efficacy:

1. **Identity Document Verification:** Just as individuals may produce official documents such as passports or driver's licenses to authenticate identity, the verifier (e.g., immigration official) wants proof of the document's authenticity and therefore checks for the relevant seals and marks. FIDO attestation provides proof of the authenticity of a user's authenticator, offers statements for examination, and provides cryptographic signatures for verifying the authenticity of the authenticator and the statements.
2. **Gaining Trust Through Authentication:** Think of moments where trust is contingent on proof of identity or authority. For example, accessing a secure facility where a guard authenticates you based on your identity documents, authorizing access to the facility. FIDO attestation fosters trust in digital environments when used to confirm the authenticator provenance and authenticity during online registration.
3. **Countering Threats and Weaknesses:** In real-world scenarios, ID checks exist to counteract impersonation, forgery, and fraud. FIDO attestation identifies the origins of authenticators and assists RPs to detect registrations from devices with known vulnerabilities, thereby enabling them to ensure that users employ only secure devices.

2. Practical Implications and Use-Cases of FIDO Attestation

2.1 From the Perspective of a Relying Party

Delving deeper into FIDO attestation provides invaluable insights into critical roles fortifying authentication systems:

1. **Assured Authenticator Security and Compliance:** For RPs operating in sensitive sectors, for example, finance or the public domain, there's a heightened need to ascertain that authentication devices are secure and meet specific standards. FIDO attestation helps ensure that authenticators accessing services are not only secure, but also adhere to specific standards and regulations.
2. **Authenticator Model Specificity and Trust in FIDO Authenticator Models:** FIDO attestation is tailored to distinct authenticator models, ensuring that cryptographic proofs during registrations validate said authenticator model authenticity. Beyond general trust in the attestation process, this specificity allows the RP to confirm that the passkey used in the registration request originates from a particular FIDO authenticator model. Such granularity is paramount for RPs where the details of authenticator models are crucial due to regulatory or security reasons.
3. **Verification Through Attestation Signature:** As a user sets up a new account, the onboarding RP can authenticate that the "attestation signature" linked to the freshly generated passkey is indeed from a genuine authenticator model.
4. **Incident handling and Response:** If a vulnerability is discovered in an authenticator, RPs checking attestations have the ability to discover which authenticators may be affected and require additional authentication factors or registration of a new credential for impacted users.

2.2 From the Perspective of the End-User

Although end users may not be aware of the technical details, FIDO attestation can enhance their online security:

1. **Enhanced Trust in Services:** When using services, particularly in high-assurance sectors such as banking or government portals, users can experience increased confidence. They understand that the RP isn't just authenticating but is also ensuring that authenticators accessing the platform adhere to specific standards.
2. **Authenticator Compliance:** FIDO attestation assures RPs of authenticator compliance and security, giving users the benefit of reliable functionality of their authentication devices paired with desired RP-related services.
3. **Transparent Registration and Onboarding:** The registration process is designed for seamlessness, but includes an additional step when an RP requests attestation of a FIDO authenticator. At this step, users must provide their consent to share the attestation metadata with the RP. This ensures that while backend verifications related to attestations, certification path validations, and authenticator compliance are streamlined, the user is aware of and has approved the process.

3. FIDO Attestation Explained

In this section we describe FIDO attestation and FIDO attestation types.

3.1 What is FIDO Attestation?

Within the FIDO authentication framework, attestation is a process for verifying the authenticity of a user's authenticator during the authentication process. The attestation can be used in conjunction with the FIDO Alliance's metadata service [1] to get more information about the authenticator including the model and certification level. An optional level of attestation, known as enterprise attestation, allows for further verification of specific authenticators, see section 4.5.

> *Note that the term 'attestation' might have different meanings outside of the context of FIDO. This paper discusses attestation only within the scope of the FIDO Alliance.*

In FIDO registration, a key step is the creation of a user authentication passkey, which occurs regardless of whether attestation is involved. During this process, the user's authenticator—such as a smartphone—generates a unique cryptographic key pair for each RP. The private key is securely stored within the authenticator, while the public key is shared with the RP, establishing a secure authentication framework. Additionally, during registration, the authenticator may provide an attestation, offering further assurance about the authenticator's integrity.

In addition to generating the user's authentication passkey, the FIDO authentication framework includes an optional attestation process. When attestation is requested, the authenticator may provide an attestation (synced passkeys do not currently provide attestations) by using an Attestation Key to sign the AAGUID (Authenticator Attestation Globally Unique ID) along with the passkey public key, creating signed evidence that establishes a trust anchor for the RP to validate that the authenticator properties meet the RP conditions through the MDS (FIDO Alliance's Metadata Service [1], see section 3.3 for additional information). If the authenticator cannot provide an attestation, the RP can authenticate the user with the passkey, and may obtain authenticator information (e.g. AAGUID), but it may not obtain verifiable evidence that the required authenticator properties are present.

This attestation process helps protect against supply chain attacks, such as the introduction of substitute or counterfeit authenticators. By verifying the authenticity of the authenticator, the RP understands the properties of the authenticator and assesses whether it meets the expected security standards, particularly during the registration phase, to ensure the device's legitimacy.

FIDO attestation is thus a key component of the broader security and privacy objectives of the framework. It minimizes reliance on passwords, fosters strong device authentication based on public-key cryptography, and aims to offer a standardized and interoperable approach to authentication across different platforms and devices.

3.2 Types of FIDO Attestation

There are several types of FIDO attestation which differ in how the attestation statement is signed. Note that none of these attestation types except Enterprise Attestation provide information about the specific authenticator. This is to preserve user privacy.

1. **Self-attestation:** The attestation statement is signed by the user's passkey. This provides integrity protection for the attestation statement and provides no other assurances.
2. **Basic attestation:** The attestation statement is signed by a key created by the authenticator's manufacturer and embedded into the authenticator. This provides integrity protection of the attestation statement and proof of the authenticator's manufacturer. For privacy purposes, this key must be duplicated across many of the same authenticator's model (current FIDO Alliance requirement is >100,000 devices). It is not unique to a specific authenticator instance.
3. **Attestation CA (AttCA) or Anonymization CA (AnonCA):** This is similar to basic attestation, except the attestation statement is signed by a TPM Attestation Key. In this case, the TPM, a hardware-based module where cryptographic operations occur and secrets are stored securely without leaving the module, has its Attestation Key's certificate signed by a trusted authority managing the authenticator.
4. **Enterprise attestation:** This is discussed in section 4.5,

It should be noted that the FIDO2 Specifications work along with the WebAuthn specification [2]. The type of attestation used is determined by examining fields within the attestation object which are defined in the WebAuthn specification. Further definitions provided by the WebAuthn specification includes a number of different types of formats, for example: packed, TPM, and Android-key as well as supporting custom formats if needed.

3.3 Using AAGUID

The *Authenticator Attestation GUID* or simply AAGUID, uniquely identifies the authenticator's make (manufacturer) and model. It does not uniquely identify the specific authenticator. The AAGUID is returned by the authenticator when attestation is requested by the RP and the RP may use it to determine if the authenticator's make and model meets its policies. Among other uses, the AAGUID is the lookup value within the FIDO (MDS) [1] providing the RP detailed information about the authenticator.

The authenticator's conveyance of the AAGUID provides no proof of its integrity or authenticity. The RP must trust the specific authenticator to provide truthful information.

This point is important to emphasize:

- The AAGUID without attestation is "informational" only and does not provide any assurance of its authenticity.
- Attestation provides a signature providing a level of assurance (depending on the type of attestation) of the authenticator's identity.

4. Technical Solutions

This section describes the sequence of events and involved components that make up FIDO attestation.

4.1 Authentication vs. Attestation Keys

The use of keys and methods for user authentication from FIDO have been introduced in previous documents, but the use of keys and methods used for attestation may not be familiar.

- **User Authentication:** This is the process where the user demonstrates possession of the correct system credentials, utilizing a passkey instead of the traditional password, which is a common application of FIDO technology.
- **Attestation:** This is the process of the authenticator using a key that is not assigned to a user, but instead assigned to the authenticator, to digitally sign a message providing proof of the message's authenticity. The message involved is called the "attestation statement" and contains information about the authenticator. When the attestation statement is digitally signed by the authenticator's attestation key, the RP can verify the validity of the attestation statement.

In summary:

- **A passkey authenticates the user to an RP**
- **An attestation key signs an attestation statement to authenticate its origin**

As stated in section 3.3 an RP may obtain the authenticator's make and model by simply checking the authenticator's AAGUID against the Metadata Service to get this information. Without being digitally signed by a key trusted by the RP, the RP has no proof this information is authentic or associated with the authenticator being queried.

Note: As discussed in section 3.2, there are several attestation types. One of these, "self-attestation", uses the User Authentication key to sign the attestation statement. This is not technically a contradiction, but a simplification provided to allow integrity protection, **not** authenticity, of the attestation statement.

4.2 Trust in the Attestation Key - Trust Chain

Fundamental to attestation is the RP's trust in the Attestation Key. The Attestation Key must be generated by a trusted source and protected by the authenticator. The trusted source is typically the authenticator's manufacturer however, in the case of "Attestation CA (AttCA) or Anonymization CA (AnonCA)", a trusted agent or Certification Authority (CA) is asserting the authenticity of the authenticator. The public part of the Attestation Key is obtained by the RP using a trusted channel, typically the FIDO MDS [1], mentioned previously.

4.3 FIDO Attestation Sequence

Attestation uses a key pair associated with an authenticator, not a user. It is important that all authenticators of the same make and model return the same attestation statement. The format of the attestation is examined later in this section, but it is important to understand that, at a high level, the attestation provides information about the type of authenticator, and it is not specific to a single device.

The following steps (1.a or 1.b then 2.) summarize a FIDO authenticator's attestation lifecycle:

1. **Authenticator Manufacturing:** There are two models for provisioning the Attestation Key: case "a" for roaming authenticators, such as smartphones or USB security keys used across multiple platforms, and case "b" for platform authenticators, which are built-in authentication mechanisms within devices like laptops or smartphones.

   Note: This two-model distinction is not architecturally required by the FIDO Specification, but it is the practical implementation known today and provides a simplified explanation for the purpose of this paper. Also, the descriptions are generalizations and manufacturers may deploy different methods than described here – this is only a generalization.

   a. **Roaming Authenticator:** The authenticator manufacturer generates an Attestation Keypair (AK) for a specific authenticator model. The manufacturer creates a certificate with the AK's public key. The AK Certificate is commonly put into the MDS. This allows a RP to retrieve the AK Certificate from a trusted source, MDS, when an AAGUID is

provided. The AK Certificate itself is usually signed with the authenticator's manufacturer's issuer key. This creates a verifiable cryptographic chain from the authenticator back to its manufacturer.

b. **Platform Authenticator:** The authenticator is not shipped from its manufacturer with an attestation key that can be used for FIDO attestation. Instead, it relies on persistent keys within the platform authenticator. These keys are crucial cryptographic elements that the attestation service uses to generate a FIDO Attestation Key. The attestation service is trusted by the Relying Party to provide assurance in the platform authenticator's integrity and compliance. The attestation service creates an attestation key that is used to sign an attestation object which asserts the properties of the authenticator. The RP must trust the attestation service in the same way it trusts the roaming authenticator's manufacturer.

2. **User Provisioning with Attestation:** During registration (setting up the new account), a new User Credential (a passkey) is created with a unique cryptographic key pair, and the public key is sent to the RP. The RP may optionally require an attestation. Note that the User or the authenticator may ignore the requirement for attestation. If the authenticator possesses an attestation key and it is allowed by the User, the user's public passkey (along with the attestation statement) will be sent to the RP signed with the attestation private key. This allows the RP to verify the attestation statement which includes the User's Public passkey for the newly created User. Therefore, providing confidence/proof that the User's private passkey originated from a specific authenticator with known properties.

4.4 A General Description of the Attestation Lifecycle

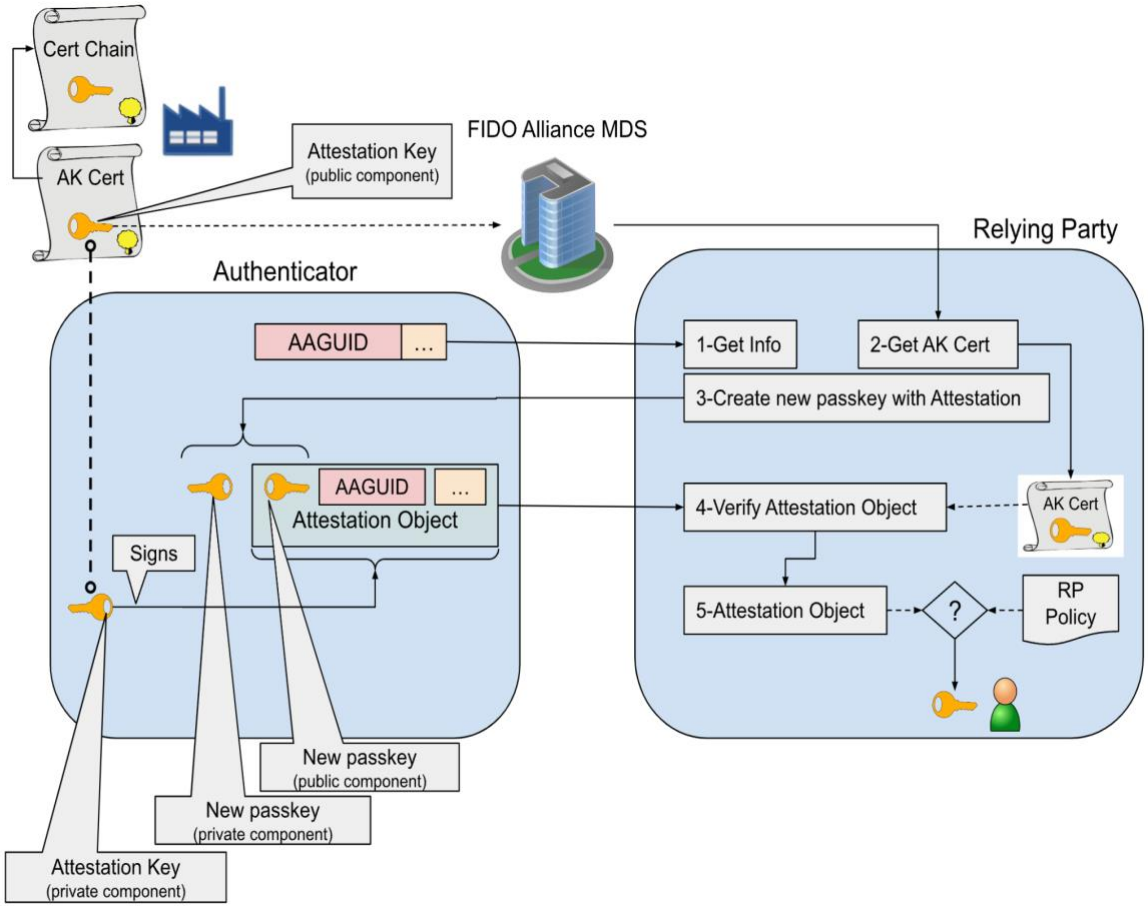


Figure 1 - New User Registration Sequence with Attestation

The attestation key generally has an associated attestation certificate, which links to a trusted root certificate of the Manufacturer. Once the RP has determined the authenticity of the signed attestation statement, the RP can use the attestation statement along with the MDS to learn more about the authenticator. For example, the RP may want to understand what level of encryption is used and what type of activation secrets is leveraged (e.g., biometrics) with a certain level of accuracy, etc. In order to get details about the authenticator an AAGUID value identifying the authenticator model is sent to the RP along with the newly created public passkey. Since the AAGUID represents a specific group of authenticator instances such as specific product release with a specific characteristic, specific form factor, or enterprise branding, an RP can use this AAGUID to lookup more information about the authenticator from the MDS.

As shown in the diagram, the attestation object, if provided, will indicate the format of the attestation statement, and then include some data the RP can examine. The attestation object includes a statement that typically contains a signature as well as a certificate or similar data providing provenance information for the attestation public key. Detail of the attestation object is provided in section 9.1 of the Appendix.

RPs should first verify the signature of the attestation statement and once verified, then examine the attestation statement. Once the RP has identified the attestation statement's format and type, the RP then reviews the contents and compares the contents against its policy.

An example attestation response resulting from a direct request to the authenticator by an RP is provided in 9.2 of the Appendix. The AAGUID provided in the attestation response can be used to obtain additional details about the authenticator from the FIDO Metadata Service.

4.5 Enterprise Attestation

By default, FIDO allows an authenticator to provide only product information using the AAGUID and high-level information about its type and capabilities, explicitly prohibiting an authenticator from providing uniquely identifying information. However, Enterprise attestation removes that limitation, as it binds a unique authenticator key pair to a serial number or equivalent unique identifier.

4.5.1 Use Cases

Enterprises actively manage authenticators for various purposes and are essential for securing high-value assets. While employees may select their own authenticators, enterprises may limit authenticators per employee and revoke them upon a departure or loss, as they oversee the entire process from purchase to collection. Additionally, enterprises may prioritize manageability and traceability to safeguard resources. Upon a threat incident, forensic investigations may need to trace activities related to a particular authenticator and correlate the authenticator's usage activity patterns in order to discover anomalies or the source of threat. Tight management enhances their ability to ensure non-repudiation for transactions. High-risk users may be assigned dedicated authenticators from the enterprise for access to restricted sensitive information or services. These authenticators are assigned specific PINs and are acquired through trusted supply chains.

Certain enterprise deployments require the use of FIDO authenticators with enterprise attestation in order to identify specific device identities (e.g. device serial numbers). Enterprise Attestation validation must also be supported by the organization's specific Relying Parties. These practices actively address enterprise-specific needs for improved control over device provisioning and lifecycle management.

4.5.2 Process

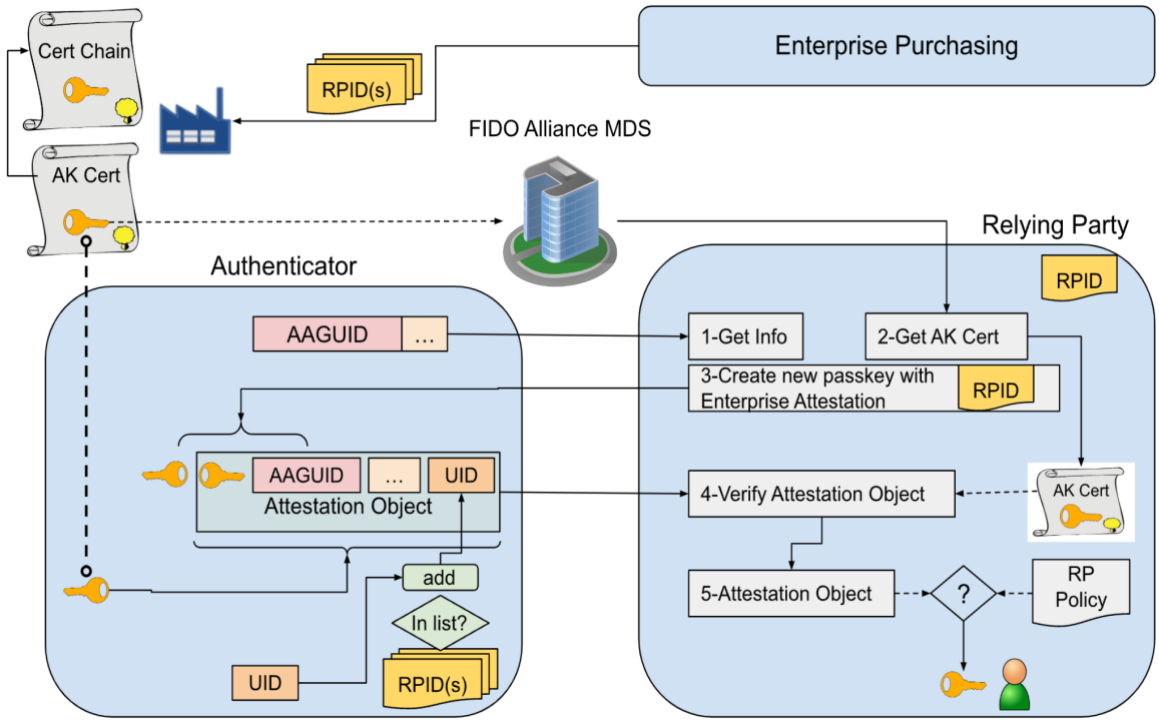


Figure 2 - Registration Sequence with Enterprise Attestation

4.5.2.1 Provisioning

Provisioning for enterprise attestation, is modified from the process described in section 4.3 to include both authenticator unique information in the attestation statement and to add any specific RPs permitted to receive this unique information from any set of RPs permanently “burned” into the authenticator by the authenticator’s manufacturer. The authenticator performs enterprise attestation only to those RPs provisioned to the authenticator. Other RPs may still perform any other type of attestation that excludes the unique identifier.

Authenticators that have the enterprise attestation burned into them **must not be sold** on the open market and may only be supplied directly from the authenticator’s manufacturer to the RP. An RP wanting an enterprise attestation enabled authenticator will order them directly from the authenticator’s manufacturer by providing a list of RP IDs (RPIDs). These specific RPIDs are the ones permanently burned/written to the authenticator.

4.5.2.2 User Registration with Enterprise Attestation

During a FIDO user registration described in section 4.3, the RP may indicate the need for enterprise attestation. This will uniquely associate the user with the specific authenticator by providing proof of the authenticator’s unique identifier. During user registration the authenticator verifies that the requesting RP (using its RPID) is among those listed in the permanently provisioned list of RPID permitted to perform enterprise attestation. If approved, this unique identifier is added to the attestation object and signed by the Attestation Key. The RP should validate the attestation object and, optionally, the certificate link/chain used to sign the attestation object. The RP can then verify, at user registration time, that the unique identifier was indeed purchased by the enterprise and may include that verification in its records.

The implementation used by an RP to authenticate the uniquely identifying information varies by authenticator. Some authenticators may use vendor facilitated methods where the enterprise provides a list of the RP IDs to the manufacturer and those are imprinted into the authenticators. Another is where some enterprise managed platforms maintain a policy, such as an enterprise managed browser.

Rather than imprinting the list of allowed RPs into the authenticator, an enterprise managed platform will make the determination if the enterprise attestation is provided to the RP based on the policy.

5. Privacy Implications and Considerations

While attestation provides a valuable assertion of trust for authenticators, privacy concerns can arise from the information shared during attestation. Some privacy considerations include:

- While the attestation properties described in this paper include a broad set of privacy controls, implementers should consider these capabilities against regional and local privacy policies.
- Attestation enables sharing information, such as authenticator's make and model, firmware version, or manufacturer details, with the RP. Concerns may arise regarding the potential exposure of sensitive authenticator-specific data and the subsequent tracking or profiling of users based on this information. For this very reason, an attestation batch of at least 100,000 is recommended so it is not a small pool to identify devices from.
- Non-enterprise attestation prevents the association of multiple passkeys within an authenticator with different RPs, thus safeguarding user privacy. For example, a person using a single authenticator may create a User Authentication passkey (passkey1) for RP 1 (RP1), then create a new User Authentication passkey (passkey2) for RP 2 (RP2). Even though the person is using the same physical authenticator for both RPs and using attestation, even if RP1 and RP2 collaborate, they cannot determine that passkey1 and passkey2 are from the same authenticator, therefore, they cannot determine the transactions are from the same person.
- Enterprise attestation adds uniquely identifying information (e.g., a device serial number) allowing an authorized RP to track the use of a specific authenticator across several pre-provisioned RPs within the enterprise. It is expected that users in this environment have an understanding of this property and the value it adds to the enterprise.

6. Adoption and Deployment Considerations

RPs can determine the registration requirements for a FIDO authenticator, as reflected in their preference for attestation conveyance. Some RPs may not require attestations to decide if registration is allowed. Other RPs may have security requirements that require an attestation object in order to make risk decisions. Security requirements may be based on characteristics of the authenticator (e.g., whether it requires a PIN) or could be as specific as the model of authenticator(s) allowed. Finally, in more protected environments, some RPs may require additional enterprise attestations to ensure an authenticator is known, controlled, and trusted by the enterprise.

7. Conclusion

FIDO attestation, a component of the FIDO and WebAuthn standards, validates the authenticity of a user's authenticator. This process provides a defense against various threats such as supply chain attacks, counterfeit authenticators, and substitution attacks. For RPs requiring higher authentication assurance, attestation is a FIDO-centric mechanism to obtain that assurance. For RPs that need to ensure the authenticity of specific authenticators, attestation provides these RPs assurance that they are dealing with a known and trusted device.

By generating unique key pairs for each RP that a user registers with, FIDO underscores its commitment to user security, eliminating potential cross-service vulnerabilities. The enterprise attestation feature provides organizations with better management of authenticators used by their personnel and is vital to environments that prioritize precise device management.

FIDO attestation brings certain privacy considerations. Disclosing authenticator-specific information, user device fingerprinting and the potential for user tracking, all highlight the importance of a privacy-aware approach. All stakeholders, including RPs, manufacturers, and users, must navigate the path between enhancing security and preserving user privacy.

FIDO attestation is adaptable. RPs have the discretion to request their desired level of attestation, ensuring a tailored approach suitable for both specialized services and large enterprises.

In summary, FIDO attestation augments online authentication. With a focus on public-key cryptography, unique key pairs, and specific attestation processes, its efficacy is maximized through careful deployment, thorough understanding of its capabilities, and a consistent commitment to user privacy.

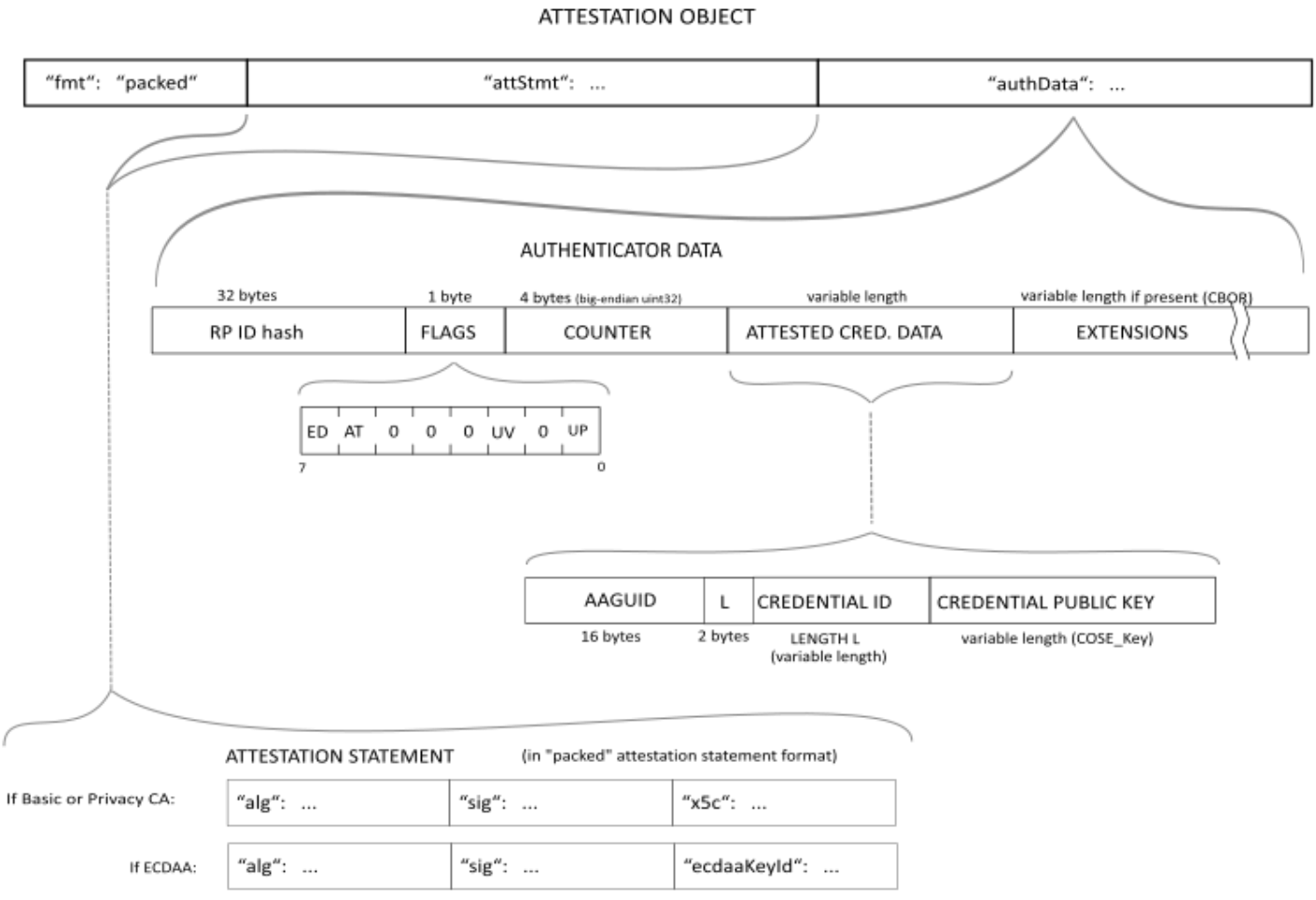
8. Acknowledgments

The authors acknowledge the following people (in alphabetic order) for their valuable feedback and comments:

- FIDO Enterprise Deployment Working Group Members
- Dean H. Saxe, Amazon, Co-Chair Enterprise Deployment Working Group
- Jerome Becquart, Axiad IDS, Inc.
- Johannes Stockmann, Okta Inc.
- Tom De Wasch, OneSpan North America Inc.
- Tom Sheffield, Target Corporation
- John Fontana, Yubico

9. Appendix

9.1 Attestation Object



Appendix Figure 1 - Attestation object*

*layout illustrating the included authenticator data (containing attested credential data) and the attestation statement.

9.2 Example Attestation Object


```
attestationObject: {
 "fmt": "packed",
 "attStmt": {
  "alg": -7,
  "sig":
"3045022100da2710ff0b5f5e5d72cda8c1e650f0b696e304942e55138672aa87a5e370a92d02205fd1a48bbda4757aac21252c7064f21130aba083151ab8ae75a26a356b675495",
  "x5c": [

"3082026f30820213a003020102020404ae6da1300c06082a8648ce3d0403020500307731 0b300906035504061302555331 0b300906035504081302 4d413110300e060355040713074265646666f726431193017060355040a13105253412053656375726974797 9204c4c433112302006035504 0b131941757468656e74696361746f72204174746573 746174696f6e311f301d060355040313165253412044533130302046494 44f204261746368203430593013060 72a8648ce 3d020106082a8648ce3d0301070342000465f2b3189a6dd2f7df9de784c1c8fd00ae804ac8de7bea042d00563dcd5d7a4094 8ae59d9dcf8722d8b6025ba98fbb80e6698bbe5003e4db4d80c4a50a3348e4a37330713021060b2b0601040182e51c01010 4041204107e3f3d3035574442bdae139312178b39301f0603551d23041830168014b851a38b84da69c9fd5b467c1f8e374a c0433419300c0603551d130101ff04023000301d0603551d0e041604142806df6c60b1656a78f97a28e168e5ec8d2937b43 00c06082a8648ce3d040302050003480030450221008812 2ea59cca8480ed57a0a60a2e203302b4d93713f837be7acc3a2c 895c6251022010f67d709ea2dc04ca63aec8d341dc9e562909dcea3f2a4abee2bdfd21dd162d"

  ]
 },
 "authData": {
  "rpIdHash": "f95bc73828ee210f9fd3bbe72d97908013b0a3759e9aea3d0ae318766cd2e1ad",
  "flags": {
   "userPresent": true,
   "reserved1": false,
   "userVerified": true,
   "backupEligibility": false,
   "backupState": false,
   "reserved2": false,
   "attestedCredentialData": true,
   "extensionDataIncluded": false
  },
  "signCount": 4,
  "attestedCredentialData": {
   "aaguid": "7e3f3d30-3557-4442-bdae-139312178b39",
   "credentialId":
"c0a3eb62197b77edd0cd1c73bffeb068dcc2595cfdf2e4dc01478bddc9cefcf52282f95bc73828ee210f9fd3bbe72d97908013 b0a3759e9aea3d0ae318766cd2e1ad04000000",
   "credentialPublicKey": {
```

```
      "kty": "EC",
      "alg": "ECDSA_w_SHA256",
      "crv": "P-256",
      "x": "D3Ki/INLfrmlNogo8d1lK7kBT4Fh3wPyVt/kusDAMKY=",
      "y": "M11KJSPXRiBn1ZtAo1eynxvaUXqipZJYV0AT0gC2czo="
    }
  }
 }
},
```

Appendix Figure 2 - Example Attestation object

10. References

[1] FIDO Alliance Metadata Service - https://fidoalliance.org/metadata/

[2] WebAuthn Specification - Attestation Section - https://www.w3.org/TR/webauthn-3/#sctn-attestation