High Assurance Enterprise FIDO Authentication

June 2023

Editor:

Sean Miller, RSA

Abstract

Enterprises should consider using passkeys, especially if they are currently relying on passwords. By replacing these credentials with passkeys, enterprises will immediately reduce the risk of phishing and eliminate credential reuse, improving authentication service security. Different types of FIDO authenticators may be used to meet users' needs with a balance between convenience and security. For enterprises that require high levels of identity assurance, internal security policies, or regulatory requirements, additional scrutiny is needed to determine the appropriate type of passkey. It is important to look at both the enterprise as a whole, as well as parts of the organization because high assurance requirements may not apply to the entire enterprise.

For many high assurance scenarios, attested device-bound passkeys may be more desirable. Relying parties with high assurance requirements will need to decide whether to accept all types of authenticators and adapt their authentication flow based on the attestation characteristics or reject registrations from unattested or unacceptable authenticators at the risk of a poor user experience.

Audience

This white paper is intended for IT administrators and enterprise security architects who are considering deploying FIDO authentication across their enterprises and defining life cycle management policies. This paper provides an overview of the different use cases for multi-factor authentication MFA and the FIDO Authenticator choices available to administrators. The intent is to help guide administrators in choosing the right authenticator types for their specific environment. Companies requiring higher levels of security, such as those involved in healthcare, government organizations, or financial institutions that have a hard requirement around the control of the credential, in particular should read this white paper.

It is assumed that the reader has an understanding of FIDO architecture, relying parties, protocols, and has read "FIDO EDWG 2023 Papers – Introduction" that introduces key concepts used in this white paper.

Contents

1. Introduction

This document focuses on deploying passkeys for enterprise users in high assurance environments.

Readers can find an introduction to the series of papers here. The introductory whitepaper provides additional descriptions and links to all papers in the series, which cover an array of use cases from low to high assurance. Most enterprises will likely have use cases that span more than one of these papers, and readers are encouraged to review the white papers relevant to their deployment environment.

This white paper examines what it means to be in a high assurance environment and how that may influence how FIDO is used. More specifically, the document addresses the challenges with password-only authentication and proposes passkeys as a stronger, phishing-resistant alternative to using passwords to authenticate users. Additionally, the document provides some adoption considerations for IT and security professionals to consider to ensure compliance with regulatory and security requirements for high assurance authentication scenarios. This white paper examines the use cases of registering a device, using a registered device, and dealing with recovering a lost device.

A key part in deciding if a passkey should be allowed in an environment is based on attestations. Attestations can be provided for credentials as part of the registration process, which relying parties can trust as provenance of the authenticator being used. For high assurance enterprise scenarios, attestations should always be requested. What can be discovered from the attestation associated with the credential, or the absence of any attestation, can help drive policy decisions about whether to accept the registration. Without any attestation, it may be difficult for the relying party to decide if the credential should be allowed. They may reject the registration outright, making for a poor user experience, or the enterprise may choose to employ additional, conditional multi-factor authentication (MFA) along with FIDO authentication to meet the high assurance requirements. With an attestation, the enterprise has assurances about the provenance, manufacture type, certifications, and features of the authenticator and often can rely on these assurances as MFA devices, providing multiple factors like credentials and a PIN to unlock the authenticator.

Synced passkeys work well in many use cases and can still work for some high assurance scenarios, depending on the security or regulatory requirements of the enterprise. Synced passkeys are attractive because of their recoverability and ease of use; however, they also change where credentials reside and who controls them. Given this external control of the credentials, some additional MFA may be desired for synced passkeys where the enterprise has control of the lifecycle management of the MFA method.

The remainder of this white paper will examine enterprises or organizations that have high assurance requirements based on Authenticator Assurance Levels [7] (AAL3) and FIDO Certified Authenticator Levels [8] (L1+) to operate.

2. Passkey Use Cases

This section will focus on use cases around passkeys in an enterprise or an organization. There are many use cases for enterprises where synced passkeys work very well for ease and convenience in registering devices, using devices, and recovering lost devices since the credentials are available on other devices. It is highly recommended that organizations look at all the benefits of synced passkeys to determine if they are appropriate for the organization. However, the use of synced passkeys, while convenient, may not meet all the security requirements for an enterprise or organization needing high assurance (e.g., AAL3 requirements). AAL3 level has several requirements with the most significant being the use of a hardware-based authenticator. Please refer to NIST for more detail on the different levels of Authenticator Assurance Levels (AAL) [7]. Quite often, AAL3 applies to companies and organizations requiring higher levels of security, such as those involved in healthcare, government, or finance, which have a hard requirement around the control of the credential, specifically, that it is device-bound and never copied.

2.1. Registration

The enterprise or organization should first consider what device(s) they will support in their environment and how they will manage the provisioning of devices. For example, an organization may support an environment where users can bring their own device (e.g., mobile phone), or an organization may have very strict requirements around issued devices that meet specific security requirements such as PIN length, particular user presence features, or even specific hardware models. Finally, organizations need to consider whether they will allow passkeys to reside on multiple devices or just a single device. This has both security and recovery implications that need to be considered.

Organizations may have use cases that require credentials to be device-bound and not copyable at all, in which case synced passkeys are not recommended. Organizations may choose to allow synced passkeys alongside traditional MFA mechanisms, replacing the password with a passkey. However, if the organization has strict requirements for where the credentials can reside, they should look closely at restricting use to device-bound passkeys. These factors will decide how organizations manage registration. All these cases put some added burden on the relying party if types of passkeys need to be restricted.

The relying party may need to check if some requirements are met during the registration process, such as requiring an authenticator that meets or exceeds the FIDO L1+ certification [8]. To assess the authenticator's compliance with these requirements, the authenticator must provide an attestation that can be validated and examined. If an authenticator does not meet the requirements of L1+ then, the relying party may be forced to reject the registration since nothing can be proven about the provenance of the credential, or the party may consider an implementation with additional MFA to meet the requirements of high assurance.

If an attestation is provided, the relying party can check what type of device it is and if it meets the requirements of the enterprise or organization. The relying party may also want to restrict based on the unique identifier for the authenticator, provided an attestation is available. The unique identifier, known as an Authenticator Attestation Globally Unique Identifier (AAGUID), can be used to look up the details against the FIDO Alliance Metadata Service [2] to understand what type of device is being registered, the certification level, and what features it provides.

Enterprise Attestation is another form of attestation that can be leveraged during registration. This is implemented by some authenticator vendors to add additional information that is unique to the organization. Including this additional information as part of the attestation and narrowing allowed authenticators can be used to further enhance the registration experience.

Similarly, there may be flags about whether the credential is eligible for backup and/or if it has been backed up. These flags cannot be trusted, however, without some attestation that the device is certified. A relying party might decide to allow or deny the registration based on this information as well as other information provided at runtime.

Unfortunately, if the relying party fails the registration of a credential, it forces the user to repeat the registration process again with a different authenticator at step one. Although WebAuthn [5] does not support a preflight mechanism to identify suitable authenticators, relying parties may provide feedback to the user before registration to identify acceptable authenticators. Additional guidance can be provided after failed registration to guide the user's choice of authenticator. This guidance should be explicit and identify why the authenticator was rejected during registration, which authenticators meet the RP's requirements, and guidance on managing browser-mandated optionality on communicating attestations.

Relying parties should be able to be more prescriptive in describing requirements of authenticators, allowing for a much better user experience where the end user can only select authenticators that meet the requirements and remove this burden from relying parties. These changes have been proposed to WebAuthn, but they have not yet gathered the support of platform vendors.

Another approach for enterprises might be not to offer any registration use case exposed to the end user. Instead, the enterprise would manage the lifecycle of registering the devices before they are provisioned to users. Similarly, the enterprise might provide some form of supervised registration experience to ensure only authorized authenticators are provisioned and registered. This avoids a number of pitfalls with the user experience mentioned above but puts more lifecycle management burden on the enterprise.

2.2. Sign In

Once a credential has been registered, FIDO credentials can be accessed when needed at authentication. The application(s) will leverage the WebAuthn browser API or platform passkey APIs to perform a FIDO authentication using a registered device. Depending on the type of registered device, there will be multiple factors involved in the authentication, like the entering of a PIN or a user presence challenge. The requirement for these interactions is there is a high level of assurance that the user is who they say they are, and they are not impersonating any user. These requirements need to be enforced during the registration process to ensure devices are allowed to meet the requirements of the enterprise or organization.

The only difference in this use case between synced passkeys and device-bound passkeys is what needs to be authenticated. For device-bound passkeys, the original hardware device used during the registration process is needed. Synced passkeys may be accessed from multiple devices that have access to an account hosted by a passkey provider. Furthermore, some synced passkeys may be shared after registration. Relying parties do not have a mechanism for identifying shared credentials in the current specifications, making it harder to understand and manage the lifecycle of synced passkeys.

There are several enterprise use cases covered in the white paper on "Choosing FIDO Authenticators for Enterprise Use Cases" [4]. Organizations should review these to evaluate how FIDO is leveraged. In particular, an organization planning to rely on FIDO as a first factor (passwordless) or a second factor is a key decision, and the white paper may help organizations understand what truly requires high assurance. For example, there may be a specific project, or a use case may apply to an entire industry driven by government or regulatory requirements. Employees might be allowed to use a synced passkey to access a laptop for example, but then need to use a device-bound passkey to sign in to a specific application restricted to certain employees with a particular clearance level.

2.3. Recovery/Lost Device

Recovery is where a synced passkey shines. If one loses a FIDO device that holds a credential, they can just access the credential from a different device that shares the same platform account. This is convenient, but also means that a passkey is only as secure as the platform account with which it is associated. Enterprises should examine the vendor solutions to understand how secure it is before relying on a service external to the organization. For example, does it provide end-to-end encryption with keys that are not known to the vendor? What additional measures like MFA are used to secure the user's account? What process is used for account recovery? End users may not be concerned about such matters, but these details may represent a security concern for the organization's security administrators. The organization's security requirements need to be examined to see if an external party can store and manage credentials. Furthermore, without requiring attestations, the relying party has no idea who or what is the issuer of a credential—whether it be the platform, a roaming authenticator, a browser plug-in, or something else. As a result, the relying party cannot provide any guidance as to how to recover access to the credentials while providing high assurance. An alternative form of account recovery external to recovering the FIDO credential would be needed to verify the identity of the user and issue a new device and credentials. Finally, the recovery of a passkey from a provider when using synced is not known to the relying party. This represents a potential attack that the enterprise is unaware of.

For device-bound passkeys, the recovery process is more involved and will likely require the involvement of a help desk [6] to issue a new device and possibly revoke access for the old device. This is a security-first approach over convenience that allows an enterprise or organization to control who has devices. It does mean there are additional steps needed for the end user before they can regain access. However, this gives enterprises more control over the lifecycle of the credentials, allowing enterprises to revoke or expire authenticators at any point and be able to guarantee that credentials are not copied or do not exist outside enterprise controls. Some enterprises have solved this by provisioning multiple devices so users can self-recover. Ultimately, there is a business decision to be made regarding recovery models. In some cases, it may be appropriate to block access until the user can receive a new device, taking loss of productivity over a lower security model. The extra burden highlighted in the registration step if an enterprise chooses to manage the registration experience has a direct impact on the recovery/replacement experience.

2.4. Unregistering

At some point an employee will either leave a project or the enterprise overall. The enterprise will want to be sure they have control over credentials and unregister their use so access is no longer possible. This is a bigger consideration when it comes to synced passkeys where the enterprise does not have full control of the lifecycle and management of the credentials. If synced passkeys require additional MFA, the enterprise can control the MFA aspect, expiring the factors involved so authentications no longer are allowed. Device-bound passkey environments have much more control over unregistering devices, either by physically handing in a device and knowing no copies were made, or invalidating/expiring the device so subsequent authentication attempts fail.

The credential lifecycle requires the ability to disable or remove a credential, whether due to a change in status of an employee, such as a leave of absence or separation from the organization, or due to the potential loss or compromise of a credential. Passkeys differ from passwords in these instances since the user may have multiple passkeys registered with the relying party, as opposed to passwords, where the user is expected to only have one password per relying party. In the case of a permanent separation between the user and enterprise, disabling the user account and/or rotating the credential in the service is standard practice to ensure the user is no longer able to authenticate. If the separation is temporary, such as for leave of absence, enterprises may choose to rotate all the user's credentials or disable the user account until the user returns.

In the case of credential loss, the next steps are dependent upon the deployment scenario. Users with device-bound passkeys who lose their security key should have the credential revoked by the service. Synced passkeys create additional challenges. If the device has been compromised, all credentials resident on the device, including those resident in different passkey providers, should be treated as compromised and revoked by the RP. If the user's passkey provider account has been compromised, the impacted credential(s) stored with the provider must be revoked. To facilitate revocation in these scenarios, RPs should allow credentials to be named or otherwise identified by the user during registration to facilitate the revocation of specific credentials where possible. Administrative controls must narrow their focus on eliminating credentials from the RP rather than removing the credential private key material from either hardware security keys or a passkey provider's sync fabric, which may not be possible.

3. Deployment Strategy

In a high assurance environment, the enterprise is likely going to want to manage the distribution and retirement of all authenticators. Device-bound passkeys would be managed by IT and provisioned to individuals. Relying parties would need to check for attestations and only allow the registration of authenticators that are managed by the enterprise or organization. If attestations are absent or do not meet the security requirements, the registration should fail. Processes should be established to manage the pool of authenticators to ensure they are retired when individuals leave or no longer require high-level access. Lastly, the organization or enterprise should define what the process looks like for recovering lost/stolen devices. Depending on how critical the access is to the continuity of the business, multiple hardware devices might be issued for a given individual to ensure they always have access.

4. Conclusion

There is no argument that passkeys are a strong phishing-resistant alternative option to traditional passwords. In an enterprise environment, it is important to look at security and regulatory requirements to determine if synced passkeys work, or if there are stricter constraints such as internal security policies, regulatory, or compliance requirements that require the use of device-bound passkeys. With either approach, enterprises should spend the time to understand how registration, management, and recovery of FIDO credentials will be managed. This includes important use cases like storage of credentials (external), recovery of lost credentials, and unregistering devices when employees leave. Based on the requirements of the enterprise, passkeys may work without any customizations, or enterprises may need to invest to ensure their authentication experience is more managed and filtered to specific devices.

5. Next Steps: Get Started Today

- Use FIDO standards.
- Think about what your relying parties are supporting and consider your enterprise security requirements.
- Passkeys are far more secure than passwords. Look for the passkey icon on websites and applications that support it.

For more information about passkeys, visit the FIDO Alliance site [3].

1. References

[1] FIDO Deploying Passkeys in the Enterprise - Introduction

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

[3] Passkeys (Passkey Authentication) - https://fidoalliance.org/passkeys/#:~:text=Can%20FIDO%20Security%20Keys%20support,discoverable%20credentials%20with%20user%20verification.

[4] FIDO Alliance White Paper: Choosing FIDO Authenticators for Enterprise Use Cases - https://fidoalliance.org/white-paper-choosing-fido-authenticators-for-enterprise-use-cases/

[5] WebAuthn - https://fidoalliance.org/fido2-2/fido2-web-authentication-webauthn/

[6] FIDO account recovery best practices - https://media.fidoalliance.org/wp-content/uploads/2019/02/FIDO_Account_Recovery_Best_Practices-1.pdf

[7] NIST Authenticator Assurance Levels - https://pages.nist.gov/800-63-3-Implementation-Resources/63B/AAL/

[8] FIDO Certified Authenticator Levels - https://fidoalliance.org/certification/authenticator-certification-levels/

2. Acknowledgements

We would like to thank all FIDO Alliance members who participated in the group discussions or took the time to review this paper and provide input, specifically:

- Matthew Estes, Amazon Web Services
- John Fontana, Yubico
- Rew Islam, Dashlane
- Dean H. Saxe, Amazon Web Services, Co-Chair FIDO Enterprise Deployment Working Group
- Johannes Stockmann, Okta
- Shane Weeden, IBM
- Khaled Zaky, Amazon Web Services
- FIDO Enterprise Deployment Group members