
# FIDO Authentication for Moderate Assurance Use Cases

## June 2023

**Editors:**

Jerome Becquart, Axiad

Greg Brown, Axiad

Matt Estes, Amazon Web Services

# Abstract

The intent of this whitepaper is to provide guidance for organizations as they analyze the abilities and features of both device-bound passkeys and synced passkeys to determine how both credential types can be utilized in a moderate assurance environment. In this paper, the term “moderate assurance” refers to an environment or organization where the legal, regulatory, and security requirements are flexible enough to allow for the use of both types of credentials, using synced passkeys to replace passwords and multi-factor Authentication (MFA) for standard user accounts and device-bound passkeys for user accounts that require the highest level of protection and assurance. The paper is designed to provide a comparison of features and requirements that are supported by device-bound passkeys and synced passkeys, providing a vision of how both types of credentials can be utilized together in an organization that has moderate assurance needs.

# Audience

This white paper is one in a series of white papers intended for anyone who is considering deploying FIDO Authentication across their organization, including IT administrators, enterprise security architects, and executives.

Readers can find an introduction to the series of papers here. The introductory white paper provides additional descriptions and links to all papers in the series, covering an array of use cases from low to high assurance. We expect that most enterprises will have use cases that span more than one of these papers and encourage readers to review the white papers that are relevant to their deployment requirements.

The white paper assumes that the reader has a foundational understanding of FIDO2 credentials and the role they play in the authentication process; introductory information on FIDO2 can be found here: FIDO2 - FIDO Alliance.

# Contents

**1. Introduction** **4**

**2. FIDO Credential Adoption Considerations** **4**

2.1. User Experience 5

2.1.1 Backup, Lost Devices, and Recovery 5

2.3 Attestation and Enforcement of Credential Type 5

**3. Conclusion** **6**

**4. Next Steps** **6**

**5. Acknowledgements** **6**

# 1. Introduction

The initial implementations of FIDO2 credentials were created as device-bound passkeys on either a roaming authenticator or platform authenticator, where the private key of the credential is stored on the device's authenticator and not allowed to be exported, copied, backed up, or synchronized from the authenticator. This configuration presents a very secure and phishing-resistant solution for authentication that gives relying parties (e.g., web sites or service providers), a very high level of confidence that the user and the device are legitimate users of the system. With this high level of assurance, however, comes some challenges – primarily regarding usability and account recovery. For example, because there is no way to get the private key off the authenticator, if the device the private key is stored on becomes lost or damaged, then access to the resources that key authenticated would be lost. With device-bound passkeys, the solution is to register a second device-bound passkey with every relying party. This creates a more difficult user experience as the user would be required to register both authenticators. This is somewhat reduced for organizations that have consolidated their authentication flow by using an identity provider (IdP) to federate access to their applications, as the relying party is then the IdP itself.

To solve these challenges, in May 2022 Apple, Google, and Microsoft announced their intent to support synced passkeys in their operating systems. Synced passkeys have many of the same characteristics of device-bound passkeys, including the continued use of private and public key pairs. One significant difference, however, is that synced passkeys allow for the private key of the credential to be synchronized to other devices the user owns that exist in the same vendor's synchronization fabric ecosystem (e.g., iCloud in the Apple ecosystem). Synced passkeys also allow for the creation of a more streamlined and user-friendly experience. All passkeys share several common security properties, are highly phishing resistant, and use unique key pairs to enable strong authentication. However, it is also important to note the difference between synced and device-bound passkeys. For example, synced passkeys introduce new security considerations when analyzed against a device-bound passkey. Conversely, synced passkeys can more easily address account recovery challenges.

As organizations work to evaluate how and where both credential types can be utilized in their environment, they will need to review and understand their organization's legal, regulatory, and security requirements. When organizations evaluate these requirements, they will many times refer to the combination of these requirements as an authentication assurance level (AAL) and will reference documentation from the National Institute of Standards and Technology (NIST), which provides guidance and recommendation for different assurance levels. While there is currently work underway by NIST to update these assurance levels to better incorporate synced passkeys, the current standards can be helpful when evaluating the implementation of device-bound passkeys and synced passkeys into an organization. More information regarding NIST and AALs can be found here: Authenticator Assurance Levels (nist.gov).

In terms of this white paper, a moderate assurance environment is an organization that has several different authentication use case scenarios that can be met by a combination of AAL1 and/or AAL2 as well as AAL3 levels of assurance. This white paper will dive deeper into the advantages and disadvantages of both device-bound passkeys and synced passkeys to provide a comparison between the two that an organization can use along with their own legal, regulatory, and security requirements to determine how and where they can implement both device-bound passkeys and synced passkeys into their moderate assurance environment so that they can take advantage of the secure, phishing-resistant, and user friendly authentication process that FIDO2 credentials provide in all parts of their organization.

# 2. FIDO Credential Adoption Considerations

When organizations are evaluating the use of both device-bound passkeys and synced passkeys to support the AAL1, AAL2, and AAL3 requirements of their organization, there are several factors that they should consider. These factors are described below and are intended to provide the organization with the information they need to help analyze both types of credentials and determine where they can be used in their enterprise.

## 2.1. User Experience

In terms of user experience, the goal of using FIDO credentials to authenticate to a system has always been to provide an easy-to-use and effortless process for the user. The original FIDO implementations provided a streamlined sign-in experience, but still presented some user experience challenges.

Passkeys introduce several enhancements to help provide improve user experience including a new feature called "passkeys Autofill UI" that provides users easier access to the creation of the passkeys and provides an autofill-like experience where users simply pick the credential they want to use when authenticating and no longer type in their username or password. This experience becomes quite easy to use and is very similar to the experience that most users already like and are comfortable with when using solutions such as password managers. Creating a passkey user experience that users like more than their current password experience removes the hurdle to adoption that has been seen with previous passkey implementations.

### 2.1.1 Backup, Lost Devices, and Recovery

With device-bound passkeys, the private key is stored on and not allowed to leave the authenticator. This creates a very secure solution but does create challenges for users and enterprises regarding backup of the key data, loss of the authenticator, and addition of new authenticators for the user. While there are recommended recovery practices for device-bound passkeys (FIDO_Account_Recovery_Best_Practices-1.pdf (fidoalliance.org)), synced passkeys work to resolve these challenges in a more user friendly manner. With the implementation of a synced passkey solution, the user no longer must register multiple authenticators with a relying party to ensure continued access in the event of a lost authenticator. If an authenticator is lost, a user can recover their passkey by using the recovery process provided by the passkey provider. Additionally, synced passkeys make for a better user experience as a user does not have to register unique credentials per device or maintain multiple device-bound passkeys to minimize the risk of credential loss. Once configured, synced passkeys are available across all devices synced with the passkey provider.

Synced passkeys do, however, create a dependency on the passkey provider and their synchronization fabric. Each provider implements their own synchronization fabric, which includes their own security controls and mechanisms to protect credentials from being misused. Organizations with specific security or compliance requirements should assess which provider(s) or hardware security keys meet their requirements.

Synced passkeys have a lower security posture as they allow the private key on the authenticator to be synchronized to authenticators of other devices the user has in the same vendor's ecosystem. Organizations should also be aware that there currently are no standards or systems that allow them to keep track of what devices these credentials have been created and stored on, nor mechanisms to identify when the credential has been shared with another person. For use cases in an organization that require a high level of assurance, the fact that this information cannot be determined or obtained means that synced passkeys would not be a good solution for those specific organizational use cases, and they should look to device-bound passkeys to support those use cases.

## 2.3 Attestation and Enforcement of Credential Type

Attestation is a feature that is designed to enhance the security of the registration process. Attestation mechanisms are defined by the specifications as an optional feature, though most hardware security keys implement it. Attestation is the ability of the authenticator to provide metadata about itself back to the relying party so that the relying party can make an informed decision on whether to allow the authenticator to interact with it. This metadata includes items such as an Authenticator Attestation Globally Unique Identifier (AAGUID), which is a unique ID that represents the vendor and model of the authenticator, the type of encryption that the authenticator uses, and the PIN and biometric capabilities of the authenticator. Some authenticator vendors also support a feature called Enterprise Attestation that allows an organization to add additional uniquely identifying information in an attestation that is included with an authenticator registration request, with the intent to use this additional information to support a controlled deployment within the enterprise where the organization wants to allow the registration of only a specific set of authenticators. Additional information about Enterprise Attestation can be found in this white paper: FIDO-White-Paper-Choosing-FIDO-Authenticators-for-Enterprise-Use-Cases-RD10-2022.03.01.pdf (fidoalliance.org)

At the time of publication, synced passkeys do not implement attestation, which means they are not an appropriate solution for scenarios with highly privileged users that require higher levels of assurance or for organizations that want to implement Enterprise Attestation. To support these highly privileged users, relying parties and organizations have historically looked to, and will need to continue to look to, device-bound passkeys and authenticators from vendors that support and include attestation in their solutions. For organizations that have regulatory, legal, or security requirements that require all users to be treated as high privilege users or have a need to implement Enterprise Attestation, it is recommended that only device-bound passkeys be implemented in their environment. A companion white paper, "High Assurance Enterprise Authentication," provides details on this scenario and can be found here: **https://media.fidoalliance.org/wp-content/uploads/2023/06/FIDO-EDWG-Spring-2023_Paper-5_High-Assurance-Enterprise-FINAL5.docx-1.pdf.** Moderate assurance organizations can support all their users by implementing synced passkeys for their standard users to replace passwords and MFA with a more secure solution and then use device-bound passkeys for highly privileged users and their access to resources that require the highest level of assurance.

Implementing both types of passkeys in the same authentication domain does however create an additional challenge that will require organizations to take additional steps to ensure that the correct type of passkey is used when accessing resources: for example, ensuring that a highly privileged user is using a device-bound passkey and not a synced passkey when accessing a resource that requires a high level of assurance. Organizations can leverage the user risk evaluation and policy engine framework of their Identity Provider to solve this challenge. Watermarking the user's session with an identifier representing the AAL (or other properties of their choosing) to be used in downstream authorization decisions can also be used to solve this challenge. In federated authentication environments, this may be communicated using standards such as the Authentication Method Reference (amr, RFC8176) standardized by OpenID Connect.

# 3. Conclusion

In moderate assurance environments, both device-bound passkeys and synced passkeys may be implemented together to provide a more secure authentication solution for all use cases of the organization. The more user-friendly synced passkeys can be implemented to replace passwords and MFA for users with standard assurance level requirements, giving them a more secure authentication method that is also easier to use. For highly privileged users in the organization that require the highest level of security, device-bound passkeys can be issued that provide an even higher level of security and an additional level of trust in the authentication process. The white paper provides information comparing synced passkeys, with their better user experience, against device-bound passkeys, with their enhanced security features. Using this information, organizations can evaluate device-bound passkeys and synced passkeys to determine how both can be leveraged in their organization to provide easy-to-use and secure authentication methods that meet and exceed the requirements of their moderate assurance environment.

# 4. Next Steps

The next step for organizations is to start the evaluation of FIDO2 credentials so that organizations can move away from passwords, which are susceptible to phishing and are well documented to be a significant weakness in their overall security posture. Organizations that have a moderate assurance need and will implement both device-bound passkeys and synced passkeys should determine which credential type will provide the best return on investment, work towards implementing that credential type first, and then follow up by completing the deployment of the other credential type when possible. Implementing either type of FIDO2 credential is a large step forward in moving to a passwordless environment and significantly increasing the overall security posture of the organization.

# 5. 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:

- Karen Larson, Axiad
- Jeff Kraemer, Axiad
- Dean H. Saxe, Amazon Web Services, Co-Chair FIDO Alliance Enterprise Deployment Working Group
- Tom Sheffield, Target Corporation
- FIDO Enterprise Deployment Working Group Members