FIDO Deploying Passkeys in the Enterprise - Introduction

June 2023

Editors:
Dean H. Saxe, Amazon Web Services, Co-Chair FIDO Enterprise Deployment Working Group

Contents

1. Introduction

Last year FIDO Alliance, Apple, Google, and Microsoft announced their intentions to support passkeys— FIDO credentials that may be backed up and made available across devices that are registered to the same passkey provider. Since then, we have seen the support for passkeys and beta implementations by multiple platforms and password managers. Enterprises have expressed interest in passkeys but do not know where to start, what type of passkeys work in their environment, or how passkeys fit in their authentication strategy.

It is important to note that FIDO Alliance has embraced the term "passkey" to describe any passwordless FIDO credential. This includes *synced passkeys* (consistent with the original announcement and intent) as well as *device-bound passkeys* – which are FIDO authentication credentials that cannot leave the issued device (e.g., on a FIDO Security Key).

In the following series of papers, the FIDO Enterprise Deployment Working Group (EDWG) will provide guidance to leaders and practitioners on deploying FIDO solutions scaling from SMBs to large enterprises. With recognition that there are a variety of different use cases for FIDO credentials, from synced passkeys to device-bound passkeys, this series will identify key decision points for identifying which solution(s) are a good fit across different enterprise use cases. Enterprises are likely to find there are multiple FIDO-based solutions required to meet their different use cases.

As organizations evaluate how to use passkeys in their environment, they will need to determine the legal, regulatory, and security requirements of their organization and evaluate how both synced passkeys and device-bound passkeys can meet these requirements.

We assume that the reader has a high level understanding of the FIDO protocols, if not, please consult the FIDO Enterprise Journey Map and https://passkeys.dev/.

2. Why Choose Passkeys?

Passwords are the root cause of over 80% of data breaches, and up to 51% of passwords are reused, making them subject to credential stuffing attacks. FIDO credentials are inherently more secure than passwords due to their design. These credentials are unique cryptographic key pairs scoped to a specific origin (e.g., https://fidoalliance.org/) to prevent discovery by unrelated services. Unlike passwords, FIDO credentials are highly phishing resistant, and the credential—a private key—cannot be stolen from the relying party (RP) servers.

FIDO credentials can be utilized across a variety of use cases—from low to high assurance, balancing user experience, convenience, and security. Authenticators—ranging from hardware security keys to biometric hardware in phones, tablets, and laptops to password managers—enable enterprises to choose the right tools for their unique environments.

While all FIDO credentials are based on cryptographic key pairs, they do not exhibit the same security characteristics, nor are they all suitable for all use cases. For example, hardware security keys may be FIPS certified devices with device-bound passkeys. RPs can identify these credentials based upon the attestation statements provided at registration. On the other hand, synced passkey implementations synchronize key material through a cloud-based service. The export and management of credentials in a third-party service introduces additional considerations and may not meet every organization's security requirements. The table on page 4 summarizes the use cases and properties of device-bound and synced passkeys.

As you read the series you may encounter terminology that is unique to the FIDO ecosystem. Please consult the FIDO Technical Glossary for definitions of these terms.

We expect that most enterprises will have use cases that span more than one of these papers. Wherever organizations find themselves on this journey, they can start using FIDO credentials today to reduce credential reuse, phishing, and credential stuffing.

In the first paper, we examine how organizations can deploy passkeys to their users who are using passwords as their only authentication factor. By deploying passkeys, companies can immediately reduce the risk of phishing or credential stuffing for their staff while using corporate or personal devices for authentication. https://fidoalliance.org/fido-in-the-enterprise/

There are many organizations that have deployed classic second factor authentication solutions such as SMS OTP, TOTP, and HOTP. In many cases, these deployments were tactical responses to reduce the success of phishing attacks. However, none of these mechanisms are immune to phishing. In the second paper of the series, we examine how passkeys can displace less phishing resistant mechanisms while improving the authentication user experience. https://fidoalliance.org/fido-in-the-enterprise/

Enterprises in regulated industries may be obligated to utilize higher assurance authentication for some, or all, of their staff. These companies (or other companies with stringent security requirements) may be able to deploy synced passkeys, device-bound passkeys, or both to meet their authentication requirements. The third paper in the series provides guidance on deciding which FIDO-based solution(s) can meet these requirements. https://fidoalliance.org/fido-in-the-enterprise/

The final paper describes using device-bound passkeys where functional or regulatory requirements require high assurance authentication. These scenarios use attestation data to securely validate the hardware devices used to generate and manage passkeys. This attestation data can be used to ensure compliance with regulatory and security requirements for regulated enterprises and use cases. https://fidoalliance.org/fido-in-the-enterprise/

	Device-Bound Passkeys	**Synced Passkeys**
Low Assurance	Sufficient	Sufficient
Moderate Assurance	Sufficient	May Be Sufficient
High Assurance	May Be Sufficient Dependent upon the authenticator and regulatory/compliance requirements (e.g. FIPS 140)	Insufficient
Portability	May be portable between devices & ecosystems (e.g. hardware security keys). Limited by available connectivity options (USB, NFC, BLE)	Portable within the Passkey Provider ecosystem
Shareable / Copyable	No - device bound credentials cannot be exported	May be supported. Dependent upon the passkey provider.
Account Recovery	Minimize credential loss scenarios by registering multiple device-bound passkeys Account Recovery via enterprise RP defined mechanisms.	Credential recovery via Passkey Provider defined mechanisms to bootstrap a new device. Account Recovery via enterprise RP defined mechanisms.
Cost	Potential additional cost to obtain and provision hardware security keys if device-bound keys are unavailable in the platform ecosystem.	Built in to existing platforms Possible additional cost for third party/non-platform passkey providers

3. Acknowledgements

- Vittorio Bertocci, Okta
- Greg Brown, Axiad
- Jerome Becquart, Axiad
- Tim Cappalli, Microsoft
- Matthew Estes, Amazon Web Services
- John Fontana, Yubico, Co-Chair FIDO Enterprise Deployment Working Group
- Rew Islam, Dashlane
- Sue Koomen, American Express
- Jeff Kraemer, Axiad
- Karen Larson, Axiad
- Sean Miller, RSA
- Tom Sheffield, Target Corporation
- Johannes Stockmann, Okta
- Shane Weeden, IBM
- Monty Wiseman, Beyond Identity
- Khaled Zaky, Amazon Web Services
- FIDO Enterprise Deployment Working Group Members