Displace Password + OTP Authentication with Passkeys

October 2023

Editors:
Husnan Bajwa, Beyond Identity
Josh Cigna, Yubico
Jing Gu, Beyond Identity

Abstract

For enterprises that have implemented a second factor, such as SMS OTP, to mitigate the risk of credential stuffing, this paper will provide guidance on displacing passwords + OTP with passkeys.

Audience

This white paper is intended for ISRM and IT staff tasked with deploying and maintaining multi-factor authentication (MFA) sign-in processes.

Contents

1. Introduction

Many enterprises aiming to secure their workforces have deployed SMS and application-based one-time passcodes (OTPs) as an additional factor of authentication to passwords. This whitepaper is aimed at these organizations that are now considering a move to FIDO authentication with passkeys. While this whitepaper focuses on OTPs specifically, the discussion and recommendations can be generalized to any system using phishable second factors including application-based OTP and push notifications.

This whitepaper compares OTPs as an additional authentication factor to passwords and passkeys in terms of security, user experience and ease of deployment. And it provides general guidance about migrating from OTPs to passkeys in order to improve user experience while strengthening the organization's overall security posture. The guidance within this paper will cover key steps for moving towards passkeys, including planning, use case identification and documentation, pilot considerations, as well as deployment and training guidance. This document targets low-assurance use cases, including internal authentication, external authentication and third party and B2B authentication strategies. Given that organizations typically implement OTPs as the second factor to passwords, for this document all references to OTPs should be assumed as being used as a second factor to passwords.

This document will not cover specific vendor technologies or implementations. For guidance on moderate or high assurance use cases please refer to additional whitepapers published by the FIDO Alliance [1]. As this document is a part of a series of whitepapers, it is recommended that the reader start with the introductory document [2].

2. OTP MFA vs Passkeys: Why Choose Passkeys

Passkeys offer several benefits to security, user experience, and ease of deployment when compared to OTPs.

2.1 Security

OTP-based MFA has been widely adopted to mitigate the risk of credential stuffing and reuse. SMS and authenticator application-based OTP are the most commonly deployed solutions due to their relative low-cost and ease of deployment across a broad set of users and use cases. The relative simplicity of this type of MFA, however, leaves it vulnerable to social engineering and many MFA bypass toolkits, because no bidirectional communication exists between the secrets generator and the validating identity provider (IDP), meaning that an OTP can be intercepted and used by a third party without the knowledge of the end user or IDP.

Additionally, OTP-based MFA requires trust in a device that an organization may not manage nor have visibility into its security posture. This means that organizations are relying on end-users to maintain the security of their own device and their ability to discern phishing attempts. While user training can help to address some of these attacks, historic guidance like checking for secure connections and familiar URLs, still relies on an ever-vigilant user base.

Passkeys provide phishing-resistant, replay-resistant sign-ins that reduce the cognitive load on users and strengthen organizations' overall security posture. This is achieved because passkeys implement a cryptographic challenge-response protocol scoped to the relying party's domain. The authenticators then rely on secure behaviors, like biometric proofs or PINS to unlock the credentials on the authenticator while retaining a user-friendly experience. With passkeys, an organization can have a strong first-factor of authentication for passwordless scenarios OR a strong second factor for traditional MFA workflows.

2.2 User Experience

Passkeys improve the user experience over passwords and OTPs in several ways, including:

- Passkeys work even when there is poor cell coverage whereas SMS OTPs require mobile network connectivity. For example, a user can have wireless access on an airplane but are not permitted to use SMS. In this instance, the SMS OTP cannot be delivered whereas passkeys can be used to authenticate.
- AutoFill UI enables seamless integration within browsers on mobile devices and on desktops.
- Up to four times faster login, no need to wait for code delivery [3]
- Protection against mis-keyed passwords and codes
- Passkeys build on common behaviors for authentication like biometric proofs (face or fingerprint).

2.3 Ease of Deployment

For some micro, small, and medium sized businesses without large, dedicated support staff, end-user deployment of dedicated authentication hardware tokens can create roadblocks. This includes both OTP hardware tokens or FIDO security Keys. Historically, the ease of deployment of SMS/App based OTPs made them a more favorable option. Procurement, logistics, and configuration are a constant battle fought by operations and IT teams. With updates to the FIDO2 ecosystem to expand the authenticator landscape, this problem is alleviated and allows the use of many different devices as passkey stores.

All of this comes together to mean that the deployment of passkeys is much easier and less costly compared to SMS OTP for a few reasons:

- There is no SMS integration required. Enterprises will not need to configure or maintain interfaces with mobile carriers or third-party SMS vendors which reduces deployment complexity.
- Enterprises will not have to pay per-transaction fees associated with SMS OTP therefore reducing the total cost of ownership for authentication.
- FIDO authentication uses passkeys. Passkeys are simple to implement across a range of devices and applications.
- SMS OTP rely on carrier-specific APIs or third-party vendor APIs that are not standardized which increases risk of vendor lock-in and lack of interoperability.
- No time-synchronization is needed. Passkeys avoid the time-synchronization requirements of SMS time-bound OTPs (TOTPs). Codes don't need to be entered within a short time window, and deliverability issues with SMS do not result in login failures.

FIDO authentication with passkeys has been embraced by operating system (OS) and browser providers. This existing OS support from most major vendors means that, in most cases, existing hardware in the enterprise, such as laptops, phones, and tables, can be leveraged to deploy FIDO with passkeys without costly updates and replacements.

In some cases, enterprises use shared, single user devices such as iPads. For these use cases, a passkey stored in the integrated platform authenticator may not be appropriate, since any user of the device has access to the credential. In these cases, organizations should use roaming authenticators (hardware security keys) to generate and store passkeys for use on the shared device. This offers the same ease of use and convenience. Keep in mind, there may be an additional cost to purchase and manage these hardware keys for users. In many cases using hardware keys there may be a need to issue users a second hardware key as a backup to reduce the risk of the user being locked out of their account(s).

3. Deployment Strategy for Migration from OTP to Passkeys

3.1 Identifying the Deployment Model

Planning for a successful passkey deployment requires organizations to consider the needs of the user and the computing devices they use in their role to maximize the utility of passkeys for staff. At a minimum, organizations should consider the following questions when planning a passkey deployment in order to make passkeys accessible to the broadest audience possible:

- What kind of computing devices are used?
- Are your users working on laptops or desktop computers? Mobile devices? Tablets?
- Are the devices single user devices or multi-user (e.g., shared) devices?
- Are the devices provisioned by the company or are users using their own personal devices at work?
- Are there limitations on using USB ports, Bluetooth, or NFC?
- Are there limitations on access to the internet?
- Are your users commonly wearing gloves or masks which limit the use of on-device biometrics?

Based on the answers to the previous questions, organizations can choose one of a few types of authenticators to store user's passkeys. The flexibility of passkeys means that organizations can mix and match as their security posture and UX needs dictate. Other documents in this series go into more detail on each type of authenticator.

3.2 Deployment Testing

After determining the deployment model and deploying a FIDO server with applications integrated, it is recommended that organizations use pilot groups to test registration, authentication, and recovery processes (see below) with users. Then use the feedback from the pilot to improve processes and address issues raised by the pilot population before embarking on a broad rollout of passkeys.

3.3 User Experience

3.3.1 Registration

Enterprises should implement a reliable registration process to ensure that users are correctly and securely associated with their passkeys, as stated in earlier FIDO whitepapers. The registration experience is critical to consider because it is a user's first interaction with passkeys. Here are a few elements to consider when it comes to designing the registration experience:

- Identity Proofing - Physically or remotely having the user prove their identity at the start of the registration process is recommended to ensure a strong, abuse resistant process. This may involve SMS OTP for the final time.
- Self-service registration - Users use their existing credentials to bootstrap a new passkey.
- Supervised registration - work with IT/helpdesk for registration. This reduces the risk associated with self-service models that are vulnerable to phishing the original creds.
- Pre-provisioned credentials - high effort, high assurance, but a mechanism is needed to get the credential into the user's hands.
- Remote users - self-service or pre-provisioned, but a mechanism is needed to provide the PIN to the user to unlock the device the first time.

3.3.2 Sign-In

The first step in designing a FIDO deployment with passkeys is to understand the user base, common work paradigms, and available devices - phones, tablets, laptops, desktops. This step is critical because enabling user-friendly workflows that work with the user's existing devices is core to developing a successful rollout.

Common users' environments and equivalent suggestions include:

- Environments with users who primarily operate on mobile devices or tablets - Look into built-in unlock capabilities.
- Mixed device environments or environments that rely on a variety of SaaS tools - Leverage SSO provided by IDP or build flexible login workflows.
- Shared accounts - FIDO RPs can be configured to allow for more than one credential to be associated with a login. Investigate cross device hybrid authentication or roaming authenticators.

3.3.3 Recovery

Any authentication process is only as strong as its weakest point, which is why recovery processes have often been abused by attackers to compromise systems. Synced passkeys are durable credentials that can survive device loss and unintentional wiping by restoring from a passkey provider and reduce the need to perform account recovery to establish new credentials for the user. With passkeys, users are expected to lose their credentials less frequently. However, there may be cases where passkeys, or access to the passkeys, is lost, thus requiring account recovery.

For passkey implementations utilizing device-bound passkeys that cannot be backed up or recovered, account recovery should be performed using the backup authentication method, such as using a backup authenticator, to bootstrap enrollment of a new authenticator. In the event that a backup authentication mechanism is not available, organizations must provide alternative pathways to recovery. Organizations should take a risk-based approach to designing and implementing account recovery systems. The specific implementation details will vary widely depending upon organizational requirements. In general, recovery mechanisms should never depend on weaker factors than the credential that the user is trying to recover. In the case where passkeys need to be re-registered, organizations should design mechanisms, either automated or manual, to prevent the use of passkeys no longer registered to that user.

For passkey implementations where synchronized passkeys are used, be sure to document the bootstrapping/enrolment process for new devices as well as building a risk averse process (including identity proofing) for full provider account recovery or replacement. While these catastrophic events should be low, it may still be necessary to have users go through this process. Knowing the proper process ahead of time will insulate organizations against manipulations and stop work events.

For additional considerations around account recovery, please see the FIDO Alliance's Recommended Account Recovery Practices for FIDO Relying Parties. [5]

3.4 Admin Considerations:

Monitoring of implementation and adoption metrics are critical to ensuring the success of the deployment and ensuring that the security benefits of FIDO authentication with passkeys is realized. Below are recommendations for metrics and processes that are indicative of the success of enterprise passkey migrations.

3.4.1 Monitoring and Visibility into Utilization

Admins are strongly encouraged to use groups or other segmentation structures to allow graceful transition of subsets of users and applications to passkeys. Pilot populations should be carefully constructed and should be composed of a variety of end user types and levels in the organization. Monitoring the usage of items below, both before and after the migration, will provide critical insights into the effectiveness of the program and guide important adjustments.

- Device enrollment:
    - How long did it take the user to enroll their first device?
- Security events:
    - Where was the device at time of onboarding?
    - What, if any, identity proofing approaches were used to ensure that the correct user was onboarded?
    - If manager, IT support, or peer approval workflows were used, who provided attestation?
    - Are there any time of day or device location anomalies that did not previously exist?
- User authentication:
    - Was the user able to successfully authenticate?
    - Are there any observable changes in their daily authentication patterns that would suggest problems or added friction?
    - Does analysis of day-of-week and time-of-day suggest any issues?
- Key management:
    - Are keys being used as expected and only from known devices? Some authenticators support device attestation which provides key provenance and assurance of the identity of the authenticator. If the source of the passkey is an important security control for your implementation, be sure to verify if your chosen authenticator solution supports this kind of attestation.
    - How many keys are associated with an individual's account? Normal guidance would be to expect the number of passkeys associated with a user's account to be close to the number of devices that a user leverages. For example, if your users use Android phones & Windows laptops then you should expect to see two to three passkeys associated with a users' account, one stored on each platform authenticator, and possibly one backup from a security key. In this scenario if an account had five to six passkeys registered, then it would be time to investigate and potentially remove excessive keys. Every organization's definition of excessive may vary, and should be defined based on observations from their environment. Additionally, depending on your deployment, consider the number of applications that you have enabled for passkey authentication. If you deployed passkeys as credentials for an SSO integration, your users may only have one passkey per device. If you deployed passkeys on an application-specific basis, there may be one passkey per device per application. Organizations are recommended to monitor the number of keys associated with each user and use this data as context for informing passkey management.
    - Whose keys are associated with administrative/service/break-glass accounts? In the same way that it is best practice to segregate administrative access from normal user access, generating a separate set of passkeys for administrative accounts is also recommended. If they are shared, be sure to include rotation, monitoring, and good cleanup practices.
    - How will passkeys be removed? If an employee leaves the company or moves into a different role, their accounts should be disabled, deleted, or access should be evaluated and vetted. In situations where this is not reasonable due to legal requirements, passkeys should be promptly removed to prevent unauthorized account access as part of the disablement process. Similarly, if a user reports a device missing or stolen, any passkeys associated with those devices should also be removed.
- Compatibility assurance:
    - Do any combinations of applications and endpoint platforms show unusual changes or decline in authentication events?
    - Are all invocation methods for passkey authentication continuously functioning, including after upgrades?

4. Next Steps: Get Started Today

Enterprise organizations should consider migrating to FIDO authentication where possible.

- Use FIDO standards.
- Think about what your relying parties are supporting as well as your own enterprise security requirements.
- Passkeys are far more secure than traditional OTP mechanisms.
- Passkeys are far more secure than passwords. Look for the passkey icon on websites and applications that support passkeys.

For more information about passkeys, check out the FIDO Alliance passkeys resource page [6] and the FIDO Alliance knowledge base [7].

5. Acknowledgments

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

- Dean H. Saxe, Amazon Web Services, Co-Chair FIDO Enterprise Deployment Working Group
- John Fontana, Yubico, Co-Chair FIDO Enterprise Deployment Working Group
- FIDO Enterprise Deployment Working Group Members
- Dirk Balfanz, Google
- Jerome Becquart, Axiad
- Vittorio Bertocci, Okta
- Greg Brown, Axiad
- Tim Cappalli, Microsoft
- Matthew Estes, Amazon Web Services
- Rew Islam, Dashlane
- 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

6. Glossary of Terms

Please consult the FIDO Technical Glossary for definitions of these terms.

7. References

[1] FIDO Alliance Enterprise Deployment Whitepapers - https://fidoalliance.org/fido-in-the-enterprise/

[2] FIDO Alliance Enterprise Deployment Introduction Whitepaper - https://media.fidoalliance.org/wp-content/uploads/2023/06/June-26-FIDO-EDWG-Spring-2023_Paper-1_Introduction-FINAL.docx.pdf

[3] Forrester Report of Total Economic Impact of YubiKeys - https://resources.yubico.com/53ZDUYE6/at/6r45gck4rfvbrspjxwrmcsr/Forrester_Report_Total_Economic_Impact_of_Yubico_YubiKeys.pdf?format=pdf

[4] High Assurance Enterprise FIDO Authentication - https://media.fidoalliance.org/wp-content/uploads/2023/06/FIDO-EDWG-Spring-2023_Paper-5_High-Assurance-Enterprise-FINAL5.docx-1.pdf

[5] Recommended Account Recovery Practices for FIDO Relying Parties - https://media.fidoalliance.org/wp-content/uploads/2019/02/FIDO_Account_Recovery_Best_Practices-1.pdf

[6] Passkeys (Passkey Authentication) - https://fidoalliance.org/passkeys/

[7] FIDO Alliance Knowledge Base - https://fidoalliance.org/knowledge-base/