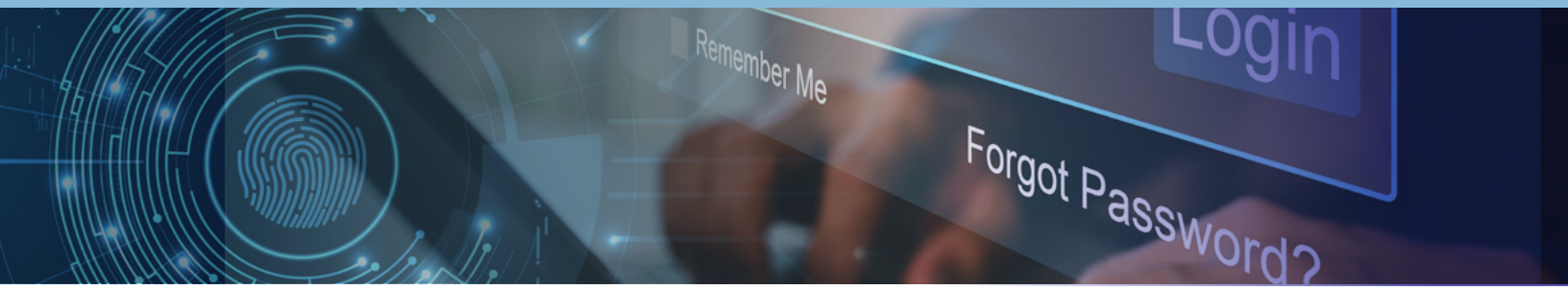
Passwordless:
A Remedy for Better Security and MFA Fatigue

TLP:WHITE This report may be shared without restriction.

Contents



Scope Statement

Nowadays, people cannot universally agree on anything except maybe one thing: passwords are a pain. Make them unique, strong, long — but not too long — don't forget the special characters and numbers. Passwords cannot in any way resemble any other password that you've used in the past and should not be a common word either. Combine the poor user experience with the fact that 83% of breaches are linked to compromised credentials and it's just awfulness all around.

And when organizations add multifactor authentication (MFA) to the mix — to cover up for the inadequacies of passwords alone as an authentication factor — the challenge shifts. Individuals still need to enter the long, complex passwords and then also respond to a push notification or enter a one-time passcode (OTP) to gain access to resources, potentially multiple times a day depending on how an organization's identity and access management (IAM) system is configured.

On the consumer side, the challenges are bigger. If a company's website or app delivers a bad authentication user experience, consumers are less likely to do business with that company and may even jump to a competitor. Additionally, protecting consumer and patient data is critical so controls need to be in place to secure that information.

There is good news here: Passwordless technology has matured significantly over the last few years and is gaining momentum. Standards have been defined to make it easier to deploy the technology across platforms to make it easy and secure to access systems.

This paper will define passwordless technologies and how healthcare organizations can deploy the authentication technology for patients and in the enterprise. It will also include case studies on different passwordless implementations.

Key Takeaways

- **Passwordless authentication** can improve a healthcare organization's security posture.
- **Not all passwordless technology is the same:** there are a handful of different passwordless technologies available.
- **Your organization can benefit from others that have implemented passwordless authentication before you;** there are many lessons learned and best practices to share.
- **Shifting to passwordless technology brings a number of change management issues,** particularly around conditioning your users to adjust to life without passwords.

Defining passwordless technology

At a high level, "passwordless" means any authentication technology that does not require a password. In practice, that means an authentication solution that dispenses with "something you know" and instead uses "something you have" and/or "something you are." This might encompass a range of technologies, including:

- **Biometrics — face, finger, and iris being the most common.**
- **Hardware tokens — security keys, smart cards, mobile devices.**
- **One-time passcodes — random digits that are either generated by an app or sent via text message.**
- **Passkeys — a modern technology that uses asymmetric public/private cryptographic key pairs, often paired with an on-device biometric match.**
- **Combinations of the above — using a mobile device and biometric verification to authenticate and enable access.**

In healthcare clinical settings today, it is common for someone to log into a workstation using their fingerprint or face, which is checked against a central database of biometrics.

More commonly today, passwordless technology uses solutions like passkeys, which combine the security benefits of asymmetric public-key cryptography with a user experience that is simpler than legacy authentication solutions.

With passkeys, the private key is stored with the individual in secure hardware inside a computer or mobile device or can be carried in a separate hardware token like a security key. Once the individual authenticates to the mobile device, computer, or token, the private key is unlocked, and a signed assertion is relayed to the relying party to enable access. Passkeys are built off of the phishing-resistant passwordless standards from the FIDO Alliance, which includes the Web Authentication (WebAuthn) standard housed in the World Wide Web Consortium (W3C).

Passkeys are FIDO credentials that can be found by browsers or stored within native applications or security keys. Passkeys replace passwords with cryptographic key pairs for phishing-resistant authentication and a better user experience. The cryptographic keys are used from an individual's devices — computers, phones, or security keys — for authentication.

There are two types of passkeys: synced and device bound. Synced passkeys are managed by a mobile device, or computer operating systems, and are synced between the devices via the cloud. The cloud service also stores an encrypted copy of the FIDO credential. Device-bound passkeys are only available from a single device such as a security key and cannot be copied.

The risk and use case will dictate which passkey should be used, but in most cases, synced passkeys will be viewed as more appropriate for consumer-facing applications than enterprise ones. Organizations should conduct a digital identity risk assessment to determine which passkey to deploy. For many use cases synced passkeys are acceptable but for others — particularly ones for access to sensitive information or applications — device-bound passkeys may be necessary. Also, some organizations may not be comfortable having backup credentials in the cloud.

Apple, Google, and Microsoft all support passkeys on mobile devices and within their browsers. From a user experience perspective, individuals are given the option of enrolling a passkey instead of a password. For synced passkeys, consumers scan a QR code with their mobile device and the passkey is stored. When authenticating, an individual will click on the passkey login button, scan the QR code, and then use the biometrics or PIN from the mobile device to unlock the passkey and gain access. For device-bound passkeys the registration and login flows are similar but instead of scanning a QR code individuals use the token associated with the account.

Passkeys also offer phishing resistance, as they are only sent to the site or application that was registered. If someone clicks on a phishing link the passkey won't be asserted.

ENROLLMENT

Individual is prompted to enroll in passwordless authentication.

Public/Private key pair is generated. Private key is stored on secure hardware, or token. Individual uses biometric, mobile device, or token for future authentication events.

Public key is sent to the relying party and registered to the user for authentication.

AUTHENTICATION

Individual wants to access site using passwordless authentication.

Individual uses biometrics, mobile device, or secure token to validate identity.

Private key is unlocked and generates a signed assertion.

Assertion is sent to the relying party and access is granted.

Case Study: Large healthcare provider uses passkeys for customer access

One of the largest healthcare providers in the U.S. enables customers to conduct a range of transactions via its website and because of that it was often the target of credential stuffing attacks, the automated injection of stolen usernames and passwords into website login forms, to attempt to gain access to user accounts. Attackers use username/password combinations from previous breaches as many people reuse the combinations in hopes of gaining access to new accounts.

With the barrage of credential stuffing attacks, the provider looked to passkeys as a solution. The healthcare organization did a limited rollout on its website in April 2023 followed by full deployment there and then expanded it to some of its other applications. Passkeys have been rolled out on the websites only, not the mobile apps.

As of January 2024, some 4 million consumers have enrolled a passkey to access the provider's site without any password. While this is a small percentage of the 70 million consumer accounts, it was achieved without any marketing or outreach. The healthcare provider is happy with the progress and plans to introduce passkeys for its mobile app in 2024 as well as for the other brands.

Additionally, the provider is refining the user experience for passwordless, making it easier to learn and use passkeys.

Case study: Healthcare software provider goes passwordless

One large U.S.-based healthcare company made the decision to go passwordless but in the end, made the conscious decision to avoid calling it that. "It became a hot button because people started thinking it was less secure," an executive said.

A one-size-fits-all approach for this company was not possible as the use cases were numerous — including logistics and delivery centers where mobile devices are not allowed — ruling out push-based MFA. With mobile devices out of the running, the company looked at the FIDO2 specification from the FIDO Alliance and security keys.

With FIDO2 technology baked into Windows Hello and Apple Touch, the company ended up introducing passwordless throughout the enterprise for those opting to use a security key. Employees still have the option to use push-based MFA and a password. Passwords remain the most popular choice due to familiarity.

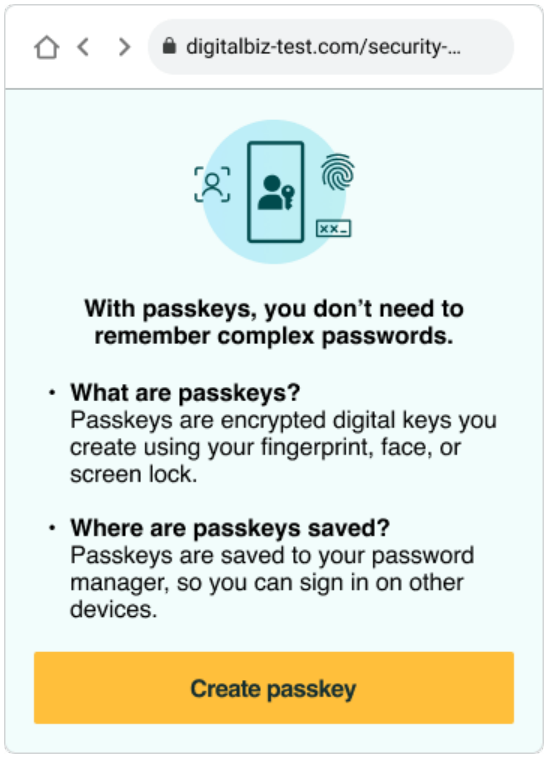
Change management and user experience

While everyone probably dislikes passwords people still often choose that route because of familiarity. For generations, we have been taught that passwords equal security. Combine that with messaging around multifactor authentication, individuals think that entering a password, hitting a button on a mobile device or entering a six-digital code is the ultimate security.

Passwordless technology removes all of the typical actions it takes to access applications and resources. For an individual not familiar with the underlying technology this can be confusing and causes them to think that there is less security instead of more. That's why using the term "passwordless" might not be the best idea when rolling out the new authentication technology as they might think it's not secure.

The FIDO Alliance hired cognitive psychologists to research how individuals react to the different authentication prompts and create a user experience based on that research. Technologists and others in the security field thought that passwordless should be touted for its security benefits but it's really ease of use.

Creating messaging that is short and simple to understand is critical. FIDO's user experience committee created a hero prompt (see right) as an example of some of the messaging that should be done when enabling individuals to create passkeys. The fingerprint and face verification images are key as individuals are used to seeing them and helps create familiarity.



The FIDO Alliance created User Experience Principles to help with adoption for organizations implementing passkeys.

	Summary	Details
1	Prompt to create passkeys alongside account-related tasks.	When people are already in an account management mindset — such as, account creation, account recovery, or as part of account settings — they are more likely to perceive the option to create a passkey as a relevant enhancement to their site experience, rather than an unwelcome interruption or barrier to accomplishing other core site tasks, such as shopping. Prompting to create passkeys during the sign in experience did not perform as well.
2	Associate the unfamiliar (passkeys) with the familiar.	Passkeys is a new term, a new visual symbol, and a new authentication method for consumers. Whenever possible, help them understand the nature and value of passkeys by associating them to familiar concepts, visuals, and experiences. For example, biometric experiences are familiar.
3	Use proven passkeys messaging and icons before and after OS dialogs.	Before triggering the passkeys operating system (OS) dialogs, display passkeys messages, icons, and actions related to the status of the current task. After the passkeys OS dialogs are completed or dismissed, show the resulting status of the task using messages and icons. This provides a "handshake" between the relying party (RP) website and the OS dialogs and clarifies how the OS and RP are working together to optimize account access and security through passkeys which helps build people's trust and interest in the new concept of passkeys.
4	Allow freedom and choice related to passkeys.	For consumers to remain in control of their experience and to engender trust with your brand, provide clear options related to creating and managing passkeys. Allow them to create accounts with or without a passkey. Allow them to create a new password upon password reset or create a passkey instead.
5	Follow accessibility principles before and after the use of passkeys.	Passkeys are most accessible when they are presented to users in ways that they can perceive, are operable using assistive technologies, and are understandable to users with a variety of functional needs throughout workflows in their journey with passkeys. Comply with accessibility guidelines such as the Guidance for Making FIDO Deployments Accessible to people with Disabilities and the underlying Web Content Accessibility Guidelines (WCAG).
6	Use a passkey hero prompt consistently across the customer journey.	Create a "hero" for passkeys which includes specific symbols, headline, messaging, and call to action. Consistently use the full hero content at account-related moments in the customer journey. For example, use the complete hero versus using only a "Create passkey" button.

	Summary	Details
7	Persist helpful information about passkeys.	Keep helpful information about passkeys in the human interface, without requiring additional clicks to see it. For example, retain the passkey "what," and "where" messages in the hero messaging in account settings even after a passkey is created. Display the text by default and do not hide it beneath extra clicks. Here's another example: because people should be given the choice to disable passkeys, but they may not understand how they will sign in without them, place the short description of what disabling passkeys will do next to the "Disable passkeys" link. Persist this description in the human interface. For example, don't put this information in a tooltip that is exposed only upon hover.
8	Make passkeys a primary option in account settings.	Match the display and interaction model for passkeys with that of other authentication items such as username, password, or 2FA within a person's Account Settings. For example, if other sign in options within Account Settings are labeled with an H2 heading, then label "Passkeys" with an H2 heading, too.
9	Display "passkeys cards" with meaningful content to give shape to passkeys.	Unlike passwords, which are tangible combinations of letters, numbers, and symbols, digital passkeys are invisible to people. Display a passkeys card affordance in Account Settings. Inside the card include the passkey icon, messaging, and options that inspire trust and reassures people that their passkeys are active, available, and manageable. If someone has two or more passkeys, each passkey has its own card.
10	Plan your UX in accord with your unique security and business needs.	The guidelines focus on UX concepts that are unique to FIDO with synced passkeys. You will see various forms of identity proofing and non-FIDO authentication examples throughout this work. The guidelines do not intend to prescribe security guidelines for identity proofing or other non-FIDO authentication mechanisms as they are unique to each RP and based on their own unique business needs and security policy. Throughout the guidelines, look for this symbol which indicates where your own security policy and business drivers come into play.

Source: FIDO Alliance UX Principles

Consideration for implementing passwordless authentication

At its core passwordless authentication is the same — a system that uses asymmetric cryptography to replace passwords. But a major difference is the mechanism used to unlock the private key and send the assertion to the relying party. Some tout one-time passcodes — either text messages or those generated from a token — and push-based notifications as password replacements but those codes can be phished, and MFA fatigue attacks have become common, so these modalities do not offer the highest level of security or best user experience.

As generative AI enables realistic phishing campaigns at scale, the need for phishing resistant MFA is more important than ever before. Any passwordless implementation should use technology that is phishing resistant, such as an external hardware token, mobile device or secure enclave on a computer.

Organizations should conduct a digital identity risk assessment to choose the best authenticator for the use case. For example, a passkey is an appropriate authenticator for access to consumer transactions on a website. But a government employee accessing controlled unclassified information on a government computer would require a hardware token for access. The risk assessment should include a review of any applicable regulatory requirements or frameworks to determine if there are any requirements that could influence the decision on which authenticator to use.

Conducting the risk assessment will help organizations determine which passwordless authenticator is best for each use case. There may be use cases within an enterprise that require good old multifactor authentication, which may still mean passwords and additional phishing-resistant authenticators. For example, privileged access management use cases are unlikely to deploy passwordless any time soon.

It's also important to layer security. Passwordless provides a first line of defense, but organizations should have risk-based technologies underneath that can provide extra security. These systems check the device that is being used, the IP address, and a variety of other attributes and metadata that are checked against previous behaviors to spot anything anomalous. For example, if a company's chief financial officer typically logs in from the office or a home office between 8 am and 6 pm time using a specific laptop or mobile device and then requests for access are coming at 4 am from an unknown laptop or mobile device thousands of miles away, that access request might need additional authentication to enable access.

Resetting lost or forgotten credentials is also an important step to consider in the journey to passwordless authentication. Organizations should ensure that identify validation practices provide a high level of confidence of the individual's identity prior to resetting the credential. Organizations should require a high level of confidence prior to resetting MFA.

Lastly, while passkey is a standard and adopted by Apple, Google, and Microsoft, each of the platform's implementation of passkeys are slightly different. The underlying technology is the same but when using synced passkeys across platforms — from an Apple to a Microsoft to an Android — there may be some idiosyncrasies that are being worked out. Organizations implementing passkeys should be aware and know these eccentricities exist and be prepared to help consumers troubleshoot.

Next Steps

The first step an organization should take when implementing passwordless is to check with their identity and access management provider. Many of the modern vendors support passwordless and passkeys so it's a matter of some configuration changes and development time to implement.

The development cycle will be a fraction of the time compared to educating your users. This change management may vary depending on the implementation — consumer rollout could be much simpler depending on how much the implementation is being marketed — versus an enterprise deployment where employees are mandated to make the switch.

If it's an enterprise rollout for workers that's a different story. Materials will need to be created, and educational seminars held to inform employees about the technology, how it works, and what will be different.

Ultimately, implementing passwordless authentication is less of a technology implementation and more about managing the people and processes that go into it. Changing decades of engrained behavior based on passwords is the biggest hurdle to overcome.

Health-ISAC's Whitepaper Series for CISOs on Identity Access Management

This whitepaper is part of the series for CISOs on Identity Access Management. In cybersecurity, identity is suddenly more important than ever before. The series of Health-ISAC whitepapers is designed to provide CISOs — and the broader healthcare community — a holistic guide on how to best approach Identity and Access Management (IAM) and its role in managing cybersecurity risk. The series provides an explanation of key concepts, outlines a framework and best practices, investigates the various identity solutions, and highlights the aspects of effective implementation.

The whitepapers can be found here: https://h-isac.org/ciso-identity-whitepaper-series/

Feedback on this white paper and suggestions for future topics are encouraged and welcome. Please email us at **contact@h-isac.org**