yubico

WHITE PAPER

Going passwordless in a passkey age

Key lifecycle management considerations when building a secure passwordless strategy

Contents

Executive Summary

Say the word “passwordless” to a room of security professionals and you will get a range of reactions. That’s because passwordless is an evolving concept, influenced by available technologies, evolving cyber threats, and myriad use cases. The purpose of this white paper is to strip back the buzz around passwordless and provide real guidance on how enterprises can evaluate passwordless authentication options in the age of passkeys. Naturally this means that we will have to first have a conversation about passwords and multi-factor authentication (MFA), and then with a solid understanding of the current landscape and risk we can dive into how to address and mitigate current and future issues with a sound passwordless deployment.

Not all MFA is created equal

Passwords remain the most common form of user authentication, used by 91% of organizations.[5] They continue to resonate because they are a form of authentication that can be applied to almost anything—ticking the box on portability, compatibility and interoperability across devices. What passwords have never offered is adequate security.

A password is a shared secret. The secret is known by the user and the validation service, is often stored across various computing devices, and may even be shared in messages or on a sticky note. Relying on password-based authentication leaves organizations open to attack since passwords are easily hacked, stolen, or simply guessed. There are also hidden **governance and support costs** associated with passwords and legacy MFA. Large organizations are estimated to spend up to $1 million each year in staffing and infrastructure to handle password resets.[6] The global average for a breach is $4.45M USD if a password is compromised, and can be much higher based on the size of the organization.[7] On top of this, consider user frustration associated with passwords and obtuse complexity requirements, and it's easy to see the benefits, both for useability and cost reduction, to getting rid of passwords.

While any form of MFA offers better security than a password alone, **not all MFA is created equal.** Basic or legacy forms of MFA such as SMS, mobile authentication, email 'magic links' and one-time passcodes (OTP) can be easily bypassed by malicious actors, as they are also shared secrets, making them vulnerable to account takeovers from phishing, social engineering and attacker-in-the-middle attacks at an attack penetration rate of 10-24%.[8]

In the move away from problematic passwords and phishable MFA, 66% of organizations report they are piloting, have deployed, or are planning to deploy **passwordless authentication**.[9] Going passwordless is a journey for most organizations—the first step is often moving away from legacy forms of MFA, and moving to strong phishing-resistant MFA with the FIDO2/WebAuthn standard. Once there, organizations are poised to leverage FIDO2 passwordless-enabled credentials, now known as passkeys, to complete their **passwordless** journeys.

Today, many passkey implementations on the market focus on the user experience of authentication; they unfortunately skip critical focus on **account lifecycle management**, including device registration and account bootstrapping. Many vendors also default to passwords and legacy MFA, creating attack points that bypass the intended security of phishing-resistant MFA solutions and undermining **Zero Trust**, which progresses toward exclusive use of phishing-resistant MFA.[10]

In order to ensure a secure bridge to passwordless, this white paper will outline **critical implementation factors to consider on the journey to passwordless using passkeys** to ensure strong security across the entire authentication lifecycle.

74%

of data breaches traced back to the human element e.g. social engineering phishing attacks, privilege misuse[1]

60%

of compromise factors in enterprise cloud environments are due to weak passwords or leaked credentials[2]

66%

of enterprises have / piloting / planning passwordless authentication within the next year[3]

50%

of the workforce will be passwordless by 2025[4]

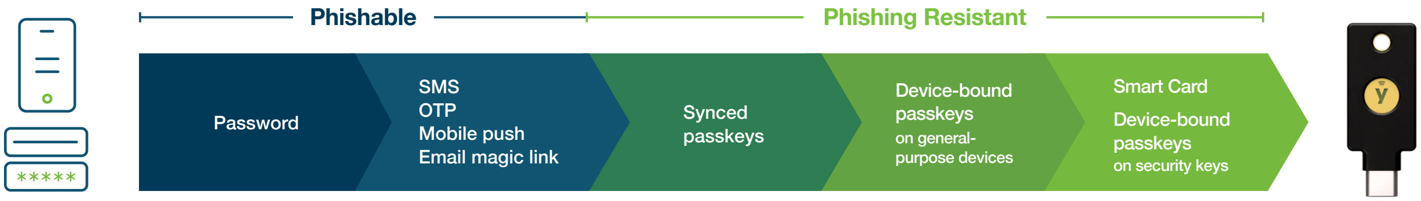
What is passwordless authentication?

Passwordless is any implementation of authentication that doesn't require the user to create and/or provide a password during **any part of the authentication lifecycle**, including:

Legacy passwordless lifecycle	Modern passwordless lifecycle				
User login	Onboarding / registration	First login	Federation and Single Sign On	Account recovery	Authenticating to legacy systems

Over the past few years, the term "passwordless" has gained momentum and now it is used by many security, authentication, and identity solution providers. As with other buzzwords in the industry, the term "passwordless" is not strongly defined, leading to an ecosystem where **not all passwordless implementations provide the protection and ease of use proposed by the term**.

Many instances of passwordless rely on the legacy definition of passwordless: any form of authentication that doesn't require a user to provide a password at login. This definition allows for many legacy MFA solutions such as **SMS** verification and **email magic links** to be considered "passwordless," when these solutions are both outdated and highly susceptible to account takeovers. Furthermore, this legacy passwordless definition lacks the nuance to ensure that **phishing-resistant authentication implementations** are **not falling back on passwords or legacy MFA** during device registration, account bootstrapping or authenticating to legacy on-premise systems. Additionally, a secure passwordless solution still needs to provide multiple authentication factors to protect access when a device is stolen such as a PIN or biometric factor.



25%

of MFA transactions using a token will be based upon FIDO authentication[11]

Passwordless authentication based on **Smart Cards or FIDO2** (FIDO2 credentials represented now through **passkeys**) fundamentally changes how authentication factors are processed. In a passwordless model, the validation of the first factor and second factor shifts solely to the authenticator. Typically the first factor is physical possession of the authenticator itself, and the second factor is the PIN or a biometric validation to unlock the authenticator and perform the cryptographic operation.

Given that this "truer" definition of passwordless authentication shifts much of the authentication process to the authenticator, it is vitally important to ensure the private key is secured so it cannot be stolen or cloned and equally vital to know that the factor is actually being used in all authentication scenarios.

Before detailing the implementation considerations to ensure modern, strong passwordless, let's take a step back and better **define phishing-resistance and passkeys**, which are the foundation of today's passwordless deployments.

What is phishing-resistant MFA?

In response to risk and regulatory requirements, organizations are deploying **phishing-resistant MFA** in the form of **Smart Cards (PIV/CAC)** and the modern **FIDO2/WebAuthn.**

NIST defines phishing-resistance in Special Publication (SP) 800-63 and Draft 800-63-4[12] as "the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an impostor relying party without reliance on the vigilance of the subscriber." Phishing-resistant MFA processes rely on cryptographic verification between devices or between the device and a domain, making them immune to attempts to compromise or subvert the authentication process.

Smart Cards (PIV/CAC) are one of the most effective ways to protect against phishing. The user must insert their Smart Card into a reader, and validate the Smart Card with a unique PIN. A PIN remains local to the device, is never transmitted, and never has to be changed, making it more secure than passwords. Where Smart Cards are not a practical solution—due to cost, access to cloud services, mobile devices, air-gapped/isolated networks, contractors, or for partners and third-parties—organizations are looking to FIDO2 and modern passwordless login flows.

The **FIDO2/WebAuthn** authentication standard is designed to support modern cloud-based environments at scale. FIDO2/WebAuthn is the most recent iteration of the FIDO standard, which leverages devices to easily authenticate to online services. With FIDO authentication, users sign in with phishing-resistant credentials known as **passkeys** alongside verification using a biometric or a unique PIN.

Passkeys

are a new name for **FIDO2 passwordless-enabled credentials**

What are passkeys?

Passkeys are a new term in the industry, but the concept is not new. Passkeys are a new name for **FIDO2 passwordless-enabled credentials**, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences. There are different passkey implementations:

Synced passkeys live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. While synced passkeys enable easier credential recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track, so it is suitable for lower security assurance scenarios.

Device-bound passkeys offer enterprises greater control of their FIDO credentials compared to synced passkeys. However, there are different types of device-bound passkeys—those that reside in general purpose devices such as smartphones, laptops and tablets, and those that reside in hardware security keys purpose built for strong security. Device-bound passkeys in modern FIDO security keys offer the highest security assurance and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach enterprises can deliver the simplest user onboarding and credential recovery experience across devices and platforms, all while staying in compliance with the most stringent requirements across industries.

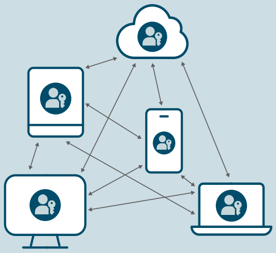
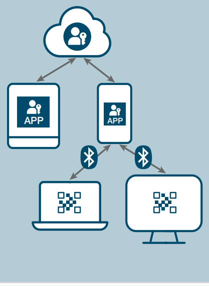
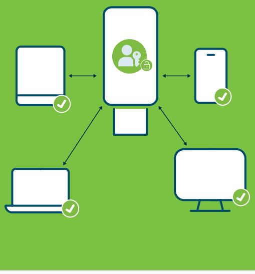
Which passkey approach is right for you?

FIDO standards and **passkeys have been embraced** by all leading Identity and access management (IAM) platforms, identity provider (IDP) solutions and privileged access management (PAM) solutions to make it possible to support FIDO2 passwordless experiences at scale for business critical applications and services.

Syncable passkeys are great solutions for many low-risk consumers and low-risk applications as they are considered lower assurance, but are generally not suitable for high risk individuals or the enterprise, increasing the difficulty to:

- **Audit** and prove how passkeys are being synced or shared and to know which copy is being used
- Manage the **lifecycle** of the passkey after it has been created, since cloned passkeys that are shared are indistinguishable from the original.
- **Support** users that can't sign-in with their passkey or when they need help with recovery.
- Cover all **use cases**, since syncable passkeys rely on mobile connectivity, making them unsuitable for mobile-restricted environments, air-gapped or isolated networks, shared workstations. Furthermore, not all computers and phones support passkeys.

Device-bound passkeys do not sync or get copied to other devices. In a synced passkey scenario where passkeys can move between multiple devices, the factor that is used to unlock the authenticator could be from a different user as all factors don't travel with the passkey. With a device-bound passkey, there is a higher assurance that the user who is controlling the device is the one who is supposed to be using the passkey, eliminating the risk that the factor used to unlock the authenticator could be from a different user. A device-bound passkey offers higher assurance because the passkey lives on FIDO2 security keys or are created on a platform and persisted into a trusted platform module (TPM), which is how Windows Hello works. Device-bound passkeys provide the best enterprise-level controls that organizations need to properly manage and secure the lifecycle of a passkey, leveraging public key cryptography for high security, where the private keys never leave the authenticator.

If you need	Synced passkeys 	Device-bound passkeys on general-purpose devices 	Device-bound passkeys on hardware security keys 
Synced/shareable between devices	Unmanaged syncing	Managed syncing	No syncing between devices
Works across Apple/ Google/Microsoft	May not work	Works across all platforms	Works across all platforms
User registration/onboarding	Weak; backed by password	Weak; app backed by password	Most secure when used with Yubico FIDO Pre-reg, as then user registration not reliant on password
Credential recovery	Easy to recover	Time to replace phone and costly	Fastest with a backup key
Compliance and audit	Authenticator Assurance Level 2 (AAL2) No attestation; unsure if user controls passkey	Authenticator Assurance Level 2 (AAL2) Supports software attestation	Authenticator Assurance Level 3 (AAL3) Supports hardware attestation
Risk/Costs	Perceived as “free”; high IT/ helpdesk costs and higher risk exposure is costly	Perceived as cheaper than HW; but risk exposure gaps can be costly in long run	Perceived as higher cost upfront; but less costly due to lowered breach risk and reduced IT burden
Works across enterprise scenarios	Not in mobile-restricted, shared workstations	Not in mobile-restricted, shared workstations	Works across all enterprise scenarios

How to choose the right passwordless strategy for your organization

Every company is parked at a different mile marker on the road to passwordless. But every move away from passwords, no matter how small, is going to improve security because we know that a password-focused environment will always be more phishable and less safe.

There are two questions worth asking to determine how to plan your journey to passwordless:

- **Do you operate in the cloud, on-premises, or a hybrid environment?** It may be comforting to know that no matter what type of technical environment you have today, you can take advantage of one or more secure passwordless options available to you.
- **How do you prioritize security levels, user experience and compliance cost?** These elements are sometimes in conflict, so it's worth knowing how you will negotiate the trade-offs if you have to make tough choices.

These questions will help you determine the best path in moving away from legacy MFA towards passwordless leveraging Smart Cards, passkeys or a hybrid approach. Further, the question will help you evaluate passkey and authenticator options that match your security appetite and create an implementation strategy that fits your risk profile.

> "By moving to passwordless, you're eliminating the forgetfulness of users. You don't have to worry about them getting locked out, writing passwords on a piece of paper, or falling prey to a phishing attack. You remove the human element."
>
> **Jason Rucker** | Director of IT | City of Southgate, MI

Smart Card

If you are operating in an on-premises Active Directory (AD) environment or use legacy on-premise systems, then a Smart Card passwordless implementation is probably your best choice. Consider the benefit of hardware-based security keys to eliminate the need for Smart Card readers.

Passkey

If you have already transitioned to a cloud-first environment such as Microsoft Entra ID, then you'll be able to easily implement passkeys to use Office 365 and other federated enterprise applications.

Hybrid

In a hybrid environment, it's possible to implement both a Smart Card implementation and passkey depending on business use cases.

Which passkey authenticator is right for you?

Passkeys are an attractive option to secure and simplify user authentication experiences to modern work environments. Passkeys make credentials harder to exploit and unauthorized access much less likely, thanks to the use of public key cryptography, and are increasingly common within Apple, Microsoft and Google ecosystems.

While the passkey definition specifies that cryptographic keys are used for login rather than passwords, there are significant differences between **synced passkeys** and **device-bound passkeys**—and further between device-bound passkeys on **general-purpose devices** such as those created on a Windows platform and persisted into a trusted platform module (TPM) using Windows Hello versus those on **purpose-built security keys** such as the YubiKey.

The choice in authenticator determines how well you have **control of the passkey**:

- **Security keys** create passkeys on dedicated authenticators that are portable, allowing you to bring your passkey from workstation to workstation and to your mobile devices to seamlessly sign-in on any platform. Security keys provide the strongest assurance that the private keys are created and always remain on the authenticator on which they were created. Security keys that support both FIDO2 and Smart Card are a critical bridge to passwordless, supporting both legacy and modern environments.
- **Platform authenticators** are supported by secure enclaves that are built-in to the devices that you are already using for productivity and are frequently used with the biometric sensors that are available on the device. The passkeys that you create on the platform may be syncable or device-bound, depending on the platform that you are using.
- **3rd party passkey providers** are software authenticator apps and password managers that can create and store passkeys in the vaults managed by the 3rd party provider. Most 3rd party passkey providers leverage syncable passkeys, but emerging options will be able to hold device-bound passkeys.

The authenticator needs to ensure that processes it performs are secure and key material cannot be copied off the device. If it can be, a cloned authenticator could be developed and used to authenticate.

In addition, **authentication assurance levels (AALs)** classify the strength of authenticators. An authenticator at AAL1 (e.g. a password) provides low confidence while an authenticator at AAL3 provides very high confidence that someone logging onto your system can prove, by possession, who they are claiming to be, reducing the threat of compromise and attack from phishing.

In order to understand the security properties of an authenticator, relying parties should check device attestation statements. **Attestation** enables each relying party to use a cryptographically verified chain of trust from the device's manufacturer so that access decisions can be made based on a risk profile. Attestation information should be captured so current and future decisions can be made, up to and including blocking, if issues arise. The attestation keys are set at manufacturing time and cannot be altered or exported. **Only device-bound passkeys can offer enterprise attestation capabilities**.

	Synced (more focused on usability; less security)	Device/hardware bound (higher security assurance; not all are built equal)	
Platform	iOS OS X android	Windows Hello	Security key YubiKey
3rd party application providers	DASHLANE 1Password	Microsoft Authenticator	

How to cultivate phishing-resistant users

Account lifecycle management considerations

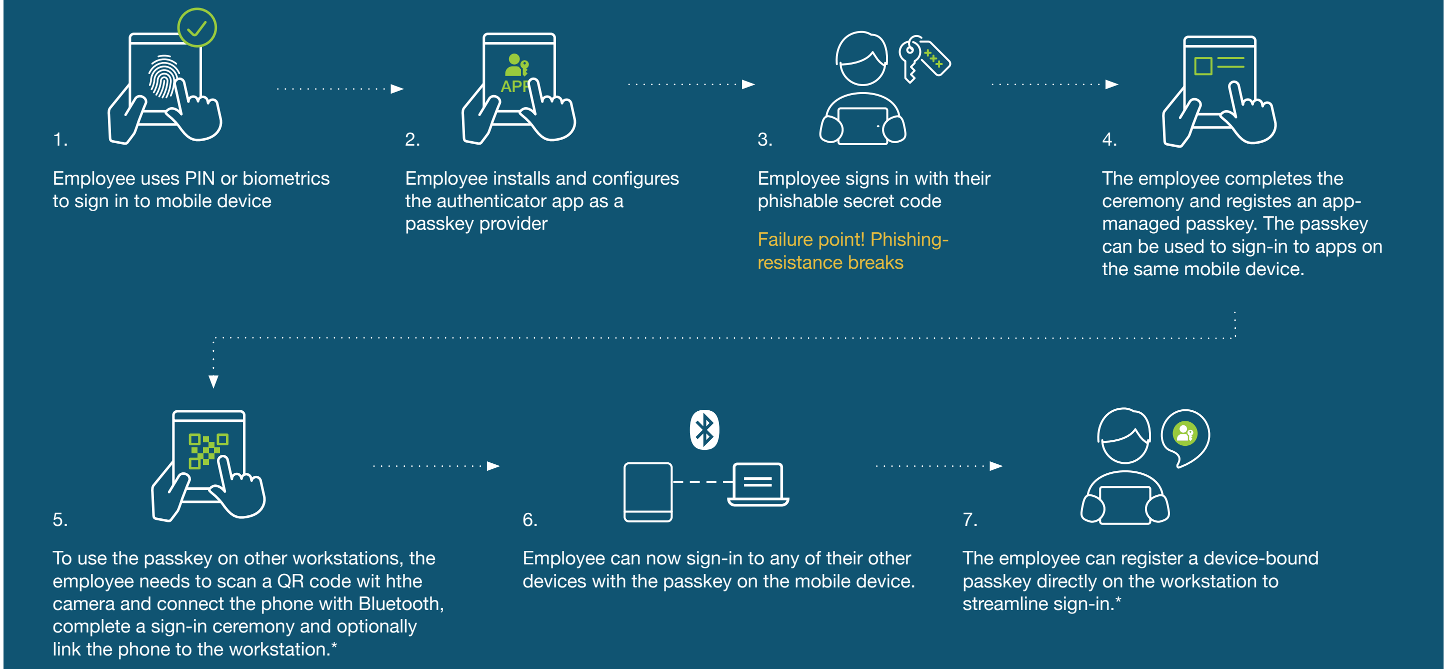
All passwordless solutions require organizations to establish a relationship that registers the Smart Card or passkey, to establish trust that the user is who they say they are. Most organizations establish Smart Card relationships in-person, but this is more challenging for passkeys, which typically rely on self-service registration. Many implementations will fall back on passwords or legacy MFA for this stage of the authentication lifecycle, undermining efforts toward Zero Trust.

Secure passwordless implementations consider the entire authentication lifecycle, considering not just **phishing-resistant authentication** but rather **phishing-resistant users**. This shift includes a broader consideration for strong authentication that moves with the user and closes gaps related to onboarding, bootstrapping, first login, or authentication to legacy systems.

> “The only effective approach to removing phishing from an organization’s threat landscape is to ensure that every user and process within the organization becomes phishing-resistant.”
>
> **Derek Hanson** | VP Solutions Architecture and Alliances | Yubico

Onboarding 3rd party passkey providers; device-bound passkeys on general purpose devices

A day in the life of a new employee getting onboarded using device-bound passkeys residing in a general purpose device, such as a smartphone



1. Employee uses PIN or biometrics to sign in to mobile device

2. Employee installs and configures the authenticator app as a passkey provider

3. Employee signs in with their phishable secret code

Failure point! Phishing-resistance breaks

4. The employee completes the ceremony and registes an app-managed passkey. The passkey can be used to sign-in to apps on the same mobile device.

5. To use the passkey on other workstations, the employee needs to scan a QR code wit hthe camera and connect the phone with Bluetooth, complete a sign-in ceremony and optionally link the phone to the workstation.*

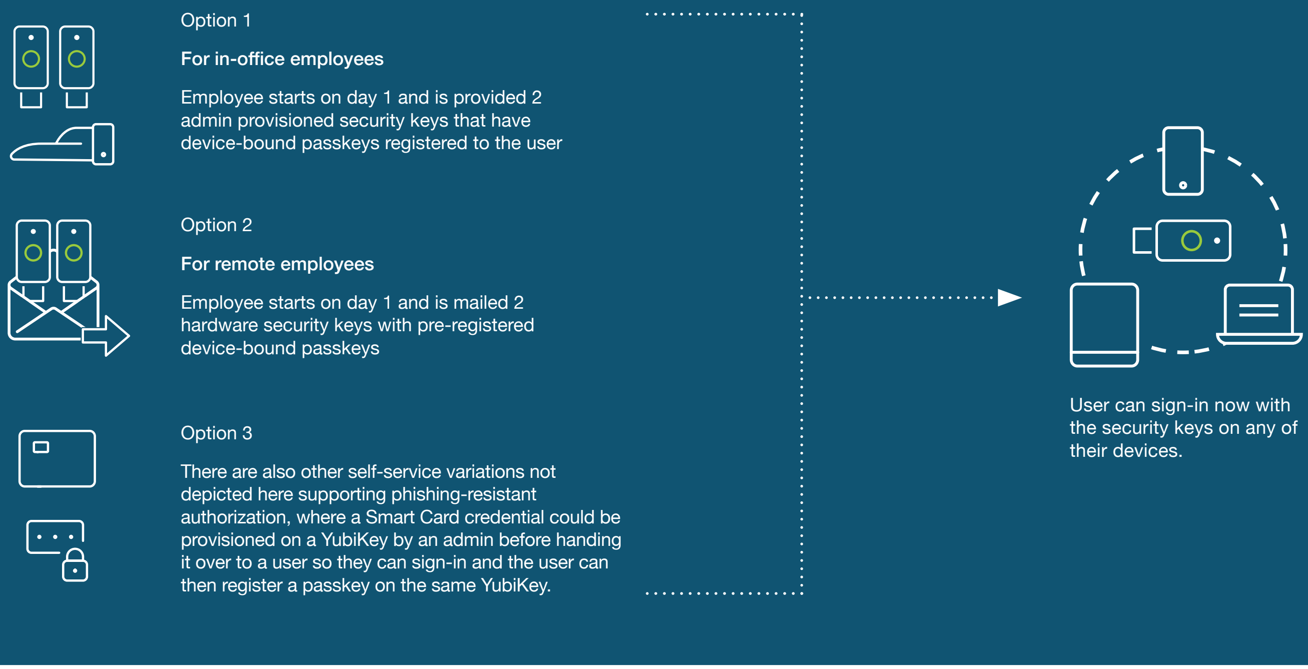
6. Employee can now sign-in to any of their other devices with the passkey on the mobile device.

7. The employee can register a device-bound passkey directly on the workstation to streamline sign-in.*

*where supported by the device and use-case

Onboarding Security keys; device-bound passkeys on authenticators built for security

A day in the life of a new employee getting onboarded using YubiKeys



Option 1

For in-office employees

Employee starts on day 1 and is provided 2 admin provisioned security keys that have device-bound passkeys registered to the user

Option 2

For remote employees

Employee starts on day 1 and is mailed 2 hardware security keys with pre-registered device-bound passkeys

Option 3

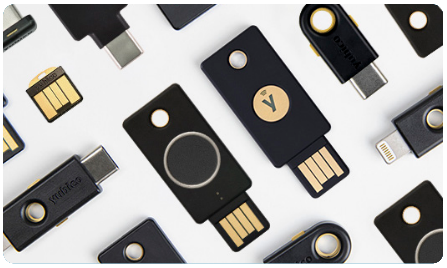
There are also other self-service variations not depicted here supporting phishing-resistant authorization, where a Smart Card credential could be provisioned on a YubiKey by an admin before handing it over to a user so they can sign-in and the user can then register a passkey on the same YubiKey.

User can sign-in now with the security keys on any of their devices.

Within FIDO2, user verification ensures that the person authenticating to a service is in fact who they say they are for the purposes of the service and is in control of the private key credential. The user is authorized to verify their identity by entering a PIN or a biometric, like a fingerprint via a prompt on the client. The authenticator performs user verification and responds to the relying party that verification was successful in a way that is cryptographically verifiable. When using a FIDO2 credential for the passwordless flow, user verification needs to be set to “REQUIRED” and the IDP has to check for and enforce it.

Creating phishing-resistant users ensures that for every authentication task, the user will use a phishing-resistant MFA solution. Most solutions and environments will only support phishable authentication mechanisms for bootstrapping a passkey provider unless you also have a **portable root of trust** like a security key.

Security keys are uniquely positioned to meet this demand. Security keys are portable and high assurance, supporting both Smart Card and WebAuthn in a highly portable format, making them extremely useful for bootstrapping other types of authenticators to support and secure other tools. This is how organizations can establish a phishing-resistant user.



> The biggest benefit that Hyatt is going to receive from deploying YubiKeys is to be able to get rid of passwords in our environment. You can't compromise what you don't have."
>
> **Art Chernobrov** | Director of Identity, Access, and Endpoints | Hyatt Hotels Corporation

YubiKey is the bridge to passwordless

Passwordless is a journey, not an overnight transition. And Yubico is on this journey with you.

Yubico created the **YubiKey**, a hardware security key that houses device-bound passkeys and delivers **phishing-resistant MFA and passwordless authentication at scale with an optimized user experience**.

The YubiKey is a multi-protocol security key, supporting a range of authentication protocols, passwordless authentication via both including Smart Card/PIV and passkey (FIDO2/WebAuthn), along with OTP and OpenPGP, integrating seamlessly into both legacy on-premises and modern cloud environments to help organizations bridge to a passwordless future.

YubiKeys work with over 1,000 products, services and applications including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services. The YubiKey is proven to **reduce risk by 99.9%** and deliver significant business value to large enterprises at scale, delivering an ROI of 203%[13], all while delivering a frictionless user experience, letting users quickly and securely log in with a single tap or touch.

Single factor (passwordless): authenticator + touch/tap

Replaces weak passwords with a hardware authenticator for strong single factor authentication.

Multi-factor (passwordless): authenticator + touch/tap + PIN

Multi-factor with combination of a hardware authenticator with user touch and a PIN, to solve high assurance requirements such as financial transactions or submitting a prescription.

Unlike synced passkeys that reside in devices not purpose-built for security, and delivering the ease of copying and sharing which introduces risk for the enterprise, device-bound passkeys residing in YubiKeys are not shareable or copyable, enabling the enterprise to better track and trust the FIDO credential, which is critical at scale, for compliance and for audits. Passkey credentials that live on the YubiKey ensure that users can seamlessly and securely work across a range of platforms and devices, across ecosystems (e.g. Apple, Google, Microsoft), and as a valuable root of trust to support other authenticators (e.g. Windows Hello for Business, Okta FastPass).

Device-bound passkeys enable enterprises to implement passwordless and meet the most strict security and compliance assurance needs with NIST AAL3 support, a common requirement across regulated industries. Any other passkey available today supports only up to AAL2.

Getting started on your passwordless journey with Yubico FIDO Pre-reg

To help organizations accelerate passwordless deployments securely at scale with the YubiKey, Yubico offers an innovative service called FIDO Pre-reg, that enables turnkey FIDO activation for YubiKeys. FIDO Pre-reg raises the bar for security by eliminating reliance on less secure processes for initial access or recovery scenarios, helping eliminate the risk of account takeovers. It requires minimal IT admin set up and standardizes and streamlines the YubiKey onboarding and account recovery processes, reducing the IT admin burden while improving the end user experience.

Takeaway

Organizations need to move away from passwords and legacy authentication to protect against the growing number of cyber threats and be future-proofed for compliance.

Yubico solutions are designed to meet you where you are on your journey to passwordless, offering a secure standalone passwordless solution to support passkey, Smart Card or hybrid deployments and a portable root of trust to bootstrap other authenticators to cover the critical lifecycle authentication gaps that can undermine Zero Trust.

The YubiKey offers a high-assurance path to passwordless at scale across a wide variety of complex authentication scenarios. We offer a simple 6 Step Best Practice Deployment Guide to get started with passwordless using device-bound passkeys.

> “When you’re looking at passwordless and Zero Trust, everything I do becomes the same security. I’ll just keep circling around, expanding passwordless and thinking outside the box to keep my fortress secure.”
>
> **Jason Rucker, Director of IT,**
> **City of Southgate, MI**

Plan
Ensure readiness by clarifying use cases and user populations

Validate
Confirm the process with a small group of users before broader rollout

Integrate
Ensure key apps and services are YubiKey-ready

Launch
Distribute keys to users with turnkey delivery services or channel partners

Adopt
Drive adoption with best practice training and support

Measure
Report on security and business value impact

To remove all the guesswork out of planning, purchasing and delivery, Yubico offers YubiKey as a Service, a service-based and affordable model to simplify how organizations procure, upgrade and support YubiKeys, as well as streamlined global distribution to remote and in-office locations through YubiEnterprise Delivery and trusted channel partners.

If you want a closer partnership on any of the six steps of this plan, Yubico’s Professional Services team is here to help.

Contact us
yubi.co/contact

Learn more
yubi.co/passwordless

Sources

1. Verizon, 2023 Data Breach Investigations Report, (June 6, 2023)
2. Google Cloud, August 2023 Threat Horizons Report, (August 2023)
3. S&P Global Market Intelligence, With Security Breaches Mounting, Now Is the Time To Move From Legacy MFA to Modern, Phishing-Resistant MFA, 2023
4. David Jones, Microsoft, Apple and Google double down on FIDO passwordless standard, (May 5, 2022)
5. S&P Global Market Intelligence, With Security Breaches Mounting, Now Is the Time To Move From Legacy MFA to Modern, Phishing-Resistant MFA, 2023
6. Forrester Research, Inc, Optimize User Experience With Passwordless Authentication, (March 2, 2020)
7. IBM, 2023 Cost of Data Breach Report, (July 24, 2023), https://www.ibm.com/reports/data-breach
8. Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019)
9. S&P Global Market Intelligence, With Security Breaches Mounting, Now Is the Time To Move From Legacy MFA to Modern, Phishing-Resistant MFA, 2023
10. CISA, Zero Trust Maturity Model v 2.0, (April 2023)
11. David Jones, Microsoft, Apple and Google double down on FIDO passwordless standard, (May 5, 2022)
12. NIST, NIST SP 800-63-4 Digital Identity Guidelines, (December 2022)
13. Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)

yubico

About Yubico

Yubico (Nasdaq Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries.

For more information, please visit: www.yubico.com.