yubico

Creating phishing-resistant users across financial services in a passkey age

Key considerations for vetting passkeys across financial services use cases

User-centric authentication—the new frontier of enterprise authentication

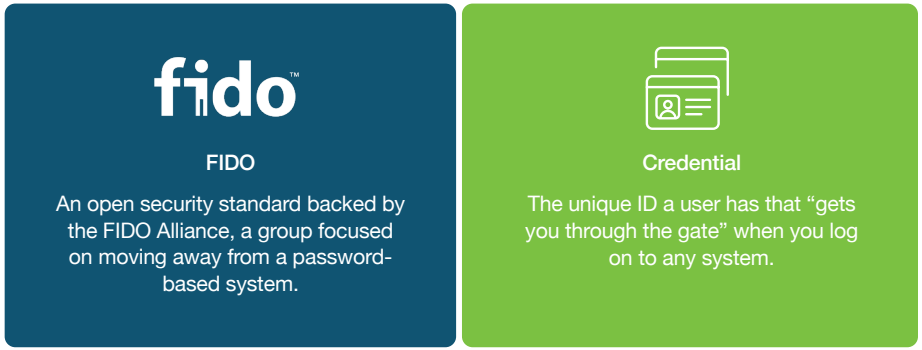
Passwords are ingrained in every aspect of the traditional Identity and Access Management (IAM) identity lifecycle stages. Unfortunately, stolen passwords are one of the largest threat vectors that cyber criminals use to make inroads into a company. However, of late, many financial services organizations are recognizing the importance of hardening cybersecurity defenses against phishing attacks by replacing highly vulnerable legacy multi-factor authentication with phishing-resistant multi-factor authentication (MFA) and then ideally to passwordless authentication, eliminating passwords altogether.

With recent advancements in passwordless and new on-device authentication solutions, the way an organization can establish and manage a user's identity credential throughout its lifecycle has evolved.

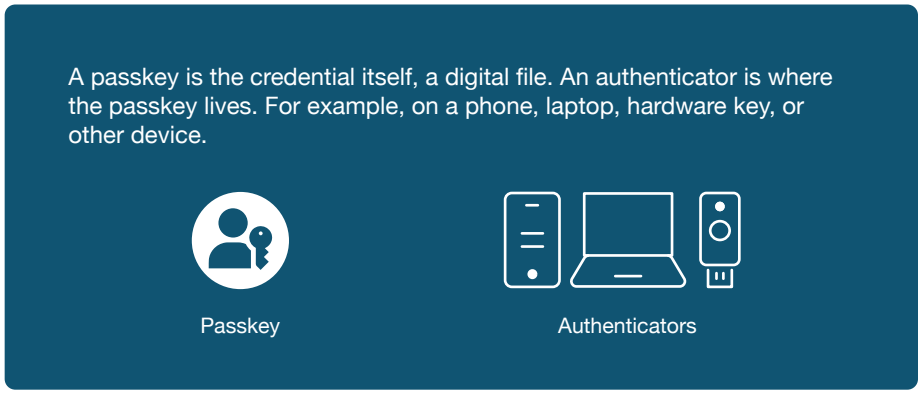
Traditionally, organizations think of phishing-resistant authentication and not phishing-resistant users. The difference lies in thinking about authentication events as points in time as they are logging into sensitive systems, apps, and services versus thinking about how users live and work. Users often move across platforms (Apple, Google, Microsoft) and devices (smartphones, laptops, tablets), and between personal and corporate apps and services in the course of their day. Financial services organizations need to think of equipping their users with the type of authentication that offers phishing-resistance no matter which business scenario they are engaged in—remote worker, mobile-restricted, shared workstations, supply chain 3rd party, end customers etc, and no matter what platforms or devices they are using.

The introduction of passkeys

Passkeys have been introduced by the FIDO Alliance as a way to accelerate passwordless for consumers and organizations alike. Passkeys are now available on every major platform including Google, Apple, Microsoft and web browsers. The development of passkey solutions has created new enterprise identity security events for every enterprise.

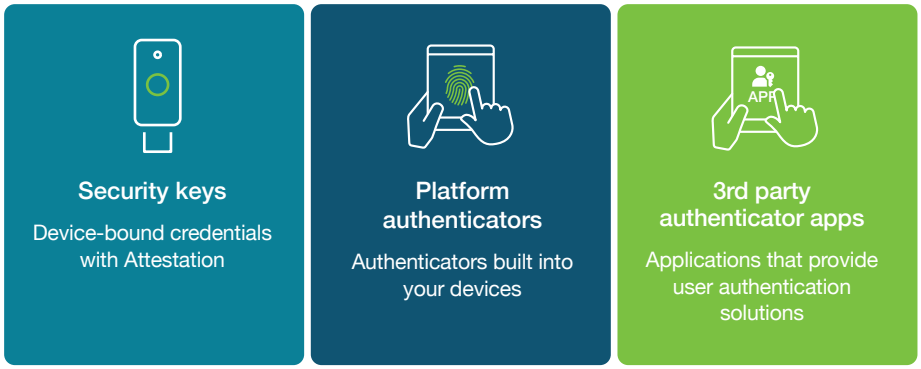


Organizations and their users often confuse the passkey with the authenticator it resides in. **A passkey is simply a FIDO2 credential**, and it can live on a smartphone, or another general-purpose device, such as tablets or laptops. Alternatively, they can reside in portable devices which are authenticators purpose-built for security, such as FIDO hardware security keys.



Securing the enterprise user and the end customer

Users have different authentication needs



Not all enterprise users do the same job everyday. Depending on the needs of the business a user may need to work on a laptop remotely, access their email on their phone during a meeting or access or use a shared workstation or shared devices such as in a call center or a retail banking location. Enterprise users will have different types of authentication needs and therefore the types of authenticators they should use. An enterprise user may be a remote or hybrid worker, or operate in a mobile-restricted environment such as a call center, where mobile phones simply are not an option. They may also be working on shared workstations where different users need to securely log in and log out, all on the same computer terminal.

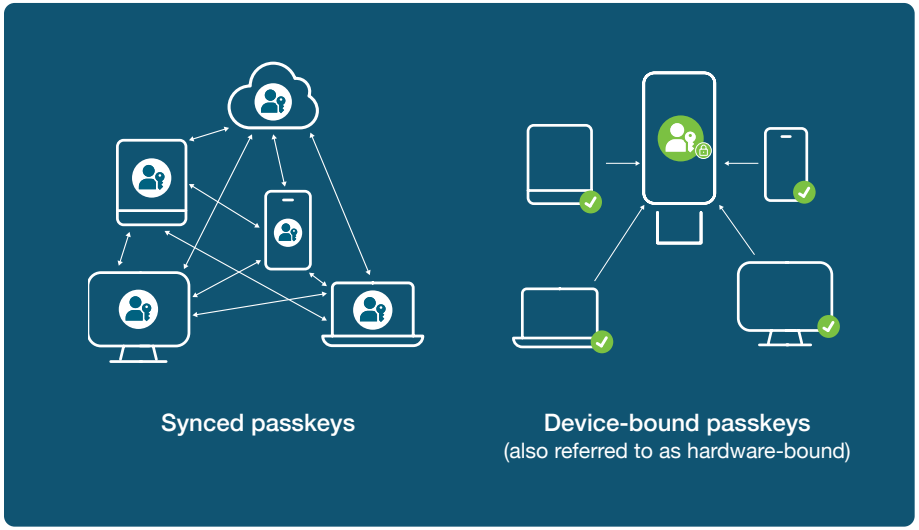
Therefore, the type of authenticator the user will need to store their passkeys on, may differ based on the sensitivity of their roles, or the type of data or system they need to access. Hardware security keys are portable authenticators purpose-built for security, and allow users to work securely and seamlessly across the widest range of enterprise business scenarios. Alternatively, platform authenticators are built into general-purpose devices such as smartphones and laptops. And finally, mobile applications, such as authenticator apps, offer user authentication solutions as well. All of these authenticators have security and usability tradeoffs. It is up to the enterprise to decide what level of security assurance they need and the level of risk they can live with.

Enterprise users aren't the only kind of user that financial services organizations need to be concerned about. The primary goal of any financial services organization is to serve the end customer, and end customers are vastly different from a typical enterprise user. But with many regulatory bodies such as the FFIEC starting to mandate more secure forms of authentication for the end customer, it is critical to consider stronger forms of security for digital services that are built to serve the end customer, such as for online and mobile banking applications. Here, the needs will be different, especially having to cater to a much larger ecosystem of devices used by the vast end-customer base to access digital services. Not moving toward stronger forms of authentication than just a username and password for end customers can put the organization at liability of payouts in the case of an account breach.

Different passkey classes

Not all passkeys are created equal

Passkeys are more secure than passwords and enable a speedy move to passwordless authentication that enables greater security and efficiency. While there are different passkey implementations, each with its security and usability tradeoffs, not all passkeys are created equal, and not all are ideally suited for the enterprise.



Synced passkeys

Designed for consumers, not enterprises

Synced passkeys are copyable credentials that are copied across all the devices connected to the user's account, including their smartphones, laptops and tablets. This may create some chilling failure points for the enterprise. Synced passkeys introduce major risks and exposure gaps in key enterprise scenarios such as remote work, supply chain security, compliance, and support complexity.

Read more about the pitfalls of synced passkeys for the enterprise.

Device-bound passkeys

Designed for the enterprise user

Device-bound passkeys offer greater manageability than synced passkeys, and, therefore better suited for the enterprise.

However, there are different types of device-bound passkeys. Those that live in hardware security keys are known to offer the highest security assurance and provide enterprises with the attestation that lets them prove the security of their credentials. Hardware security keys enable enterprises to build trusted credential lifecycle management processes. Security keys enable enterprise users to register new devices, authenticate to their enterprise passkey providers, and register other device-bound credentials (like Windows Hello or Okta Fastpass) because each user has a portable, phishing-resistant credential for simply and securely authenticating themselves during these processes. This solution removes risk from the help desk and enables enterprises to comply with the most stringent requirements across any industry.

Synced vs device-bound passkeys

Synced passkeys

Lives on a smartphone, tablet, laptop or other device where it can be copied and synced across many devices.

Device-bound passkeys

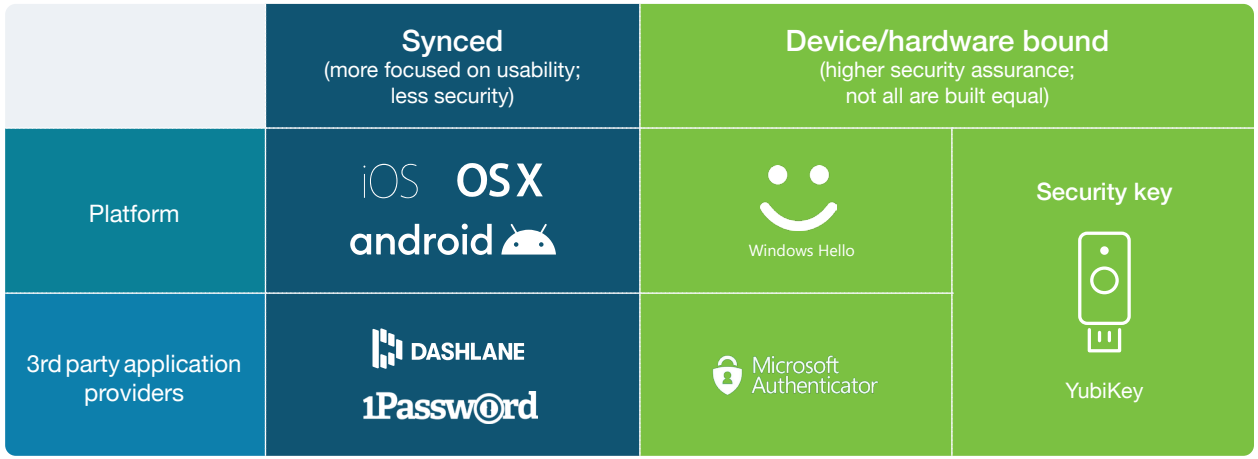
Lives on a USB key or other piece of hardware separate from everyday devices and delivers higher security assurance.

Netting it all out with the passkey toolbox

Different passkey implementations across synced and device-bound passkeys

Users essentially have three types of authenticators that they can use to authenticate using passkeys residing within them. The first passkey solution on the market, and the gold standard for authentication, are hardware security keys. Security keys enable users to authenticate with passkeys that are stored on their key and the user is responsible for moving the security key from device to device. It is important to note that purpose-built authenticators solve specific enterprise use cases that authenticators on mobile simply cannot, such as securing mobile-restricted and shared workstation environments, which is critical to many enterprises.

Other emerging solutions on the market are 3rd Party Passkey providers and these applications can be created to help users manage both device-bound or synced passkeys. The launch of synced passkeys in 2021 was complemented by the platforms' support for these consumer-grade passkeys. The various platforms now support synced passkeys and some of these platforms only allow synced passkeys to be used with their platform authenticators.



iOS and MacOS, now only support the creation of synced passkeys on their platform. Google Android now also only supports synced passkeys as well. Chrome supports both synced and device-bound passkeys, giving the relying party or service (e.g. Dropbox) a choice as to what they can create. To add to the options, Windows Hello only enables the creation of the passkeys bound to that workstation device. And finally, 3rd party providers, like 1Password and Dashlane, support the creation of synced passkeys for users. There are also solutions on the market that will support app-based device-bound passkeys, marking yet another development in the emerging passkey landscape.

Passkey terminology soup? Here is the main thing to remember… It's all about protecting the private key.

Proving where the private key is stored is fundamental to understanding the risk associated with passkeys. The relying party or service can leverage the device attestation included in the credential registration to prove that the passkey is stored on an acceptable device for the enterprise.

All passkeys are based on public key cryptography where there is a key pair with a private key that is securely stored and a public key that is shared or made public. The private key needs to stay private and that is the job of the passkey solution and the underlying system where the passkey resides. **Synced passkeys** allow for the private key to be copied to multiple devices and to a cloud management system. This makes it difficult for an enterprise to track and trust the passkey. **Device-bound passkeys** offer greater management and control which an enterprise needs. But only device-bound passkeys residing in portable hardware authenticators specially built for security offer the private key protection enterprises need.

Cultivating phishing-resistant users

And not just phishing-resistant authentication

As passkeys are introduced to accelerate the adoption of passwordless authentication, the new goal for enterprise authentication should be to establish phishing-resistant users, not just phishing-resistant authentication. Passkeys should be considered within the context of true user-centric authentication and how users work in the organization. This strategy requires that every user must use a phishing-resistant authentication solution for every authentication task. When the objective moves from phishing-resistant authentication to phishing-resistant users, an enterprise can empower users to register new devices without calls to the help desk and maintain high levels of assurance enabling users to securely work remotely while removing operational risk and security risks for the help desk.

With this in mind, the conversation shifts from choosing the right authenticator (phone vs security key, etc.) to ensuring that every authentication option (and passkey) the user has—whether an enterprise users or an end customer—is registered securely and meets both the user experience goals and enterprise security needs.

Moving away from passwords and legacy phishable MFA solutions such as SMS, one-time passwords, and mobile authentication means we are moving into a world where users will have multiple credentials, passkeys, and passkey providers. With this change, the **credential lifecycle** becomes the new inflection point for enterprises that need to manage their critical interactions with the user.

For each user, whether internal-facing employees or end customers, financial services organizations need a solution for the following events:

- **First Authentication**—First authentication on a new computing device (phone, laptop, or desktop) to securely enroll that device in the device management system
- **Credential Registration**—Phishing-resistant registration of synced or device-bound credentials on trusted/managed or untrusted/unmanaged devices
- **First Authentication to Passkey Provider**—First authentication to passkey provider on a new device to begin synchronization of passkeys to a trusted/managed device
- **Web Authentication to Passkey Provider**—Authentication to a passkey provider to access passkeys on an untrusted/unmanaged device
- **Secure Self-Service Credential Management**—Self-service tool for when a user
  - Loses or retires a managed device that revokes any credentials stored on it
  - Needs to recover access to their passkey provider
  - Needs to recover access to their platform account
  - Needs to manage any existing YubiKeys, and to revoke/mark lost any credentials that will no longer be in use
- **Secure Self-Service Authenticator Management**—Self-service process for ordering additional device-bound passkeys (e.g. residing on a YubiKey) if a user needs a new one to prevent risking account lockout
- **Account Lockout**—A secure process for a user to get a new credential issued for their enterprise-managed account after losing access to all their authenticators/credentials

The phishing-resistant user and portable passkeys

YubiKeys

Device-bound Passkey Credentials with Attestation

Phishing-resistance should not be tied to a particular isolated device or platform, but should be **able to move with the user**, no matter which app, service, or system they are logging into, and across their corporate or private lives. This builds a phishing-resistant enterprise end-to-end. Device-bound passkeys, such as those in a YubiKey, combine the secure cryptography of passkeys on a portable piece of hardware. Using YubiKeys creates phishing-resistant users where strong authentication travels with the user and is not tied to a specific platform or mobile device.

Considerations to select the right passkeys

All passkeys may be phishing-resistant, but not all are ideal for financial services use cases

Many password replacement solutions focus on bringing phishing-resistant authentication to the market, and enterprises are looking for easy solutions to replace passwords. As part of this consideration financial services organizations must also remember to address each phase of the account lifecycle and related regulatory requirements to determine what passwordless technologies are adequate. Device-bound passkeys on authenticators built specially for security can fill these requirements. The ideal strategy will not only make key authentication control points phishing-resistant, but also provide a path to create phishing-resistant users, so that they are protected throughout the various authentication ceremonies on any device that they use.

Regulated customer applications

Banking applications, brokerage sites, and insurance portals can all fall into a broad category of high risk customer-facing applications. Local, federal and international regulations may require higher assurance methods of authentication to protect individual and organizational resources. However these additional steps often introduce friction to a process and may deter customers from using these services.

Our recommendation is to enable passkey authentication, including synchronized and device-bound authentication. It will provide an easy, phishing-resistant workflow for end users building off the security controls of the devices they already use, and offer a path to higher levels of assurance for your high value or risk adverse customers by supporting device-bound passkeys. Many Yubico financial services clients send their high value clients device-bound passkeys as a security service differentiator.

Customer-facing regulated interactions

Retail banking and call center supported transactions prove an interesting opportunity. Requirements from regulatory bodies require traceability and auditability of transactions conducted on behalf of end customers, and the solutions to both of these requirements starts with strong identity proofing, including proofing of the customer requesting the transaction as well as proofing of the agent facilitating the transaction. Authentication with passkeys can help solve both of these problems. On the customer side, passkey-based identity proofing can be built into an application or a web-page sent to end customers, or as part of a ceremony that is conducted in an in-person scenario. On the employee side of the picture, passkey authentication unlocks the powers of strong cryptography to tie individual enterprise users to specific transactions and actions. Additionally, device-bound passkeys provide a simple and highly-assurant identification process that does not break end-customer interactions and functions within mobile-restricted environments.

Development teams

When it comes to your development teams, those employees that are writing the code for your enterprise applications, it is critical to take the path of highest-assurance security as these users hold the ‘keys to the kingdom’.

Protecting these users with highest-assurance authentication will ensure that your applications and your business stay protected. Preventing account takeovers and ensuring secure code signing processes are essential. In these cases, it is best practice to deploy device-bound passkeys and require signatures at time of code check in, into enterprise code management platforms such as GitHub or Atlassian, in order to have traceability of your application.

Secure onboarding and recovery is a must for all users

The MFA that customers decide to implement is only as secure as the registration and recovery. Registration or onboarding processes using phishable methods like sending OTP codes lead to vulnerable MFA deployment. If anyone can register or reset the FIDO credential then it defeats the purpose of using phishing-resistant MFA. Organizations need to have a robust onboarding and recovery solution to bootstrap the enrollment of the MFA method.

Key implementation considerations for different passkey types

Platform passkey provider (Synced passkeys)

- Does the user have MFA setup?
- Is it phishing-resistant MFA? How do I know?
- Is the user able to recover
- their platform account?
- How secure is it?
- If the user recovers access to their platform account?
- Will I know? Should I care?

3rd party passkey provider (Synced passkeys)

- Does the user have MFA setup?
- Is it phishing-resistant MFA? How do I know?
- Does the account only allow phishing-resistant authentication?
- Does the account support phishable account recovery?
- If the user registers a new device how would I know this?

Device-bound passkeys

- Is there a reason to prevent a device-bound passkey using a hardware security key from working in my application?
- Does the user have more than one hardware authenticator?
- What happens if/when a user loses access to their account?

YubiKeys make other device-bound passkeys more secure

It doesn't have to be one or the other: A hybrid approach might suit an organization best in key scenarios, like using 3rd party passkey providers for low-risk apps/users or for dedicated for temporary use during recovery scenarios. Also consider that using a pre-enrolled YubiKey provisioned and delivered to the end user creates the strong binding needed to bootstrap the setup of another type of device-bound passkey within a 3rd party passkey provider. This significantly raises the bar for security and usability creating a robust credential lifecycle strategy that an organization can build upon.

Additional enterprise considerations: compliance, audit and risk

Compliance and audit with device-bound passkeys on general purpose devices

Challenges

Limited attestation abilities; hard to determine which devices/hardware are protecting passkeys

Device-bound passkeys on general purpose devices, such as smartphones or laptops or tablets only meet AAL2

Does not meet strictest compliance and certification needs

Compliance and audit with device-bound passkeys on authenticators purpose-built for security

Benefits

Hardware authenticator attestation offers the most confidence that passkeys are stored securely on known trusted hardware with known properties

Device-bound passkeys on YubiKeys are the only ones that meet AAL3

Meets strictest compliance and certification needs

The YubiKey

Raise the bar for security for all other passkey providers

It is important to note that for enterprises to remove passwords from their users' daily lives there is one more important way to ensure that users have a simple, secure, and portable authentication solution. The YubiKey enables users to authenticate to their workstations, unlock their passkey providers (both platform and 3rd party) and bootstrap their passkey applications.

Device-bound passkeys residing in YubiKeys provide the **highest level of assurance** on how the private key is managed based on the built in FIDO attestation standard. The YubiKey ensures that the private key is stored and protected within a purposely built security hardware module. Other forms of device-bound passkeys need to rely on less reliable approaches to provide information about the security and control of the private key. The lack of visible controls might not meet enterprise needs to meet compliance regulations or necessary security standards.

Summary

Key passkey takeaways for your enterprise

Passkeys offer a FIDO-enabled world, but for highly regulated financial services organizations that require strict control of user identity, device-bound passkeys living in general purpose devices such as smartphones, laptops and tablets may not lower risk for your organization. Device-bound passkeys that live on security keys offer the highest security assurance and provide enterprises with the trusted credential lifecycle management and attestation abilities they need to have the strongest security, the simplest user onboarding and credential/account recovery experience across devices and platforms, and stay in compliance with the most stringent regulatory requirements.

1. Look for phishing-resistant authentication methods that can support all areas of authentication and credential management to create phishing-resistant users. Onboarding and recovery flows are common areas where phishing-resistance breaks down and is an attractive attack vector

2. There may be some or no attestation for a large variety of different devices. The Service/Relying Party or enterprise cannot know what type of device was used or know the trust that they can put into the authenticator and how the passkey is stored. It is critical that enterprises be able to trust the passkeys their users use.

3. Passkey credentials, such as the ones that reside in modern FIDO security keys, provide a higher degree of assurance than passkeys on a smartphone, While these lower security passkeys offer AAL2 assurance, passkeys in security keys offer AAL3 assurance—highest authenticator assurance Level 3—which is critical for ensuring compliance.

Contact us
yubi.co/contact

Learn more
yubi.co/finance

yubico

About Yubico Yubico (Nasdaq First North Growth Market Stockholm: YUBICO), the inventor of the YubiKey, offers the gold standard for phishing-resistant multi-factor authentication (MFA), stopping account takeovers in their tracks and making secure login easy and available for everyone. Since the company was founded in 2007, it has been a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO2, 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.

Yubico's solutions enable passwordless logins using the most secure form of passkey technology. YubiKeys work out-of-the-box across hundreds of consumer and enterprise applications and services, delivering strong security with a fast and easy experience.

As part of its mission to make the internet more secure for everyone, Yubico donates YubiKeys to organizations helping at-risk individuals through the philanthropic initiative, Secure it Forward. The company is headquartered in Stockholm and Santa Clara, CA. For more information on Yubico, visit us at www.yubico.com.