yubico

WHITE PAPER

What is FIDO and why is it important for business security?

The modern authentication standard for phishing-resistant multi-factor and passwordless authentication

Contents

The critical need for modern, strong authentication

Yubico is proud to be a creator and core contributor to the FIDO Alliance and its authentication specifications, and a leading contributor to the World Wide Web Consortium (W3C)'s WebAuthn.

Across the globe for every industry, cybersecurity is a top priority. As organizations mature their digital capabilities, they also experience new levels of risk and escalating data breach costs, now averaged at $4.45M USD globally.[1] Further, cyber attacks can have severe and long-lasting consequences including damage to physical assets, impact to customer trust and brand reputation, increased cyber insurance premiums, and potential loss of intellectual property. In the case of the public sector and critical infrastructure organizations, cyber attacks can also impact a nation's security, economic security, public health and/or safety.[2]

When tracing breaches, attacks against identity are pervasive; 74% of data breaches can be traced back to the human element including the use of social engineering phishing attacks and privilege misuse.[3] Further, a recent Google Cloud report indicates that credential issues, including weak passwords or leaked credentials, account for over 60% of compromise factors in enterprise cloud environments for Q1 2023.[4]

Authentication specifications

Smart Card/PIV

functionality based on the Personal Identity Verification (PIV) interface specified in NIST SP 800-73, supporting sign/decrypt operations using a private key stored on the smart card.

Learn about Smart Card/PIV >

FIDO U2F

is an open authentication standard, based on public key cryptography, enabling a single security key to access hundreds of online services without drivers or client software.

Learn about FIDO U2F >

FIDO2

is an evolution of FIDO U2F and offers the same high level of security, with expanded authentication options such as Passwordless, 2FA and MFA.

Learn about FIDO2 >

WebAuthn

a global authentication standard for web browsers, delivers users greater choice of authenticators to secure accounts, including security keys and built-in platform authenticators available in modern devices.

Learn about WebAuthn >

Risk of account takeovers

0%
Security key (YubiKey)

10%
On-device prompt

21%
Secondary email

24%
SMS code

50%
Phone number

Organizations face mounting pressure from regulators and cyber insurers to strengthen cybersecurity defenses with multi-factor authentication (MFA). However, while any form of MFA offers better security than a username and password, the truth is that **not all MFA is created equal** in terms of security, usability and scalability. Legacy mobile-based authentication methods such as SMS, one-time passcodes (OTP) and push notification apps are highly susceptible to account takeovers from phishing, social engineering and attacker-in-the-middle attacks. A Google, New York University (NYU), and University of California at San Diego (UCSD) analysis of 350,000 real-world hijacking attempts revealed that a SMS-based OTP only blocked 76% of targeted attacks and a mobile push app only blocked 90% of targeted attacks.[5] In other words, even the best case scenario using these forms of MFA still afforded a 10% attack penetration rate.

In late 2023, biotechnology organization 23andMe was the victim of a credential stuffing attack that leveraged previously exposed credentials from other organizations, and highlights the persistence of password reuse and weak account security due to a lack of MFA, to expose the data of 7 million individuals.[6] In the year prior, a phishing attack at Twilio successfully exfiltrated credentials, giving the attackers a clear path to systems and data, impacting a further 163 customer organizations.[7] Further, an increasing number of breaches, including the 2022 attacks on Uber[8] and Cisco Systems,[9] can be tied to MFA fatigue—where users mindlessly approve two-factor approval requests due to an over-abundance of notifications.

Beyond security, legacy authentication carries many **hidden governance and support costs** around setting and managing password policies at scale, as well as productivity costs associated with forgotten passwords and account lockouts, and time-consuming workflows to generate and enter OTP/push app codes. As these issues persist and ultimately erode the bottom line of many enterprises, user experience (43%) and IT complexity (41%) are often cited as the top obstacles preventing them from achieving MFA adoption.[10] Moreover, there are always gaps where users can't, don't or won't use mobile authentication—where users lack devices, where availability or mobile-restrictions may apply, as well as spark environments and clean rooms, among other scenarios.

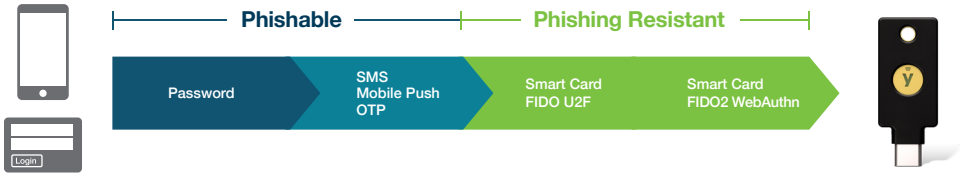
In response to the aforementioned problems with passwords and legacy authentication, **Fast Identity Online or FIDO authentication** was created—a modern solution that offers secure, phishing-resistant multi-factor and passwordless MFA, a simpler user experience and simplified administration.

What is phishing-resistant MFA?

Phishing-resistant MFA refers to an authentication process that is highly resistant to attackers intercepting or even tricking users into revealing access information. It requires each party to provide evidence of their identity, but also to communicate their intention to initiate through deliberate action.

Globally recognized for promoting equitable standards, the National Institute of Standards and Technology (NIST) defines phishing-resistance in Special Publication (SP) 800-63 and Draft 800-63-4[11] 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."

Currently, two forms of authentication meet the mark for phishing-resistant MFA: **Smart Card//PIV** and the modern **FIDO2/WebAuthn** authentication standard.



Many global regulators now specifically mandate **phishing-resistant MFA**, including the Office of Management and Budget (OMB) Memo 22-09[12] and the National Security Memorandum/NSM-8[13] in the U.S., in line with the U.S. White House Executive Order 14028;[14] NIS2 in the EU;[15] the Essential Eight Maturity Model (E8MM) guideline in Australia;[16] as well as the global PCI DSS v4.0 standard for those organizations that handle payment card data,[17] with additional regulators likely to follow suit.

While strong phishing-resistant authentication has existed for many years in the form of public key infrastructure and Smart Cards, these solutions are costly and difficult to implement at scale for digital services. This white paper will introduce you to **FIDO** and the evolution of the **modern FIDO2/WebAuthn standard** that enables phishing-resistant authentication for the modern, online work environment.

> “I urge every CEO to ensure that FIDO authentication is on their organization’s MFA implementation roadmap. FIDO is the gold standard. Go for the gold.”
>
> **Jen Easterly, Director, CISA**[18]

What is Fast Identity Online (FIDO)?

FIDO (Fast Identity Online) refers to a set of global authentication standards based on public key cryptography. Developed by the FIDO Alliance, FIDO authentication standards provide phishing-resistant security and a streamlined user experience that can be implemented across a wide variety of use cases and deployment scenarios. Gartner research predicts that by 2025, 50% of the workforce will be passwordless and 25% of MFA transactions using a token will be based upon FIDO authentication.[19] FIDO authentication provides a simpler user experience with phishing-resistant security.

What makes FIDO phishing resistant?

FIDO uses strong public key cryptography for phishing-resistant authentication. During registration, the user login is bound to the origin or domain—also called origin binding. When a user registers a FIDO credential with a specific site, it is unique for only that service—if a user were to try to use that credential on a fake website (phishing), it would fail. So even if a user is fooled into thinking the fake site is a real site via a phishing email, the **FIDO credential is never fooled**. This greatly mitigates against dependence on user training to identify phishing emails, due to the increasing volume and sophistication of phishing attacks, especially AI-driven phishing attacks.

FIDO authentication options

FIDO authentication specifications will leverage one or more of the following:

Passwordless authentication

Strong single-factor authentication using FIDO, eliminating the need for weak password-based authentication.

Two-factor authentication (2FA)

Strong two-factor authentication using FIDO authenticator as an extra layer of protection beyond a password.

Multi-factor authentication (MFA)

Strong multi-factor authentication using a FIDO authenticator and a PIN or biometric, to meet high assurance requirements such as those in regulated industries.

FIDO authentication specifications

The FIDO Alliance has created two primary authentication specifications: FIDO Universal Second Factor (**FIDO U2F**) and its successor, **FIDO2**.[20] In order to understand these specifications, we need to break down the building blocks of FIDO technology first.

FIDO building blocks: CTAP, WebAuthn

FIDO Client to Authenticator Protocol (CTAP)

W3C Web Authentication

CTAP1

Two-factor authentication leveraging FIDO U2F devices.

Previously FIDO U2F.

CTAP2

Two-factor, multi-factor and passwordless authentication leveraging hardware authenticators

WebAuthn

API built into browsers and platforms to support relying parties enable FIDO authentication

Both FIDO CTAP standards support communication between an authenticator (e.g. mobile device, hardware key) and client (browser or platform), with support for either two-factor (**CTAP1**) or two-factor, multi-factor and passwordless (**CTAP2**).

The World Wide Web Consortium (W3C), the primary standards body for the web, created **WebAuthn**,[21] a core component of FIDO2 and an authentication protocol that standardizes strong authentication across all major browsers and operating systems, raising the bar for authentication to websites, services and applications.

WebAuthn is an Application Programming Interface (API) that enables communication between the client and relying party, allowing for the creation of a public key-based credential for authenticating users. This type of cryptography is asymmetric, since only the user retains control and possession of a mathematically related private key used for encrypting and decrypting data,[22] and is noted as being robust and extremely resilient to server side breaches despite communication over an insecure medium such as the internet.

WebAuthn makes it easy to replace legacy authentication by offering a choice of strong authentication experiences—everything from scanning a fingerprint, to entering a PIN, to tapping the contact on a hardware security key.

FIDO Universal Second Factor (FIDO U2F) / CTAP1

FIDO U2F was designed to act as a second factor to strengthen existing username/password-based login flows. FIDO U2F is built on a scalable public-key infrastructure in which a new key pair is generated for each service, all while maintaining full separation between them to ensure privacy even if any one service is compromised.

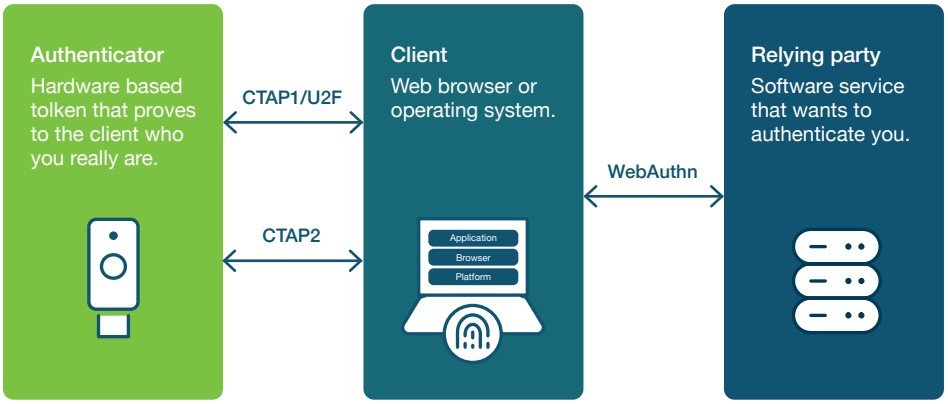
The original FIDO U2F specification included both the web API component, and the protocol for communication between the authenticator and client. With the release of FIDO2 however, the original U2F web API now refers only to communication protocol between the client and authenticator- Client to Authenticator Protocol version 1 or CTAP1—and has been superseded by WebAuthn and CTAP2.

FIDO2/WebAuthn

FIDO2 is the evolution of FIDO U2F, offering complete backwards compatibility for existing U2F deployments and the same high level of security based on public key cryptography, but with an extended set of functionalities to cover additional use-cases, including **phishing-resistant** two-factor, multi-factor and passwordless login flows.

FIDO2 relies on both CTAP1 and the enhanced CTAP2 combined with the WebAuthn specification, collectively referred to as the combined FIDO2/WebAuthn specification, as illustrated below:

FIDO2 Building Blocks



FIDO2 replaces weak passwords with strong phishing-resistant authentication using public key cryptography to protect against phishing, session hijacking, attacker-in-the-middle, and malware attacks, with no secrets shared between services. FIDO2 is an open standard, offering flexibility and choice to support a variety of different device form factors as well as communication methods including USB and NFC.

An introduction to 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.

How to choose the right FIDO2 authenticator

While WebAuthn allows for broad choice in authenticators, not all FIDO2 authenticators are created equal in terms of ease of use, portability, flexibility across use cases or strength of assurance.

Common FIDO2 authenticators

A platform (internal) authenticator

- Apple Touch ID or Face ID
- Microsoft Windows Hello
- Fingerprint scanners built into devices

A roaming (external) authenticator

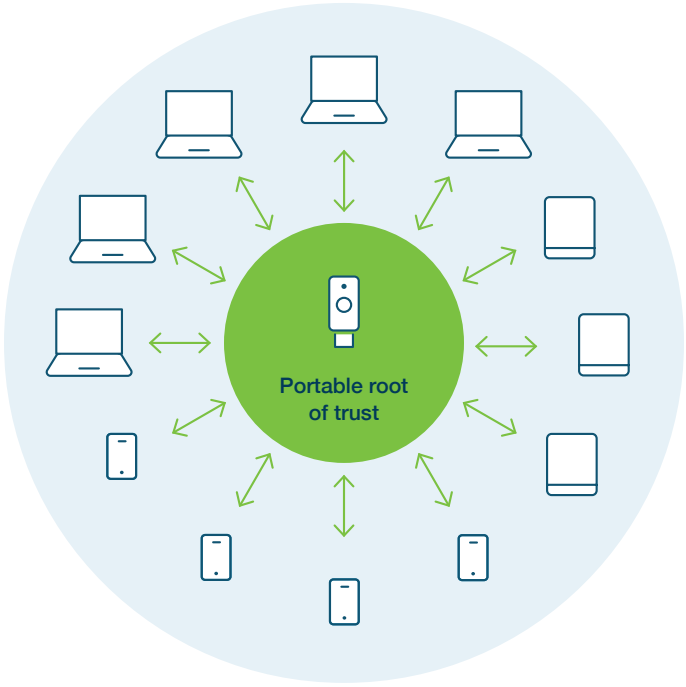
- A hardware security key

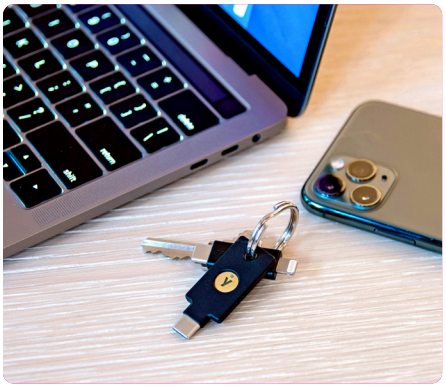
Platform or internal authenticators rely on a built-in Trusted Platform Module (TPM) used to secure any generated private keys and are often biometric in nature. When present, the biometric element provides a mechanism for the platform to match against the device's identity profile of a user, and in turn, use the stored cryptographic credentials to authenticate against the relying party. Platform authenticators are not portable across devices and can create unproductive workflows if a user is locked out of their account. These are typically not suitable for shared workstations and devices.

Roaming or external authenticators, also known as portable authenticators, are not tied to any single platform or device and can be used to authenticate to any number of devices. These authenticators can be plugged in directly using USB or even use NFC (Near Field Communication) or Bluetooth. External authenticators also possess an integrated secure crypto-processor, similar to the TPM used in a platform authenticator, but one that is specifically designed to be mobile (i.e. smaller in size) and accommodate authentication without a fixed anchor point.

Platform vs roaming authenticators

For platform authenticators, since the cryptographic material is embedded within the devices themselves, this form of authentication introduces **portability challenges** that make it difficult to switch between devices, access shared workstations and devices or work in mobile-restricted environments. On the other hand, roaming **authenticators—such as a hardware security key—act as a portable root of trust** to support uninterrupted access to applications and services across any platform or computing device.





Platform authenticators also require ongoing **patch management** to account for **vulnerabilities that are discovered with TPMs** or secure enclaves, including Windows Hello for Business. For example, in March of 2023, two vulnerabilities were discovered that allow cyber threat actors to overwrite or access cryptographic keys.[23] Unfortunately, any upgrade to the firmware on the TPM will have downstream implications on the services and applications that rely on these TPM-backed secrets, requiring re-registration.

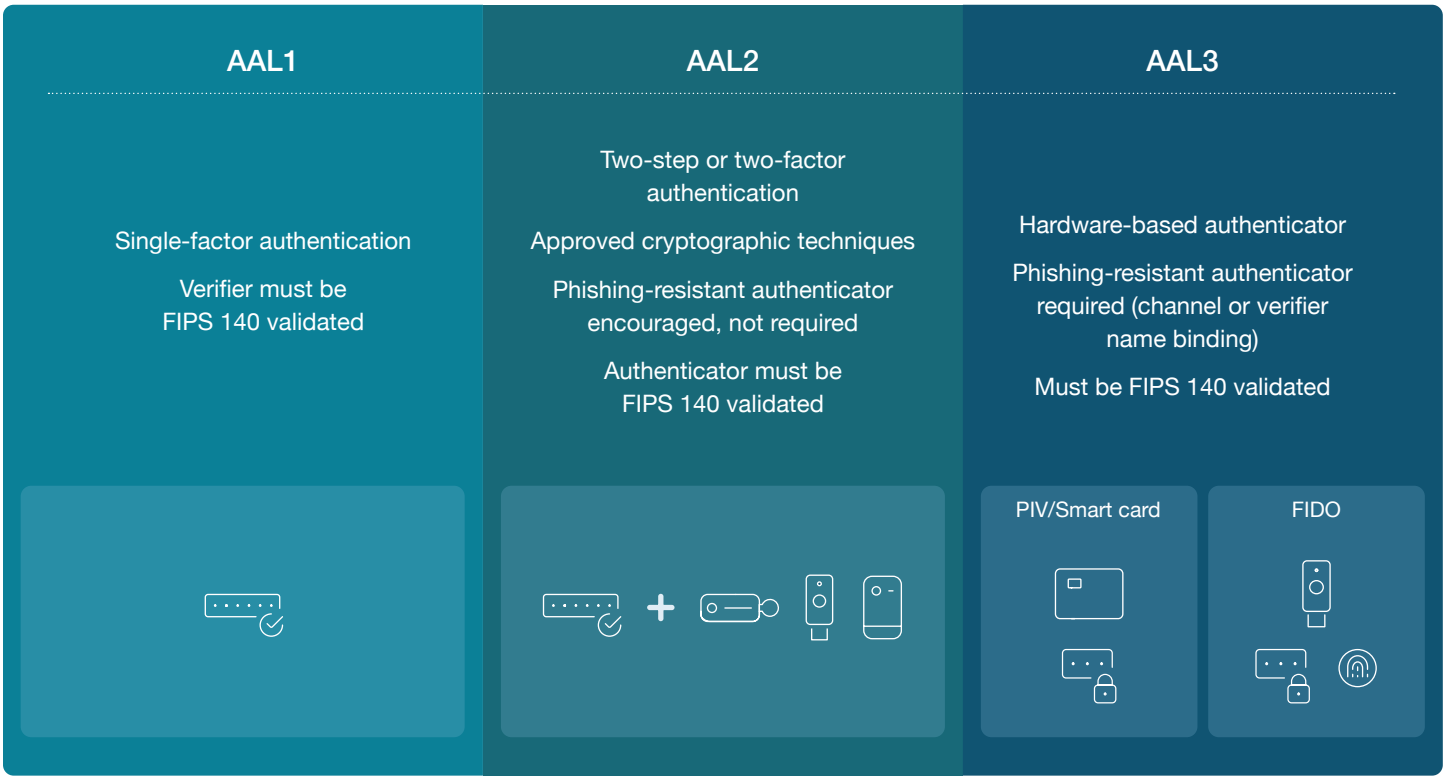
With the introduction of passkeys, many of the platform authenticators on popular devices will have a preference to create **multi-device credentials** (MDC) that can be moved and synced between devices. **MDCs cannot be utilized for high-assurance scenarios** and cannot provide **attestation**, which is the ability of a device to prove its own identity and for a relying party to attain details about the security device it was created on, and which manufacturer created the device. In contrast, roaming authenticators such as **hardware security keys, have the ability to provide attestation** during the credential registration process to help validate devices, customize user experience, offer authentication metrics, and provide an audit trail to support high assurance MFA.

WebAuthn does not constrain organizations or individuals to the use of a single type of authenticator. Instead, users should explore the ways in which platform and roaming authenticator technologies can complement each other in **hybrid flows** that allow platform authenticators to be used in combination with a possession-based roaming authenticator for high assurance whilst reducing friction.

What is high-assurance authentication?

This white paper posits that **not all MFA is created equal**. Reinforcing this, NIST SP 800-63[24] articulates the relative **strength of authenticators** through the creation of authentication assurance levels (AALs).

While any form of MFA will provide greater security than a password (AAL1), 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.



Best practices for security key registration

- Registering a **FIDO enabled hardware security key as the root of trust**, since it is external and can be used to quickly and easily bootstrap other devices, offering the highest level of security. Account recovery issues are exacerbated in instances where a platform authenticator is the primary option and the host device is subsequently lost or stolen.
- Where **high assurance and attestation** are required, it is recommended that security administrators configure the registration process such that the first credential registered on any account must be a FIDO enabled security key.
- For security keys that will be left inside computing devices, **set up second factors** such as PINs or facial / fingerprint scans, depending on the type and properties of the authenticator.
- It is generally recommended for users to register **two keys**, where one is stored securely for backup and only used if the primary is lost or unavailable. If the primary cannot ultimately be recovered, it should be deregistered from the account and a new backup created and again stored securely.
- The strength and validity of less secure fallback methods must be **continuously and vigorously investigated** if they are being permitted as account recovery options, since attackers may target these avenues for account takeover if the primary option can be circumvented.

FIDO2/WebAuthn use cases

Secure web authentication is both rapid and easy with FIDO2/WebAuthn, streamlining registration and login to websites, services or applications via a variety of authentication options. Furthermore, roaming authenticators or hybrid flows can support many other critical business scenarios.

Use cases supported by **all FIDO2 authenticators**	User registration	User authentication	Passwordless authentication
	Step-up authentication	Account recovery	Manage credentials
Use cases supported only by **external authenticators or hybrid flows**	Shared workstations / multi-device access	Mobile-restricted environments	Uninterrupted access Battery | cell signal | presence | damage
	New device onboarding	TPM-less devices / BYOD	Integration with legacy systems
	High-assurance authentication requirements FIPS 140-2 Level 2 and Level 3		

User registration

For new online accounts, WebAuthn makes it possible to replace the standard username and password with a variety of authentication methods. Let's follow the example of setting up a new account with passwordless registration. In this case, no password is created during login. Instead, a user selects only a username and is then prompted to register one or more FIDO2 authenticators.

Once the user has nominated an authentication option (e.g. inserted and tapped a hardware security key), the WebAuthn-compliant browser sends the authentication credential back to the online service provider, which then creates and binds the account to the authentication credential for subsequent authentications.

User authentication

Let's assume that a user has leveraged security best practices and has registered a security key to an online account. Now, when the user wants to log back into the account, only the username and a physical action (e.g. use of the hardware security key) is required.

Passwordless authentication

Passwordless authentication is any form of authentication that doesn't require the user to provide a password at login. FIDO2 passwordless replaces weak passwords with an external authenticator for strong single-factor authentication or multi-factor authentication that involves the use of an external authenticator with user touch and a PIN to provide high assurance requirements.

Organizations can choose to implement smart card passwordless, FIDO2 passwordless using a biometric or a PIN, or a hybrid passwordless approach involving both methods, depending on the existing infrastructure and user scenarios. For the latter, it is important to choose an external authenticator that can support both smart card and FIDO2 protocols in order to minimize complexity, but also streamline the overall user experience.

Step-up authentication for high-value, high risk scenarios

There are certain scenarios where services may choose to require step-up authentication to complete a high-risk action, such as transferring a large sum of money between bank accounts or for access to privileged systems and data. Step-up authentication or secondary authentication provides an opportunity to re-verify users for additional protection against attackers. Without ties to the internet or a multi-purpose chip used for computing, the attack vector naturally becomes much smaller with an external hardware authenticator.

In these scenarios, users will be prompted to re-authenticate with their chosen authenticator before the transaction can proceed. Given the number of potential authentication scenarios presented to users during the day, organizations should consider choosing an authenticator that reduces friction in the authentication experience as well as security.

Account recovery

By enabling users to register multiple authenticators for each website, service or application, WebAuthn makes it easier for users to recover access to accounts if a device is lost or stolen.

While all FIDO credentials can be used to help with self account recovery, they may also require help desk support. Account recovery based upon copyable passkeys generally revolves around a user's cloud account synced across devices (potentially including personal devices), increasing the internal support burden and potentially requiring the support of cloud providers to resolve authentication or credential syncing issues.

External authenticators such as a **hardware security key can serve as a portable root of trust**, enabling users to re-establish trust with online accounts and re-register other authenticators or devices without the need to contact help desk support. An external root of trust, where the user's credential cannot be tampered with, allows a high degree of trust to be transferred from device to device and establish all of them as a trusted entity, thereby limiting the number of devices that may be used in conjunction with a service and protecting the account from untrusted devices or sources.

Shared workstations / multi-device access

There is a wider need to secure and simplify authentication in situations of both **multiple users per device** (e.g. shared workstations or devices in call centers, retail or manufacturing) as well as **multiple devices per user** (e.g. employees who hop between laptop, tablet and personal and work phones).

As noted earlier, platform authenticators embed the cryptographic material in the devices themselves, making it difficult to switch between devices or access shared workstations. A portable external authenticator that can work across computing devices makes these transitions seamless, including options to connect via USB or NFC.

Mobile-restricted environments / availability

Not all work environments allow employees or contractors to have a mobile phone, including call centers, manufacturing floors, as well as secure and remote locations such as oil rigs,boats and server rooms. An external authenticator provides a portable solution for authentication that does not require the user to carry or use a smartphone.

Uninterrupted access

Not all authenticators support field work or situations that require a solution that does not rely on cellular connectivity and battery life. Hardware authenticators offer a more durable solution than those that rely on laptops or smartphones and can be certified water- and crush-resistant in addition to being dust proof.

New device onboarding

To authenticate to a service from a new device, the user needs to present some type of portable credential. Traditionally users would use passwords, SMS messages, or QR codes, but all those methods are cumbersome and insecure. A better solution is to set up a hardware security key as a root of trust and optionally use that security key to "bootstrap" other devices.

Once bootstrapped, any other devices are then considered trusted and services will no longer require the security key in every authentication sequence. In this way, a security key can serve as a **portable root of trust for all devices**—smartphones, tablets, laptops, and desktops–belonging to the user and for all WebAuthn-compliant services with whom the user has accounts.

TPM-less devices / BYOD

While most modern laptops, tablets or smartphones will have a TPM, older devices may lack support. This consideration with platform authentication extends to seasonal staff, contractors, third parties or any affiliates requiring the use of personal devices throughout an organization. Furthermore, the use of any device for authentication creates problems around equity (users who don't have a device or live in low-connectivity areas) as well as restrictions (legal or union regulation) that may prevent employees from using personal devices for authentication. In such cases, organizations face steep costs to deploy and manage such a vast array of devices.

Integration with legacy systems

Most enterprises use a variety of systems, platforms, and devices, not all of which will support newer authentication specifications such as FIDO and WebAuthn, but may support older authentication standards such as OTP or Smart Card, whose credentials can be stored in the secure chip on a security key. Security keys are available that support both new WebAuthn credentials as well as older types of credentials in a single, convenient, and portable format.

High-assurance authentication requirements

For US government agencies and the organizations that work with them, the new NIST 800-63-4 guidelines[25] require the exclusive adoption of a phishing-resistant MFA by the end of FY2024.[26] While Smart Cards (PIV/CAC) do support phishing-resistant MFA, in cases where PIV/CAC cannot be used, those authentication mechanisms must move to or be complemented by a phishing-resistant method like FIDO2.

For federal agencies bound by the Federal Information Processing Standards (FIPS) 140 standard,[27] the minimum standard will be the AAL2 level, though many are choosing to leapfrog from legacy authentication directly to AAL3 solutions such as a **FIPS 140-2 validated hardware security key**, which offers both the highest assurance defense against phishing attacks with the greatest productivity gains.

Getting started on your passwordless journey with Yubico featuring '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.

YubiKey offers highest-assurance security as an external FIDO authenticator

Modern, phishing-resistant MFA and passwordless authentication

Modern, phishing-resistant MFA, offered only by FIDO2 or Smart Card/PIV protocols, have been proven to stop account takeovers in their tracks. Hardware security keys, such as the **YubiKey**, support multiple authentication protocols, including **FIDO2, FIDO U2F and Smart Card/PIV**, making them truly phishing-resistant and delivering peace of mind.

The YubiKey is an ideal option for FIDO authentication because it doesn't require external power, batteries or a network connection—a user can use a single key for secure access to multiple applications and services with the secrets never shared between services. The YubiKey is proven to deliver significant business value to large enterprises at scale, delivering an ROI of 203%,[28] while delivering a frictionless user experience, letting users quickly and securely log in with a single tap or touch.

As a portable hardware root of trust, the YubiKey is proven to **reduce risk against phishing attacks and account takeovers by 99.9%**:[29]

More Value
Reduce support tickets by 75%

High Return
Experience ROI of 203%

Strongest Security
Reduce risk by 99.9%

Faster
Decrease time to authenticate by >4x

The YubiKey enables organizations to take full advantage of the benefits of FIDO2/WebAuthn, making authentication both easier to use and more secure to log into websites, services and apps from any device.

The YubiKey is:

- FIPS 140-2 validated to AAL 3 requirements
  Overall Level 1 (Certificate #3907) and Level 2 (Certificate #3914), Physical Security Level 3
- CMMC Level III compliant
- DFARS / NIST SP 800-171 compliant
- Manufactured securely in the US

YubiKey form factors
From left to right: YubiKey Bio - FIDO Edition, YubiKey C Bio - FIDO Edition, YubiKey 5C NFC, YubiKey 5 NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano.

How does the magic of the YubiKey work?

Hardware with strong crypto

- Any software downloaded on a computer or phone is vulnerable for malware and hackers.
- Besides smart cards most authentication schemes rely on centralized servers with stored credentials that can be breached.
- With the YubiKey, security is significantly enhanced by storing encryption secrets on a separate secure chip, with no connection to the internet, and using strong public key cryptography where only the public key is stored on the server.

Origin bound keys

- Once a user registers a YubiKey to a service it is bound to that specific URL and the registered credential cannot be used to login to a fake website, making the YubiKey an effective defense against phishing attacks.

User presence

- Many authentication solutions expose vulnerabilities through remote attacks after the device is authenticated.
- The touch sensor on the YubiKey verifies that the user is a real human and the authentication is done with real intent. It also verifies that the authentication is not triggered remotely by an attacker or trojan.

Many apps, no shared secrets

- And finally, YubiKeys authenticate through the FIDO open standard, enabling access to thousands of applications and services, providing high security and privacy at scale, across both your work and personal life.

FIDO for developers

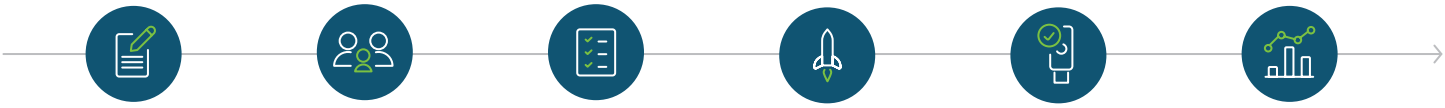
Learn how to adopt passkeys in your application: developers.yubico.com

Takeaway

Organizations need to move from legacy authentication standards to modern FIDO2-based authentication standards to ensure modern phishing-resistant authentication and be future-proofed for compliance.

Yubico solutions are designed to meet you where you are on your cybersecurity journey, paving the way to a modern authentication infrastructure based on the passwordless FIDO2 specification.

We have made it easy to get started with the YubiKey. We offer a simple 6 Step Best Practice Deployment Guide to help **accelerate modern MFA adoption at scale**:



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 YubiEnterprise Subscription, 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/mfa

Sources

1. IBM, 2023 Cost of Data Breach Report, (July 24, 2023)
2. CISA, Critical Infrastructure Sectors, (Accessed October 24, 2023)
3. Verizon, 2023 Data Breach Investigations Report, (June 6, 2023)
4. Google Cloud, August 2023 Threat Horizons Report, (August 2023)
5. Kurt Thomas, Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking, (May 17, 2019)
6. Edward Helmore, Genetic testing firm 23andMe admits hackers accessed DNA data of 7m users, (December 5, 2023)
7. Lily Hay Newman, Why the Twilio Breach Cuts So Deep, (August 27, 2022)
8. Jessica Lyons Hardcastle, Uber explains how it was pwned this month, points finger at Lapsus$ gang, (September 19, 2022)
9. Jeff Burt, Cisco: Yes, Yanluowang leaked our data. No, it's not serious, (September 13, 2022)
10. 451 Research, 2021 Yubico and 451 Research Study, (April 2021)
11. NIST, NIST SP 800-63-4 Digital Identity Guidelines, (December 2022)
12. OMB, M-22-09, (January 26, 2022)
13. The White House, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, (January 19, 20220)
14. The White House, Executive Order on Improving the Nation's Cybersecurity, (May 12, 2021)
15. European Parliament, The NIS2 Directive, (February 2023)
16. Australian Signals Directorate, Essential Eight Maturity Model, (November 2023)
17. PCI, PCI DSS: v4.0, (March 2022)
18. Jenn Easterly, Next Level MFA: Fido Authentication, (October 18, 2022)
19. David Jones, Microsoft, Apple and Google double down on FIDO passwordless standard, (May 5, 2022)
20. FIDO Alliance, User Authentication Specifications Overview, (Accessed December 18, 2023)
21. W3C, Web Authentication: An API for accessing Public Key Credentials Level 2, (April 8, 2021)
22. Margaret Rouse, Cryptographic Key, (January 18, 2017)
23. Bill Toulas, New TPM 2.0 flaws could let hackers steal cryptographic keys, (March 4, 2023)
24. NIST, NIST SP 800-63-4 Digital Identity Guidelines, (December 2022)
25. NIST, NIST SP 800-63-4 Digital Identity Guidelines, (December 2022)
26. OMB, M-22-09, (January 26, 2022)
27. NIST, FIPS 140-3 Security Requirements for Cryptographic Modules, (March 22, 2019)
28. Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)
29. Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)

yubico

About Yubico

Yubico (Nasdaq First North Growth Market 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 modern, hardware-based passkey authentication security at scale to customers in over 160 countries.

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