yubico

Modern *authentication* for the Federal Government

How the YubiKey complements the PIV and solves U.S. Federal modernization use cases with phishing-resistant MFA

MFA Evolution Across the Federal Government

Using Personal Identity Verification (PIV) for authentication is not practical or possible for all federal employees and contractors. Guidance such as the White House Executive Order 14028 and Office of Management and Budget Memo M-22-09, and more importantly, cyber attacks from nation-states to criminal organizations have put pressure on the federal government to deploy phishing-resistant authentication as part of a Zero Trust Architecture to secure users along with sensitive and critical citizen data.

While PIV meets the highest assurance of MFA when using Federal Government Public Key Infrastructure (PKI), there are a growing number of scenarios that have the same assurance requirements where PIV is not available or practical. These scenarios include secure access for personal devices, remote users, privileged users, shared devices, air gapped networks, SCADA and ICS environments, and non PIV eligible users. For example, PIV reader support for mobile phones or tablets is limited or non existent, and teleworking with an external COTS PIV reader leaves the device open to potential malware.

What is Fast Identity Online (FIDO)?

FIDO2 is an open authentication standard, created by the FIDO Alliance, that consists of the W3C Web Authentication specification (WebAuthn API), and the Client to Authentication Protocol (CTAP). CTAP is an application layer protocol used for communication between a client (browser) or a platform (operating system) with an external authenticator such as a hardware security key. FIDO2 authentication options include strong single factor (passwordless), two-factor, and multi-factor authentication. Yubico is a core contributor to the FIDO2 open authentication protocol.

Not All MFA Is Created Equal

For those use cases where the PIV is limited or not practical, falling back on username and passwords or legacy multi-factor authentication (MFA) is risky. Usernames and passwords are easily hacked, and legacy mobile-based authentication such as OTP, SMS and push notification apps are not phishing resistant. Accounts using MFA that are not based on phishing-resistant protocols are susceptible to having credentials stolen.

The draft National Institute of Standards and Technology (NIST) Digital Identity Guidelines (SP 800-63-4), designed to guide agencies with digital identity assurance and authentication, outlines the technical requirements for phishing-resistant authentication, recognizing two methods as being phishing-resistant: channel binding such as using a PKI-based SmartCard and verifier name binding such as using a Fast Identity Online (FIDO)-based credential and authenticator.

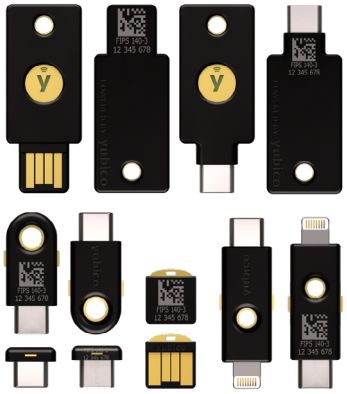
What qualifies as phishing-resistant MFA?

Channel binding PIV/CAC/Smart Card

PIV CAC Smart Card

Verifier name binding FIDO2/WebAuthn

External authenticator | Client/platform (internal authenticator) | Relying party

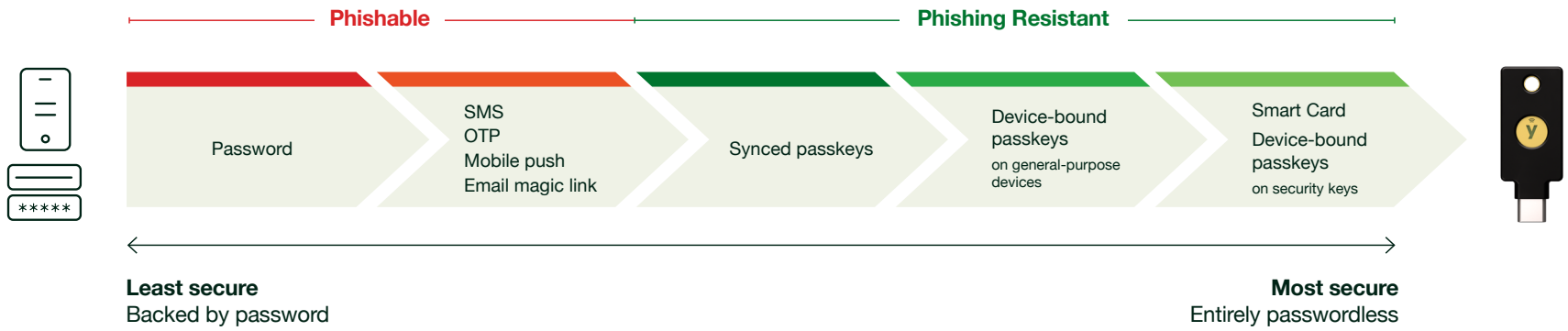


The YubiKey 5 FIPS Series

The YubiKey Offers FIPS-Validated Phishing-Resistant MFA

Yubico offers the phishing-resistant FIPS 140-3 validated YubiKey, a hardware security key that offers highest-assurance multi-factor and passwordless authentication in accordance with Homeland Security Presidential Directive 12 (HSPD 12). The YubiKey has been adopted by many departments and agencies where the PIV card format is not available nor practical, by leveraging derived PIV credentials.

The YubiKey supports derived credentials and provides the highest levels of security needed to protect against modern day attacks along with the flexibility to secure even the most complex scenarios—from remote work and cloud services—all from a single key. With multi-protocol support including Smart Card (PIV), FIDO2, OTP and OpenPGP, the YubiKey supports both legacy and modern architectures with a single solution, and offers a future-proofed bridge to modern FIDO authentication standards.



A single YubiKey can provide both PKI and FIDO2/WebAuthn phishing-resistant authentication to securely authenticate users to applications and services across government furnished equipment (GFE) or personal devices such as laptops, desktops, tablets, and mobile phones. Unlike managing multiple certificates across mobile devices along with a PIV card, a YubiKey with a USAccess derived credential issued through a modern Credential Management System (CMS) can be used as a portable root of trust across multiple devices including mobile and personal devices, eliminating the cost of deploying certificates across multiple devices. A single YubiKey can provide both PKI and FIDO2/WebAuthn phishing-resistant authentication, housing multiple of each credential. Following industry standards for smartcard certificates, a YubiKey can hold either USAccess PKI credentials, issued by commonly used CMS, or an organization can host their own PKI to provide credentials to non-PIV eligible personnel, or for air-gapped and other accepted networks.

Phishing-Resistant MFA Scenarios

Securing non-PIV eligible users

Non-PIV eligible personnel such as interns, onboarding new employees, contractors and other users that require 3rd party access still require secure access to federal systems. To meet these needs, the YubiKey meets OMB M-22-09 phishing-resistant MFA at Authenticator Assurance Level 3 (AAL3) when PKI is infeasible—a FIPS 140-3 validated alternative to the PIV that allows non-PIV personnel or personal non-GFE devices in a Bring Your Own Device (BYOD) environment to securely authenticate to government networks.

Securing telework, field workers & personal devices

Supporting remote workers, field workers such as security agents, inspectors, and auditors using personal devices with a PIV creates complexity. While password-based authentication may simplify remote access, relying on single-factor authentication does not satisfy zero trust security and phishing-resistant authentication requirements.

Fortunately, YubiKey works with leading Identity and Access Management (IAM) and Identity Provider (IdP) solutions to enable phishing-resistant access for remote and hybrid employees and employees on the move, without the need for supporting devices. In cases where remote and hybrid workers are sent GFE devices, the YubiKey can also be used as a portable root of trust to ensure the device hasn't been compromised enroute.

YubiKeys have the flexibility to be used with a wide range of mobile devices and unmanaged and managed workstations, including Chromebooks and personal phones. When a YubiKey has been provisioned with derived credentials, it becomes a portable root of trust for user's identities, making it easier to authenticate regardless of the device. Users in sensitive areas or in public places, may want to maintain a level of anonymity from those around them. Authenticating with the YubiKey precludes them from using an identifiable HSPD-12 card.

Securing privileged users

Using a YubiKey with an additional PIV certificate for elevated privileges significantly enhances security by segregating routine access from high-risk administrative functions, reducing the attack surface if one set of credentials is compromised. This setup offers streamlined management by consolidating multiple certificates on a single device, where allowed, simplifying user workflows and administrative oversight. It also ensures compliance with strict regulatory standards through robust, multi-factor authentication mechanisms and detailed audit trails.

Ensuring secure phishing-resistant user access to classified, secret and personal information is critical for those privileged users that cannot use the PIV to authenticate. The YubiKey offers the highest-assurance alternate authentication that can be used to authenticate privileged users to both legacy and modern applications. The YubiKey's hardware design enables the authentication secret to be stored on a secure hardware chip that cannot be copied or stolen, offering the highest security for authenticating privileged users. The YubiKey can also be used for step-up authentication for high-security applications.

Microsoft 365 tenant admins cannot use their primary PIV credentials to authenticate for daily tasks and maintenance. Microsoft Azure supports the enrollment of a YubiKey as a FIDO2 authenticator. Admins are able to quickly enroll a YubiKey for their privileged user roles to meet phishing-resistant authentication requirements. A YubiKey as a FIDO2 token uses public/private keypairs, bound to the tenant URL, to ensure strong authentication is met.

Securing shared devices & workstations

Shared devices have the challenge of supporting multiple users, each requiring their own credentials for authentication. By shifting the storage of the credentials from the device to a hardware-based authenticator, like a YubiKey, each individual can be issued a security key for authentication on any of the shared devices. Users and contractors that use shared workstations and shared devices such as government call center workers, healthcare employees across agencies such as Department of Health and Human Services, Centers for Disease Control and Prevention and Department of Veterans Affairs, operational technology environments (OT) across laboratories, research centers and manufacturing floors such as those run by the Department of Energy, federal educational institutes and others, can benefit from using the YubiKey as a portable root of trust for secure authentication. Users can authenticate to the network using the trusted credential on their YubiKey, proving that they are a trusted user.

A single YubiKey works across multiple shared devices including desktops, laptops, mobile, tablets, and notebooks, enabling users to utilize the same key as they navigate across devices. YubiKeys are also easily re-programmed, making them suitable for rotating-shift and temporary users across these environments.

Securing citizen data and access

Many government agencies store citizen-related sensitive and personal personally identifiable information (PII) including but not limited to social security numbers, tax, banking information and health information. Breaches to these databases and user accounts can have damaging consequences. Ensuring secure access to such data includes phishing-resistant access controls not just for government employees that require access to the data, but also for citizen self-service portals. Securing these digital accounts with legacy, phishable forms of authentication is putting citizens at risk. The YubiKey can be offered as a high-security solution to citizens to ensure their digital accounts are not at risk of being breached. YubiKeys can be shipped directly to each user even at their residential address.

Ready to get started?

When you choose YubiKeys as a service, you make decisions as you go with our insight and help, simplifying the process of scaling YubiKeys to wider circles of use cases and leveraging the insight from over 150 U.S. government implementations to date. We have created a six step deployment process to plan for and accelerate adoption of phishing-resistant MFA at scale.

Plan

Ensure **readiness** by clarifying use case 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**

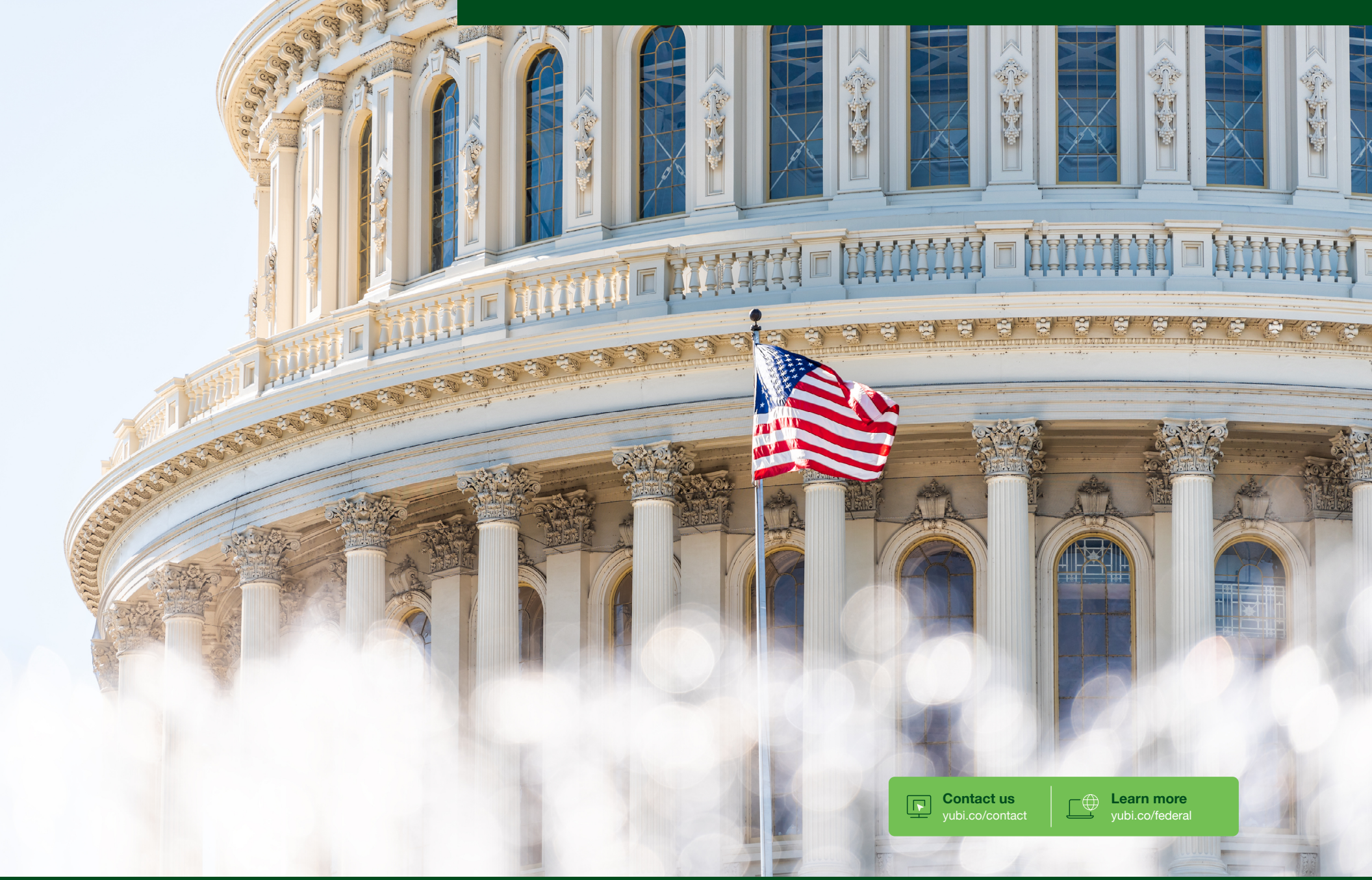
Measure

Report on security and business value impact

Bailment agreement can be established to obtain Not for Resale (NFR) YubiKeys for proof of concept (POC) programs. These YubiKeys are not required to be returned and, as a condition of use, are not to be continued for enterprise use at the conclusion of the POC. Yubico also offers solutions engineering support for architecture design and review, and IDP configuration guidance through the POC.

Once ready to purchase, Yubico is focused on helping agencies easily access security products and services in a flexible and cost-effective way to heighten security:

- With YubiKey as a Service, organizations can benefit from simple and scalable global deployments of YubiKeys for their workforce, supply chain, and end customers. YubiKey as a Service offers customers a choice of form factors, replacement stock, and priority customer support, all for less than the price of a cup of coffee per month. Customers also have access to turnkey Enrollment and Delivery services that help IT get users quickly onboarded with YubiKeys to fast track to phishing-resistance and then get YubiKeys to end users across the world, including corporate and residential addresses. Users can even experience self-service ordering of YubiKeys, giving them the freedom to have the keys shipped to their preferred address anytime they need. YubiKey as a Service customers receive continual enhancements to available and new services assuring a smart and future-proofed security investment.
- Yubico's Professional Services team can help you with a successful implementation. Yubico offers a wide variety of advisory services in support of your YubiKey implementation and deployment, including best practices workshops, technical implementation packages, on-demand consulting resources and custom engagements. Our Professional Services team is comprised of trained and accredited security professionals with experience gained from hundreds of customer implementations across a wide range of industries and the government sector. From standard implementations to complex enterprise rollouts, Professional Services has the skills and expertise to help guide you through all facets of your YubiKey implementation and deployment.



Contact us
yubi.co/contact

Learn more
yubi.co/federal

yubico

Yubico (Nasdaq Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA), and a creator and contributor to FIDO open authentication standards. The company is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries. For more information, visit: www.yubico.com.