



BEST PRACTICES GUIDE

How to get started with phishing-resistant MFA to secure federal government

Six deployment best practices to accelerate adoption at scale



89%



of high value assets unprotected by MFA, according to 2023 audit of the U.S. Dept. of the Interior

>20%



of active user passwords were easily cracked.

Choosing the right MFA approach for federal government

Government entities remain under **persistent cyberattack**, often from threat actors who leverage sophisticated technologies that combine malware, phishing and/or hacking. These complex attacks are often linked with the use of stolen credentials and the supply chain, including notable attacks against Colonial Pipeline and SolarWinds.¹

In the face of these attacks, the White House Executive Order 14028, Office of Management and Budget (OMB) Memo M-22-09², and the Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems (NSM-8)³ charged agencies to modernize information technology (IT) and operational technology (OT) systems, implement stronger cybersecurity standards based on Zero Trust such as phishing-resistant multi-factor authentication (MFA), and to improve the software supply chain. Further, NIST has released several updates (FIPS 201-3⁴, SP 800-157r1⁵, SP 800-217⁶) that **expand authentication options beyond PIV cards** to support modern FIDO authentication standards and expand the use of derived PIV credentials to new form factors and use cases to support the expanded use of cloud services and the need to establish and authenticate digital identities.

The Zero Trust Maturity Model (ZTMM) was developed by CISA (v 2.0 April 2023) to assist federal agencies in the development of their **zero trust strategies**, recognizing the incremental processes necessary to support change across all five pillars of the model: identity, devices, networks, applications and workloads, and data. The ZTMM represents a gradient of zero trust architecture implementation from a “traditional” starting point toward three further stages, each with greater levels of protection.

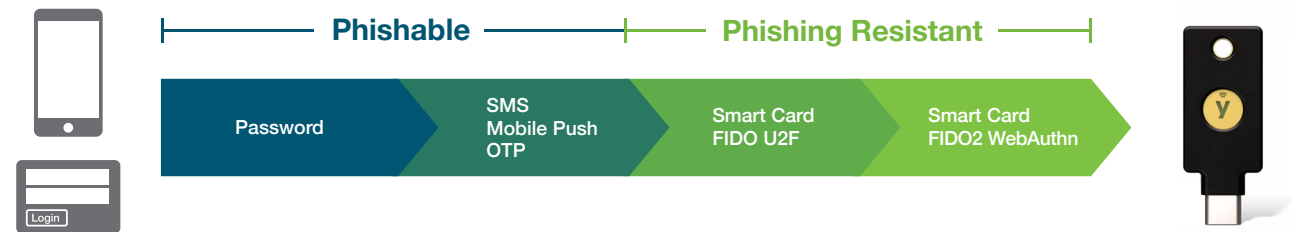
A zero trust strategy reduces risk by assuming all users, devices, applications and transactions are potential threats that should be **verified and authenticated** before access is granted toward the “optimal” of continuous validation. The National Cybersecurity Strategy released in 2023, commits the Federal government to replace or update IT or OT systems in the next decade in order to support the OMB zero trust architecture strategy.⁷

MFA is a foundational aspect of establishing trust as part of a zero trust architecture, yet a 2023 audit of the U.S. Department of the Interior found that 89% of high value assets were unprotected by MFA and more than one-fifth of active user passwords were easily cracked.⁸ Most basic authentication methods, including SMS, mobile push apps and one-time passcodes, are susceptible to account takeovers from phishing, social engineering and attacker-in-the-middle attacks. OMB Memo M-22-09 recognizes that **not all forms of MFA are created equal** and directs federal agencies to adopt the exclusive use of **phishing-resistant MFA** by the end of Fiscal Year 2024.⁹

What is phishing-resistant MFA?

Phishing-resistant MFA processes rely on cryptographic verification directly between devices or between the device and a domain, making them highly secured against attempts to compromise or subvert the authentication process.

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63¹⁰, two forms of authentication currently meet the mark for phishing-resistant MFA: PIV/Smart Card and the modern FIDO2/WebAuthn authentication standard.



YubiKey offers phishing-resistant MFA

Yubico offers the phishing-resistant **FIPS 140-2 validated YubiKey**, a DOD-approved¹¹ hardware security key that offers highest-assurance multi-factor and passwordless authentication in accordance with Homeland Security Presidential Directive 12 (HSPD 12)¹². The YubiKey is successfully deployed in federal agencies including the U.S. Army, U.S. Navy, U.S. Air Force, U.S. Marine Corps, U.S. Space Force, DoD Missile Defense Agency, Federal Bureau of Investigation (FBI), National Security Agency (NSA), Department of Energy and more.

Hardware security keys such as the YubiKey are an ideal option for **strong phishing-resistant MFA** because they don't require external power or batteries, or a network connection—a user can use a single key to secure hundreds of products, services and applications, including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services, with the secrets never shared between services. The YubiKey cultivates phishing-resistant users which then creates phishing-resistant enterprises. YubiKeys are also ideal for defense personnel as they offer anonymity over Smart Cards with no visual amplifying personal information on the YubiKey.



Mutli-protocol support

The YubiKey is multi-protocol, supporting both **PIV/Smart Card** and **FIDO2/WebAuthn standards**, as well as Defense Information System Agency (DISA) **Purebred derived PIV/CAC credentialing**.

FIPS validation

The YubiKey is FIPS 140-2 validated to meet the highest authentication assurance level 3 requirements (AAL3) of the revised NIST SP800-63B guidelines, Overall Level 1 ([Certificate #3907](#)) and Level 2 ([Certificate #3914](#)), Physical Security Level 3. The YubiKey meets DoD mobile PKI credential storage requirements for mobile PKI credentials.¹³ The YubiKey is also CMMC Level III, DFARS and NIST SP 800-171 compliant and can help supply chain services or solutions achieve FedRAMP High Certification.

The YubiKey is proven to **reduce risk by 99.9%** while delivering a great user experience, letting users securely log in with a single tap or touch:



Strongest security

Reduce risk
by 99.9%



High return

Experience ROI
of 203%



More value

Reduce support
tickets by 75%



Faster

Decrease time to
authenticate by >4x

*Forrester Research, The Total Economic Impact of Yubico YubiKeys, September 2022

The deadline for exclusive use of phishing-resistant MFA is fast approaching. **But how do you start the journey?** The remainder of this guide will detail six key best practices for a successful YubiKey deployment.

What are passkeys?

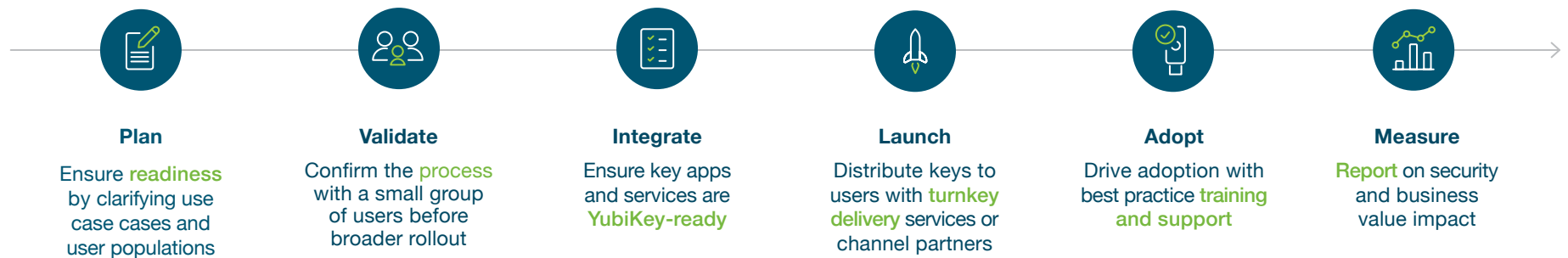
Passkeys are a new term in the industry, but the concept is not new. Passkeys are a new name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences. There are different passkey implementations:

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.

Six key best practices to accelerate the adoption of phishing-resistant MFA

Getting started is easy. Based on Yubico's experience assisting hundreds of customers to deploy phishing-resistant MFA, including over 150 U.S. government implementations, we have created a six step deployment process to plan for and accelerate adoption of phishing-resistant MFA at scale.



01. Plan

Clarify use cases and ensure readiness

A phased approach is the best way to ensure a frictionless deployment. Put your **high value users and data first**, then expand. Rank use cases and user populations based on risk, workforce location, business impact and ease of technical integration.

Determine use cases

Top scenarios for modern, phishing-resistant authentication



Privileged access/high-security applications

Protect targeted users who have elevated access to systems or access to classified data, systems or high-security applications.



Remote work

Add a hardware-backed AAL3 token to add extra protection for access to VPN, IAP, IAM, & IdP platforms for government teleworkers.



Air-gapped networks & SCIFS

Authenticate in closed environments without transfer of information across a CDS & no need for network or cellular connectivity.



Cloud access

Authenticate to web apps with federated access via IAM, SSO, Microsoft's native support for the YubiKey, or YubiKey as PIV with CBA direct to Azure.



Mobile devices

A DoD-approved authenticator used with GFE and personal mobile devices to securely authenticate end users to government networks, apps, and services.



Legacy systems

Multi-protocol functionality supports access to older operating environments, code signing, key escrow for email encryption and more.



RSA SecureID replacement

YubiKeys can lower TCO for an on-premises OTP solution by reducing infrastructure & software while allowing an organization to evolve to modern phishing-resistant MFA.



Authentication backup

An affordable backup method of authentication if a primary method is lost, stolen or inaccessible.

User groups



Non PIV/CAC eligible employees & contractors

Phishing-resistant MFA access via FIDO2/WebAuthn for employees, contractors and partners.



Supply chain

A bridge solution supporting Smart Card and FIDO2/WebAuthn for technology vendors now required to support authentication on their own.



Citizen-facing services

Meet the OMB-22-09 requirement to offer phishing-resistant MFA for all public-facing services.

Assemble key stakeholders

While the number of resources on the project can vary based on the size and breadth of the YubiKey deployment, key stakeholders within the following departments can

positively influence the implementation of phishing-resistant MFA across the agency. It's important to have buy-in across all teams to ensure a smooth rollout:







Engage Yubico experts as needed

Yubico, building on its years of helping secure some of the most security conscious organizations in the world, is focused on helping federal agencies easily access security products and services in a flexible and cost-effective way to heighten security. Agencies can benefit

highly from a YubiKeys as a Service model and our Professional Services team offers best-in-class technical and operational guidance in support of your YubiKey implementation and rollout.



YubiEnterprise Services*		Yubico Professional Services	
 YubiKey as a Service	 YubiEnterprise Delivery	 Deployment 360	 Deployment planning
Simplifies how businesses procure, upgrade and support YubiKeys	Global turnkey YubiKey distribution through YubiEnterprise Delivery or local channel partners	Turnkey planning, technical integration and deployment	Jump start with workshops and projects to review use cases or develop a customized strategy

* YubiEnterprise Services are available for organizations of 500 or more users.

02. Validate

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

Validate with a small group of users across a priority use case to gain quick validation and feedback, leveraging Yubico best practice resource guides, videos and

engagements. **Practice, learn and then move forward with expansion.**

03. Integrate

Ensure your environment is YubiKey-ready

YubiKeys can work with any number of professional and personal services with no shared secrets between the services, enabling high security and privacy at scale. A single key can work across over 1000 applications and services and secure your users' work and personal digital lives. To ensure that YubiKeys

are integrated seamlessly with key applications and services you wish to secure, below are some critical questions to think about. It's good to first answer these questions for your validation exercise, then circle around for each expanded deployment.



Works with YubiKey

YubiKeys, the industry's #1 security keys, work with hundreds of products, services, and applications. To browse YubiKey compatibility go to yubi.co/wwwyk.



Who

Who needs access?

Employees, contractors, third parties, supply chain



What

What authentication approach will you take?

MFA (password and strong second factor), passwordless



Where

Where in your environment do you require strong authentication?

Critical infrastructure elements, network, applications, developer tools.

How do you manage access?

IAM, IdP, PAM, SSO, VPN



How

How does location impact deployment?

Remote, hybrid, on-premise, multi-office

What types of devices need to be supported?

Desktop, laptop, smartphone (BYOD or owned)

Prepare to deploy

Optimizing deployment involves organizational change management through effective communication, training

and support. Yubico offers a variety of Professional Services to help you deploy quickly:

Yubico Professional Services



Deployment planning

Rollout plan development and ongoing assistance



Integration services

Architecture and infrastructure review, vendor integration analysis



Implementation projects

Technical engagements to implement YubiKeys in your environment



Service bundles

Flexible consulting hours for when & how you need them



04. Launch

Get keys in hands and plan Go Live events

We want your deployment to be as frictionless as possible for all teams and all users. This includes simplifying deployment plans, helping you answer critical questions about how you will distribute keys to users and how you will manage the YubiKey lifecycle. Yubico solutions are fully vetted and approved for

sale throughout the public sector, both domestically and abroad. Yubico works with FedRAMP-compliant Sebastian Tech Solutions (STS) for rapid, secure logistics/shipping of YubiKeys directly to users in the office, in the field, or even at home.



What?

Increase awareness

Build up **user training** and **support** materials



Why?

Boost engagement

Demonstrate value to the **organization** and the **user**



Distribution

Self-service | Channel Partner | YubiEnterprise Delivery



Key management

Onboarding | Support | Offboarding

YubiKey rollout best practice recommendations



Offer **flexibility and choice** since YubiKeys are available in a variety of form factors



Two YubiKeys per person for backup



Future-proof with **extra keys** to cover for churn or lost/stolen keys



Encourage **security** with personal use policies



Plan an event to make the future of your agency's security exciting

Go Live events

Support the launch with a series of kick-off communications that introduce the YubiKey to users—communicate early, often. The ideal Go Live

communications make users **excited** about the modern features of the YubiKey.

Why users love the YubiKey



Faster



Easier



More Secure





How to?

Educate users

Have clear calls to action on how to **get started** and how to **get help**



05. Adopt

Support adoption and boost engagement

At Yubico, we believe success should not be measured by how many YubiKeys you have, but by **how many keys are being used**.

While the Go Live communications educate users on the 'what YubiKeys are' and the 'why they are important',

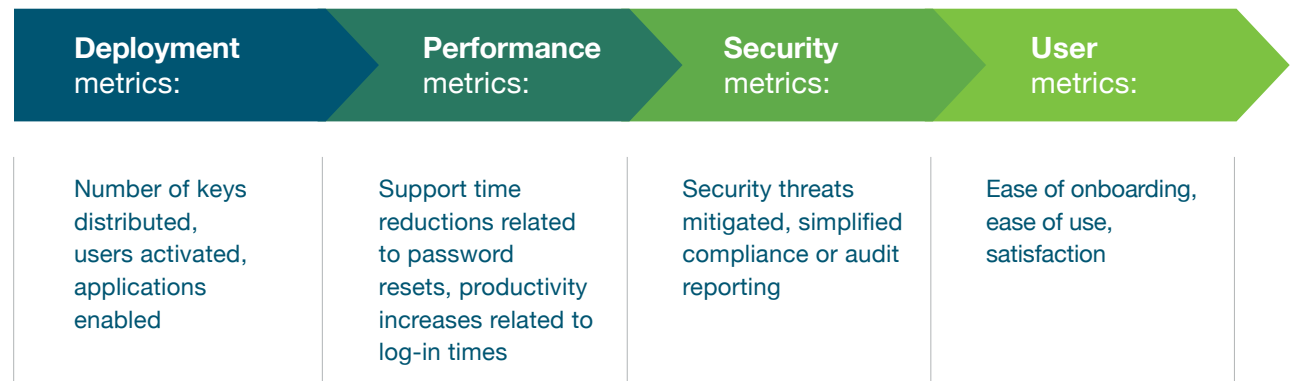
support teams need to be prepared to explain the **how**, with FAQs available to help with any questions that may arise for onboarding and troubleshooting (e.g. what to do in case of a lost key).



06. Measure



Report on security and business impact

We know the truth is in the numbers. Validate the priority use case against these metrics, then continue to measure metrics as you expand to other users to increase the overall business impact.



Ready for scale

Yubico offers expert consulting services, including operational and technical workshops, implementation projects, on-demand resources and custom engagements, designed to jump-start and accelerate your YubiKey deployment at scale.

Professional Services

Expert consulting services, including operational and technical workshops, implementation projects on-demand resources and custom engagements, designed to jump-start and accelerate your YubiKey deployment.

Services Offered
Deployment 360 Program
 A turnkey program packaging all of the essential elements and expertise to ensure your successful YubiKey deployment.

Workshops
 Interactive sessions designed to help jump-start YubiKey integrations and deployments.

Technical Implementation Projects
 Tailored projects designed to facilitate your YubiKey implementation and rollout.

To download the Professional Services Solution Brief go to yubi.co/ps

YubiEnterprise Services*		Yubico Professional Services		
YubiKey as a Service	YubiEnterprise Delivery	Launch planning	Training and support	Analytics and reporting
Cost effective and flexible YubiKey procurement	Global turnkey YubiKey distribution through YubiEnterprise Delivery or local channel partners	Create a marketing and communication plan tailored to your users	Best practice training and support materials and processes	Customized metrics and dashboard design

* YubiEnterprise Services are available for organizations of 500 or more users.



YubiKey as a Service

Gain leading, phishing-resistant authentication security for less than the price of a cup of coffee per user, per month. YubiKeys as a service, via subscription, delivers peace of mind in an uncertain world.

Learn more yubi.co/YKSvc



YubiEnterprise Delivery

Yubico and trusted partners provide IT teams with powerful capabilities to manage delivery of hardware security keys to users globally and accelerate the adoption of strong authentication.

Learn more yubi.co/delivery

YubiEnterprise Services*



YubiKey as a Service



YubiEnterprise Delivery

Yubico Professional Services



Deployment 360

Service hour bundles



Workshops

Implementation projects

* YubiEnterprise Services are available for 500 or more users.



Ready to get started?

As federal agencies accelerate toward zero trust and meet the OMB M-22-09 requirement to adopt the exclusive use of phishing-resistant MFA, federal agencies are shifting to identity-centric authentication that includes traditional PIV/CAC as well as modern FIDO2/WebAuthn to allow for fine-grained authorization and future proof access.

Though the path to adopting strong alternate authenticators to the PIV and CAC or accommodating derived credential requirements can seem daunting, it doesn't have to be.

Don't know where to start? The good news is that you don't need to know all the answers upfront about key choices, technical integration or how to support the expanding set of authentication use cases.

Government agencies can leverage **security as a service** and experienced FedRamp approved channel partners, taking all the guesswork out of achieving success. 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 insights from over 150 U.S. government implementations to date.

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/ps

Sources

- ¹ Verizon, [2024 Data Breach Investigations Report](#), (Accessed May 28, 2024)
- ² Shalanda D. Young, Office of Management and Budget, [M-22-09](#), (January 26, 2022)
- ³ National Security Memorandum/NSM-8, [Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems](#)
- ⁴ NIST, [FIPS 201-3](#), (January 2022)
- ⁵ NIST, [SP 800-157r1](#), (January 2023)
- ⁶ NIST, [SP 800-217](#), (January 2023)
- ⁷ White House, [National Cybersecurity Strategy](#), (March 2023)
- ⁸ Dan Goodin, [A fifth of passwords used by federal agency cracked in security audit](#), (January 10, 2023)
- ⁹ Shalanda D. Young, Office of Management and Budget, [M-22-09](#), (January 26, 2022)
- ¹⁰ NIST, [NIST SP 800-63-4 Digital Identity Guidelines](#), (December 2022)
- ¹¹ DoD OCIO, [Memo](#), (December 20, 2019)
- ¹² Homeland Security, [HSPD 12](#), (January 27, 2022)
- ¹³ DoD OCIO, [Memo](#), (December 20, 2019)



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.