


Strong Phishing-Resistant MFA for EO 14028 compliance


Achieve federal compliance with YubiKeys and Okta


Thank you for downloading this Yubico white paper. Carahsoft is the master government aggregator and distributor for Yubico’s Cybersecurity solutions available via ILTPP, MHEC, NJSBA, and other contract vehicles.


To learn how to take the next step toward acquiring Yubico’s solutions, please check out the following resources and information:


 For additional resources:
carah.io/YubicoResources

 For upcoming events:
carah.io/YubicoEvents

 For additional Yubico solutions:
carah.io/YubicoSolutions

 For additional CyberSecurity solutions:
carah.io/CyberSecuritySolutions

 To set up a meeting:
Yubico@carahsoft.com
844-214-4790

 To purchase, check out the contract vehicles available for procurement:
carah.io/YubicoContracts

For more information, contact Carahsoft or our reseller partners:
Yubico@carahsoft.com | 844-214-4790



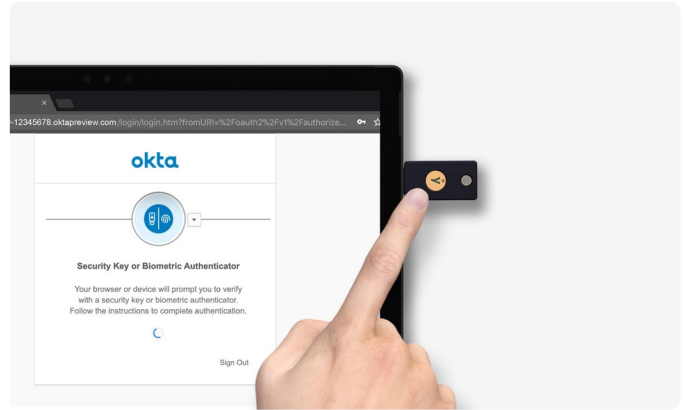
Strong phishing-resistant MFA for EO 14028 compliance

Executive Order (EO) 14028 and OMB memo M-22-09 shift the cybersecurity principles for federal agencies, their staff, contractors, and partners from perimeter-based defenses to a Zero Trust architecture strategy that includes the requirement for phishing-resistant MFA.

Phishing-resistant MFA refers to an authentication process that is virtually immune to sophisticated attacks that could intercept or trick users into revealing access information. Phishing-resistant MFA establishes an authenticated protected channel with the verifier, protecting against verifier impersonation attacks through impostor websites or fraudulent push authorization attempts.

As defined by the Federal Information Processing Standards (FIPS) 140-2 and NIST SP 800-63B, only two authentication technologies currently meet this requirement: the federal government’s Personal Identity Verification (PIV) standard/ smart card and the modern FIDO2/WebAuthn standard.

According to this guidance, agencies and their supply chain partners must move beyond authentication methods that fail to resist phishing, including passwords, as well as those that rely on SMS or voice calls, one-time codes, or mobile push notifications.



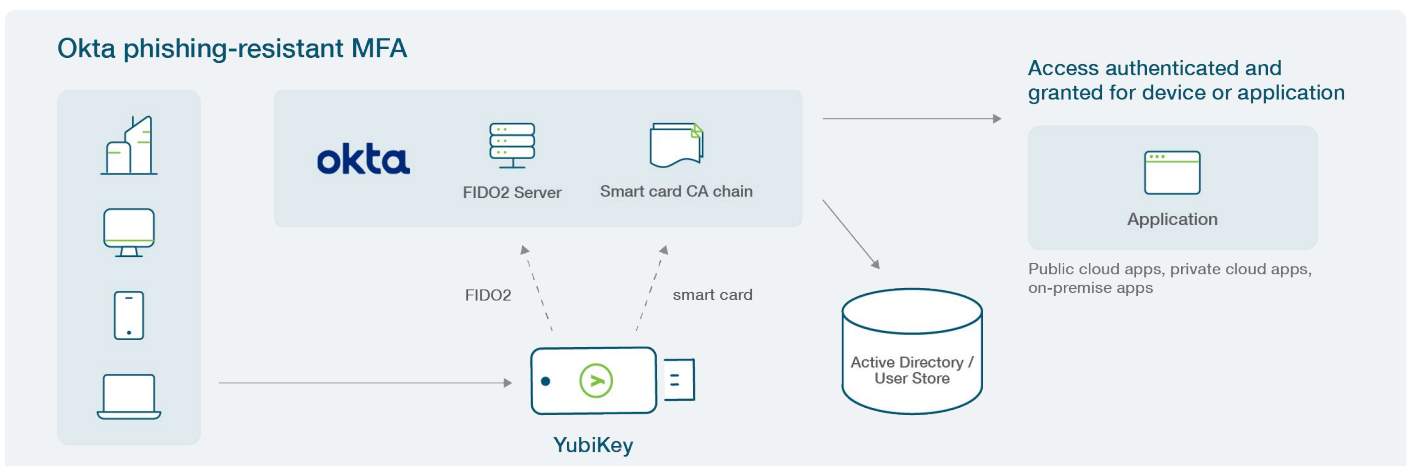
Achieve federal compliance with YubiKeys and Okta

Yubico offers the YubiKey—a FIPS 140-2 validated hardware security key proven to stop 100% of account takeovers in independent research. Users of Okta Adaptive MFA can combine adaptive authentication and contextual access management with native support for the YubiKey as a PIV-compatible smart card for immediate compliance with the authentication requirements of OMB M-22-09 in a Zero Trust framework:

- FIPS 140-2 validated (overall level 1 and level 2, physical security level 3)
- Validated to NIST SP 800-63-3 Authenticator Assurance Level (AAL) 3 requirements

With Okta and the YubiKey, government agencies can deploy FIPS validated, hardware-backed MFA across multiple applications and operating systems, as well as modern devices with single-sign-on (SSO) capabilities. Okta and the YubiKey support the strongest authentication methods including certificate-based authentication (CBA) and FIDO2/WebAuthn. With CBA supported by a PKI, a user can leverage the YubiKey as a PIV-compatible smart card with Okta to access protected applications and services using a x.509 compliant digital certificate. For customers without a PKI option, FIDO2 can also be used to provide a strong phishing-resistant authentication option.

61% of data breaches are traced to credentials¹



¹ Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021)

Stronger together

Yubico, combined with Okta Adaptive MFA, offer the best of both worlds—intelligent, modern phishing-resistant MFA to protect against account takeovers, as well as a simplified user experience that is adaptive to the level of identity assurance all the way up to hardware-based authentication for stronger levels of protection. YubiKeys are also durable, don't require batteries or need a cellular connection, and are water-resistant and crush-proof. Here are some additional benefits to using YubiKeys with Okta:



Enable the bridge to passwordless authentication

Yubico and Okta work together to meet organizations where they are on their journey to passwordless, seamlessly supporting legacy infrastructures with multi-protocol flexibility as well as modern, cloud-based systems that leverage the latest FIDO2/WebAuthn standards.



PIV-compatible smart card

For organizations with PKI infrastructure, YubiKey enables smart cards as a primary authentication method to sign in to Okta managed applications and services using a x.509 compliant digital certificate; Okta accesses the certificate revocation list from the certificate authority.



Convenient login for higher employee productivity

No matter the device, user or login context, Okta Adaptive MFA and YubiKey together deliver a more reliable, secure and simplified login experience to Okta's SSO, reducing support calls and downtime.



Supply chain and customer access

Provide federated support to partners, 3rd party entities and even customers to prevent breaches.



Secure privileged users, mobile-restricted environments

Improve security and productivity for privileged users or those sharing workstations and provide support for remote workers, contractors, air-gapped/isolated networks, cloud services, high-risk military scenarios, and mobile-restricted environments.



Superior authentication

High-assurance authentication provided by the combination of the YubiKey 5 FIPS Series (FIPS 140-2 / NIST SP800-63B AAL3 validated) hardware security key and Okta Adaptive MFA policy framework.



Adaptive and risk-based authentication

Administrators can define advanced authentication with Okta Adaptive MFA, pairing and device posture policies to trigger intelligent step-up MFA with the YubiKey or to accept trust within geo-fenced or other defined scenarios.



Enhance security posture with streamlined deployment

Okta and the YubiKey add strong authentication to identity platforms to bring a complete, easy-to-scale offering to organizations of all sizes, supported by YubiEnterprise subscription and delivery options.

Does the EO impact you?

While the Executive Order mandates requirements for federal agencies, it reaches far beyond. It has critical implications for many regulated and private sector industries such as defense, supply chain, healthcare, technology, and financial services.

Talk to us

www.yubico.com/contact-us
www.okta.com/contact-sales/

Learn more

yubi.co/eo-hub

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: www.yubico.com.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
5201 Great America Pkwy, #122
Santa Clara, CA 95054, USA
844-205-6787 (toll free)
650-285-0088