yubico

# YubiKey for Mobile in the Public Sector

Securing mobile, tablet and notebook users with high-assurance multi-factor authentication

## Growing mobile usage exposes security risks

Mobile device usage across government agencies is on the rise, yet PIV and CAC cards are cumbersome to use with mobile devices. Mobile authenticators including SMS, OTP and push notifications aren't secure against malware, SIM Swapping, and man-in-the-middle attacks. And in the case of BYOD/BYOAD, put government and other public sector entities on point to reimburse employees and contractors for mobile costs. Public sector entities need to provide enhanced authentication that is secure, doesn't create high recurring expenses and can enable personnel to securely work in any location, on any device, and across any network.

## The YubiKey works across Microsoft Windows, iOS, macOS, Android, Linux, and leading browsers

The YubiKey offers secure authentication for mobile phones, tablets, notebooks and leading operating systems, comes in a FIPS 140-2 validated model, and supports derived PIV/CAC requirements. The YubiKey is designed to provide authentication and a portable root of trust for both mobile devices and computers and provides a faster, more secure alternative to authentication using passwords, SMS codes and mobile apps. The YubiKey makes it easy to deploy strong, scalable authentication that eliminates account takeovers from phishing and other attacks. By providing a secure and easy way for users to enroll to their mobile app, and use step-up authentication, the YubiKey significantly enhances security and reduces IT support costs.

## The YubiKey is a hardware-based solution that offers the following capabilities:

- The YubiKey 5 FIPS Series is FIPS 140-2 validated and enables government agencies and regulated industries to meet the highest authenticator assurance level 3 (AAL3) requirements from the new NIST SP800-63B guidance.
- The YubiKey 5 NFC FIPS supports multiple authentication and cryptographic protocols including WebAuthn/FIDO2, U2F, PIV-compatible smart card, and Yubico OTP, and is available with USB-A, and NFC to protect employee access to computers, mobile devices, networks, and online services with just one touch or secure tap-and-go.
- The YubiKey 5C NFC FIPS supports multiple authentication and cryptographic protocols including WebAuthn/FIDO2, U2F, PIV-compatible smart card, and Yubico OTP, and is available with USB-C and NFC to protect employee access to computers, mobile devices, networks and online services with just one touch or secure tap-and-go.
- The YubiKey 5Ci FIPS offers multi-protocol support and is available with both USB-C and Lightning connectors to secure apps and services across all major platforms, including Apple devices.

**YubiKey** works across iOS and Android devices, as well as Microsoft Windows, macOS, Linux, and leading browsers

# YubiKey: DOD approved strong authentication for mobile and BYOD/BYOAD

## Secure enrollment for internal and citizen-facing mobile apps

- The YubiKey stores the authentication secret on a secure element hardware chip. This secret is never transmitted and therefore cannot be copied or stolen, providing superior defense against phishing.

## Reduces IT costs

- The YubiKey dramatically reduces the primary IT support cost—password resets—which cost Microsoft over $12M per month.
- By switching from mobile one time passwords (OTPs) to the YubiKey, Google reduced password support incidents by 92% because the YubiKey is more reliable, faster, and easier to use.
- In the event of an organization using mobile devices as a second factor, replacement costs are high if a user loses their device or it is stolen. In contrast, replacing a YubiKey is far more cost efficient and fast.

## Easy to use, fast, and reliable

- Users don't need to install anything—customers or employees simply register their YubiKey, enter their username and password as usual, and plug in and tap the YubiKey when prompted.
- YubiKeys are crush-resistant, water-resistant and tamperproof.

## Easy to deploy

- IT can deploy the YubiKey in days, not months. A single key can access multiple modern and legacy systems.

## Trusted authentication leader

- Yubico is the principal inventor of the U2F and WebAuthn/FIDO2 authentication standards adopted by the FIDO alliance and was the first company to produce the Security Key Series by Yubico that incorporates both U2F and FIDO2/WebAuthn support.
- Widely deployed in the US Government with over 150 unique implementations including US Army, US Navy, US Air Force, US Marine Corps, US Space Force, DoD Missile Defense Agency, Federal Bureau of Investigation (FBI), National Security Agency (NSA), Department of Energy and more.
- YubiKeys are produced in our offices in the USA, maintaining security and quality control over the entire manufacturing process.

### Yubico SDK for iOS and Android:

- Enable rapid integration of the YubiKey with mobile apps on iOS and Android
- Effectively secure enrollment to in-house and consumer apps
- Enable step-up authentication for sensitive transactions
- Deliver a seamless user experience

For more information on the Yubico SDK for iOS and Android, please visit: https://www.yubico.com/why-yubico/for-developers/

**About Yubico** Yubico sets new global standards for easy and secure access to computers, servers, and Internet accounts. Founded in 2007, Yubico is privately held with offices in Australia, Germany, Singapore, Sweden, UK, and USA. Learn why nine of the top 10 internet brands and millions of users in more than 160 countries use our technology at **www.yubico.com.**

**Yubico Inc.**
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088