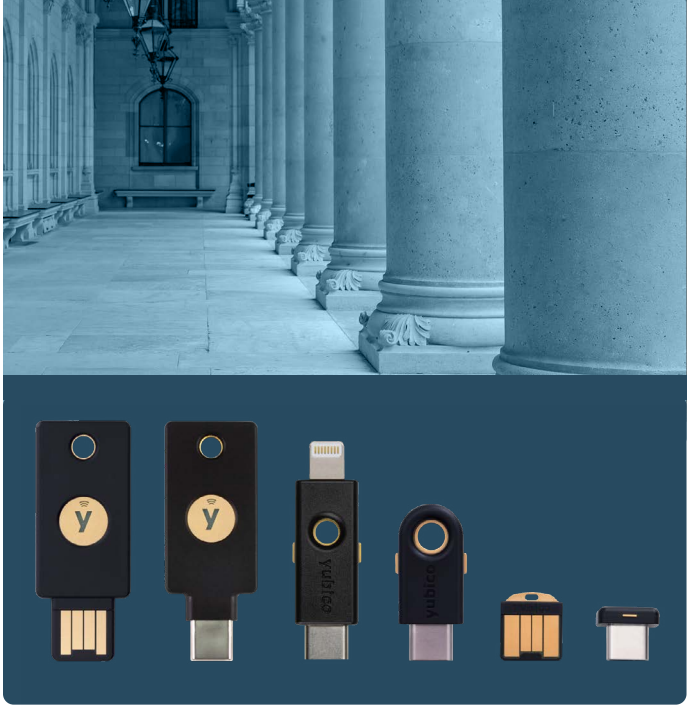
yubico

YubiKey as Root of Trust for Government

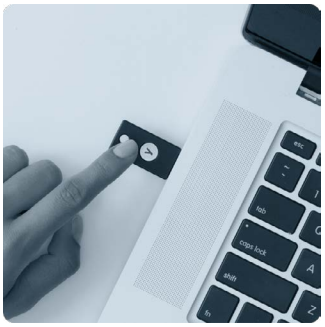


A hardware root of trust offers the most secure authentication implementation as it is protected against malware attacks. For the Department of Defense (DoD) and other government agencies, Personal Identity Verification (PIV) and Common Access Card (CAC) have been traditionally used as the hardware root of trust. But there are many situations where PIV and CAC are difficult to set up or not applicable; such as for remote workers, non PIV and CAC eligible workers, mobile devices and Bring Your Own Approved Devices (BYOAD), and shared devices/workstations.

The YubiKey is a DoD approved, FIPS 140-2 validated hardware security key (Certificate #3914), that supports derived credentials such as Purebred. Government agencies can leverage the YubiKey as a portable root of trust to keep workers, contractors, DIB partners and constituents secure against account takeovers. Credentials are stored on the YubiKey enabling users to move seamlessly across devices such as mobile devices, laptops and desktops without the need for PIV and CAC infrastructure, SMS codes or authenticator apps.

With the YubiKey as a portable root of trust, users can:

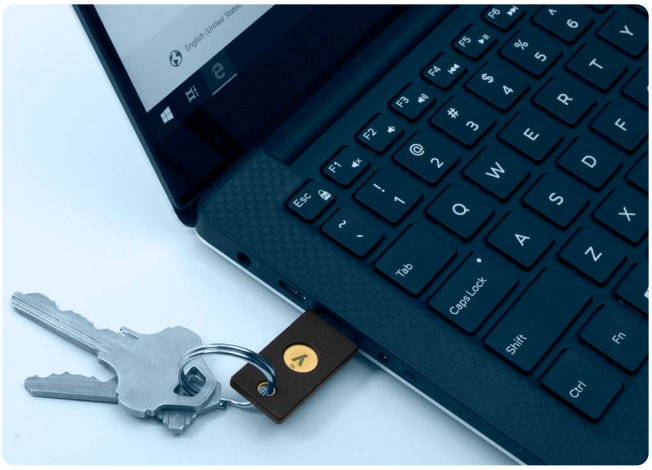
- Rapidly convert any device into a trusted device
- Have a portable credential to authenticate seamlessly across multiple devices
- Experience fast account recovery in case of a lost or stolen device



In the case of derived credentials stored directly on a device, if a phone or computer is lost or stolen, it can cause a security breach if a cybercriminal is able to extract the derived credential from the device. On the other hand, credentials stored on YubiKeys are much more secure and cannot be extracted or tampered with. If a mobile/computer device is lost or stolen, the YubiKey can be used as an easy method to re-establish trust with online accounts and re-register the internal authenticator on a new device. The YubiKey as an external root of trust allows a high degree of trust to be transferred from device to device, establishing them as trusted entities.

YubiKey as portable root of trust use cases:

BYOAD and GFE—Whether BYOAD or Government Furnished Equipment (GFE), most mobile devices don't support smart card based authentication. With the YubiKey as a portable root of trust; government workers, contractors and DIB partners can authorize their personal mobile devices for use on government networks, and to install government applications, mobile device management applications, email programs etc., making these devices trusted. Devices need to be authorized only a single time, but based on agency policies, workers may still be required to securely authenticate to government apps and services on their mobile devices. Even GFE devices can benefit from the YubiKey, especially in the case of remote workers, where government devices are mailed to personal residences. In this scenario, the YubiKey can be used as a portable root of trust to ensure the device hasn't been compromised on route by a hacker.



Multi-device access—In today's digital age, users rarely work from a single device or platform. It's common to move from a mobile device to desktop, laptop, or tablet; or even between personal and work devices. Having a portable external authenticator that can work across all computing devices makes these transitions seamless. With options to connect via NFC, USB-A, USB-C, and Lightening, the YubiKey meets the needs of all government workers and devices.

Shared devices/workstations—Government workers that use shared devices/workstations can benefit from a portable root of trust similar to the PIV and CAC. They can authenticate to the network using the trusted smart card credential on their YubiKey, proving they are a trusted user.

High-security applications—Without ties to the internet or a multi-purpose chip or computing device, the attack vector naturally becomes much smaller on an external hardware authenticator. There are certain scenarios where services may choose to require step-up authentication to complete a high-risk action, such as accessing highly classified systems and documents. The YubiKey can be used as an additional form of validation for high-security applications, to quickly re-verify the user before access is granted or a required action is taken.

Authentication for legacy systems—Most government agencies use a variety of systems, platforms, and devices, and not all of these support newer authentication standards such as FIDO, WebAuthn and PIV/CAC. YubiKeys are appropriate as they support multiple protocols such as smart card, FIDO U2F, FIDO2/WebAuthn, OpenPGP, and OTP. The YubiKey's multi-protocol functionality also helps address a wider range of security needs such as for computer login and remote access, digital signatures for code signing, key escrow for email encryption, or privilege access for older operating environments.

Authentication backup—Regardless of how users are authenticating to their accounts, it is always a best practice to have a backup method in case the primary method of authentication is lost, stolen, broken, or inaccessible. The YubiKey is an affordable, simple option that government workers can carry on their keychain, tuck into a wallet, or store in a safe place for convenient access at any time.

A portable root of trust that is future-proofed

As government agencies adopt newer authentication standards and protocols in the future such as WebAuthn/FIDO2, YubiKeys can easily transition from smart card PIV and CAC credentials to support newer FIDO-based authentication. This makes them the best choice for a portable root of trust today; and tomorrow when government agencies are ready to adopt modern FIDO2 authentication standards.

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