yubico

Modern hardware-backed multi-factor authentication and compliance for Federal Government

How the YubiKey meets
US Federal Government regulations
with phishing-resistant MFA

Contents

The evolution of Federal authentication

Authentication gaps in modern infrastructures and processes

Drivers for alternative authentication solutions include:

- Teleworkers
- Non PIV/CAC eligible workers including short-term contract workers
- Mobile and BYOD / BYOAD device support
- Closed / air-gapped network support
- Cloud services
- DIB and coalition partners

Federal agencies, both military and civilian, face some of the most stringent and shifting data protection regulations and standards. With the mix of evolving special publications, memos, standards, modules, and executive orders, it can be difficult to keep track of the shifting goalposts for data security and authentication for federal agencies and other organizations that deal with the government.

For years, government agencies have relied heavily on public key infrastructure (PKI) and the Personal Identity Verification (PIV) and the Common Access Card (CAC) smart card standards that meet Federal Information Processing Standards (FIPS) 140-2.

While PIV and CAC met the needs for traditional perimeter-based and desktop federal authentication requirements, the modernization of IT and related devices, and recent events such as COVID-19 and have created edge cases where PIV and CAC aren't the most suitable forms of authentication.

During COVID-19 specifically, many government employees were unable to get identity proofed and smart cards issued in person. Edge cases also include non PIV/CAC eligible employees and contractors, authenticating to mobile devices and BYOAD (Bring Your Own Approved Devices), air-gapped/isolated networks, cloud services, and even military scenarios where relying on a PIV or CAC may inadvertently reveal identities. In 2016, Terry Halvorsen, then the DoD CIO, noted, "It's really hard to issue a CAC card when people are dropping mortar shells on you and you need to get into your systems."[1]

In 2019, OMB Memo 19-17 recognized that "identity management has become even more critical to the Federal Government," reflected with the creation of the Federal Government's Identity, Credential, and Access Management (ICAM) policy.[2] The memo aimed to "modernize" identity management in line with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63. This memo gave Federal agencies, both military and civilian, the opportunity to use other strong authentication as alternatives to PIV and CAC.

> "We will not eliminate public-key infrastructure. We will not eliminate high security. But frankly, CAC cards are not agile enough to do what we want.
>
> **–Terry Halvorsen, former CIO of DoD[3]**

Prior to this memo, special exemptions were given to accommodate edge cases where PIV and CAC were not going to work. At the time, most edge cases adopted the most simple authentication method: username and password. OMB Memo 19-17 recognized that these edge cases were growing and it was necessary to find a stronger authentication alternative to PIV and CAC than passwords. As such, NIST and other agencies are working to incorporate newer technologies into their digital identity guidelines.

51%

of federal data in the cloud is sensitive[5]

80%

of data compromised in public administration is credentials[6]

60%

of malware in the public sector is ransomware[7]

The cyber attack landscape

The cyber attack landscape continues to shift and accelerate, triggering updated and new government regulations and mandates. New and varied threat actors and vectors are targeting privileged users such as key government officials, and security, network and database admins. With the majority of security breaches involving misuse of credentials, and the potential for credential escalation or lateral movement from third-party credentials, sensitive information and systems are at risk, including defense plans, budgets, strategic planning docs, critical infrastructure, and citizen PII/PHI.

Colonial Pipeline attack triggers new regulation

Colonial Pipeline, one of the largest fuel pipeline operators in the US, was recently a target of a cyber attack by DarkSide, an Eastern European-based ransomware group.[8] Colonial Pipeline operations were disrupted by the May 7 attack, prompting CEO Joseph Blount to agree to the $4.4 million ransom.[9]

The Department of Homeland Security made rapid moves to enact cybersecurity regulations for the pipeline industry. The Transportation Security Administration (TSA) announced a new Security Directive that will require pipeline owners to appoint a Cybsersecurity Coordinator 24 hours a day, seven days a week, and to report confirmed or potential cybersecurity incidents. The directive also requires pipeline owners to identify and report on gaps in cyber preparedness within 30 days, effective May 27, 2021.[10] The Directive references resources that specifically mention the NIST framework, which itself lays out minimum requirements for authentication.[11]

The TSA is already considering further directives to explicitly detail the cybersecurity requirements for pipeline operators.

SolarWinds attack underscores supply chain risk

In 2020, a major threat actor backed by the Russian government penetrated at least nine Federal agencies as well as thousands of organizations—one of the worst cyber-espionage incidents on record.[12] Most significantly, the cyber attack created a backdoor in SolarWinds' Orion Software, installing malware to spy on over 18,000 customers of the product, including Federal agencies such as the DHS, DOJ, and DoD.[13]

The attack went undetected for months, in part due to the supply chain attack method used to move laterally between systems and gain additional privileges. Of note is the supposed misuse of Identity and Access Management (IAM) systems like single sign on, network logon systems, SAML/OAuth/OIDC federation systems, and the like. With SolarWinds, and almost every breach, you'll find credentials, keys, and secrets abused anywhere they can be. Once the attacker has initial access to the victim's environment, they diversify their access to help maintain a persistent foothold.

As a result of this attack, the White House released Executive Order 14028 followed by the Office of Management and Budget (OMB) Memo 22-09 calling for the move to Zero Trust principles and phishing-resistant multi-factor authentication (MFA).

> “Cybersecurity is a top priority for this administration, and recent events, such as the SolarWinds cyber incident, have shown that adversaries continue to target Federal systems.
>
> **–President Biden FY2022 Budget[14]**

> U.S. government agencies may be slow to adopt and are still relying on PIV and CAC standards, physical readers, and smart cards, but the pandemic and the move to remote work raised a sense of urgency in a lot of government agencies.
>
> **– John Fontana, Program Manager for Standards, Yubico**

Modern alternate authentication with the YubiKey

The YubiKey is a FIPS 140-2 validated hardware security key manufactured by Yubico, a global authentication leader that meets Authentication Assurance Level 3 requirements (AAL3) of NIST SP800-63B. YubiKeys support PIV and CAC, and modern strong credentialing without peripheral devices, and provide highest-assurance, phishing-resistant two-factor, multi-factor, and modern passwordless authentication at scale, helping federal agencies be compliant to MFA requirements across various regulations, certifications, executive orders, and frameworks.

The DoD Office of the CIO (OCIO) Memo, 20 August 2018 approved YubiKeys as one of only two commercial alternatives to the PIV/CAC, for use as a MFA token for DoD unclassified and secret classified information systems and applications. And the DoD OCIO Memo on Mobile PKI Credentials, 19 December 2019, approved YubiKeys as a mobile authenticator.

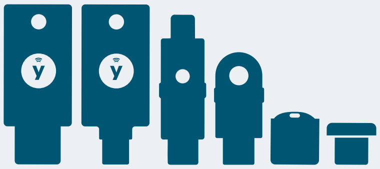
YubiKeys also support Defense Information Systems Agency (DISA) Purebred derived credentials for secure credentialing of BYOD/BYOAD and mobile devices, and are available on Department of Homeland Security, Continuous Diagnostics and Mitigation (CDM) as a preferred authenticator to meet OMB Memo M-19-17.

YubiKeys are:

- FIPS 140-2 validated, Overall Level 1 Certificate #3907) and Level 2 Certificate #3914), Physical Security Level 3
- Validated to NIST SP 800-63-3 Authenticator Assurance Level (AAL) 3 requirements
- Compliant with DFARS / NIST SP 800-171 / Homeland Security Presidential Directive 12 (HSPD 12)
- DOD Cybersecurity Maturity Model Certification (CMMC) Level III compliant
- Approved for use in DOD Non-Classified and Secret Classified environments
- FIDO2 / WebAuthn / FIDO U2F compliant
- Meet Zero Trust security phishing-resistant MFA guidelines in White House Executive Order 14028 and OMB M-22-09

To authenticate, users simply tap/touch their security key to any kind of device, including mobile phones and tablets. YubiKeys don't require batteries, have no breakable screens, don't need a cellular connection, and are water-resistant, dust-proof and crush-proof – highly durable for even the most harsh military environments.

The solution



The YubiKey 5 FIPS Series

From left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS, and YubiKey 5C Nano FIPS.

FIPS 140-2 Validation

National Security Agency[15]

How the YubiKey supports PIV/CAC requirements and a Zero Trust strategy

The YubiKey is the only DoD OCIO-approved alternate hardware authenticator to a CAC that supports multiple authentication protocols and meets DoD's cybersecurity requirements.

The YubiKey is a hardware security key that only does secure cryptographic authentication. It is not a storage device like a flash drive. It comes in a variety of different form factors with some fitting on a keyring, offering USB, NFC, and lightning connectors. Each YubiKey includes a secure built-in chip that accommodates derived PIV/CAC requirements, eliminating device-based authentication.

A single security key can be used to securely authenticate users to applications and services across multiple government issued or personal devices such as laptops, desktops, tablets, and mobile phones. In fact, the name "YubiKey" is a play on the word "ubiquitous" because it is a single, ubiquitous device to provide security for any device that connects to the Internet. The YubiKey supports multiple authentication protocols on a single device, including Smart Card (PIV), OTP, OpenPGP, and the latest authentication standards such as FIDO2/WebAuthn and FIDO U2F, supporting both legacy and modern infrastructures. In fact, Yubico is a founding member of the FIDO Alliance and co-authored FIDO's Universal Second Factor (U2F) authentication.

"The YubiKey is, in fact, a linchpin of the Zero Trust concept," notes Jeff Phillips, VP Public Sector, Yubico. "It is the token that asserts your identity and that provides high assurance that you are who you say you are."

With the YubiKey as a portable root of trust, users can establish trust on a new device and have a portable credential to authenticate seamlessly across multiple devices; and YubiKeys don't need network connectivity, cellular connections, or batteries to work, and are manufactured securely in the U.S. using stringent processes and a secure supply chain for trustworthy components. They also ensure that air-gapped networks stay secured against breaches by providing a highest-assurance MFA solution that works well in network-isolated and mobile-restricted environments. With a YubiKey, users can be authenticated without transfer of information across multiple security domains such as unclassified and classified.

> "YubiKey does much of what a CAC does and lets the DoD take advantage of modern authentication for cloud computing and implement Zero Trust philosophies.
>
> **–Jeff Phillips, VP Public Sector, Yubico**

Smart Card/PIV

Out-of-the-box native integration for the Microsoft environment using Smart Card/PIV functionality based on the NIST SP 800-73 specification.

FIDO2 & FIDO U2F

Strong two-factor, multi-factor and passwordless authentication public key crypto to protect against phishing, session hijacking, man-in-the-middle, and malware attacks.

One time passcodes

Integrate Yubico OTP natively with the free YubiCloud authentication service or program unique TOTP or HOTP secrets.

Federal compliance standards

How the YubiKey addresses regulatory requirements

Government employees and contractors are likely to be targeted by hackers and nation-states, which makes the regulatory landscape for federal agencies complex. The YubiKey helps federal agencies comply with federal regulations with highest-assurance two-factor, multi-factor, and passwordless authentication.

Executive order on improving The Nation's cybersecurity (EO) and OMB M-22-09

The recent number of attacks on critical systems has triggered increased regulatory pressure from the Federal government. On May 12 2021, the Biden administration issued an Executive Order 14028 on "Improving the Nation's Cybersecurity."[16]

This new order required agencies and software vendors selling to the US government to adopt zero trust frameworks within 60 days, as well as multi-factor authentication and encryption for data at rest and in flight within 180 days.[17] The order also gave the Director of OMB and the heads of other agencies the directive to modernize FedRAMP in an aim to improve supply chain security.[18]

The Zero Trust emphasis in the order demonstrates the high priority status the government is placing on modernizing agencies' infrastructure. Strong, modern authenticators, like the YubiKey, will be essential to reaching Zero Trust goals while providing a low-friction and secure user experience.

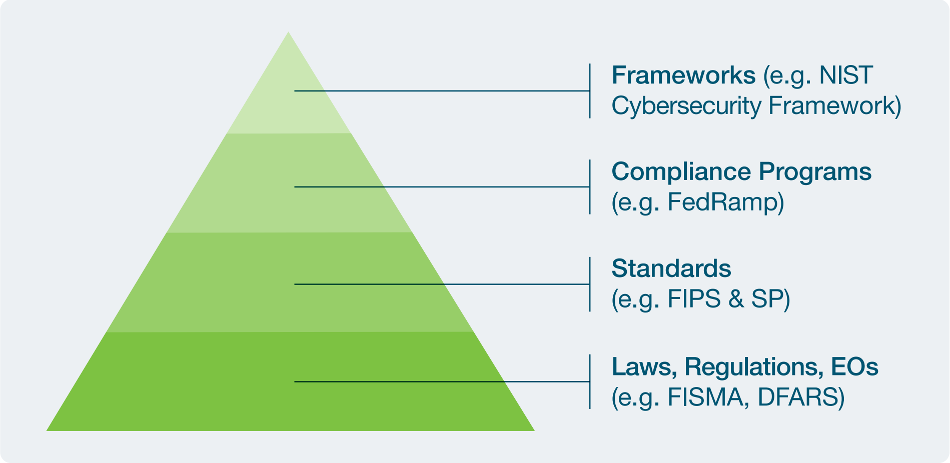
In response to EO 14028, the Office of Management and Budget (OMB) released a Federal Zero Trust strategy on January 26, 2022 M-22-09. The Memo called specifically for the use of phishing-resistant MFA throughout the federal government, as well as for access to citizen-facing digital services. While the federal government has standardized around smart cards paired with PKI — the PIV and CAC platforms, both of which are phishing-resistant — smart cards do not integrate easily with all devices and applications, especially those that are cloud-hosted or mobile-based. For this reason, the federal government is prioritizing extending phishing-resistant MFA to every device and application to address gaps that smart cards cannot fill. Here, M-22-09 highlights the ways that agencies should look to the FIDO2 standards to fill these gaps. Per the memo: FIDO2 is the overarching term for FIDO Alliance's set of specifications, of which Web Authentication (WebAuthn) is the most relevant. WebAuthn can be used in combination with a FIDO2 hardware security key for phishing-resistant MFA as the federal government moves authentication from the network level to the application level.

> "For routine self-service access by agency staff, contractors, and partners, agency systems must discontinue support for authentication methods that fail to resist phishing, including protocols that register phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications.
>
> **– Office of Management and Budget Memo M-22-09 Moving the U.S. wGovernment Toward Zero Trust Cybersecurity**

FISMA

The Federal Information Security Management Act (FISMA) is a law that requires every government agency and their third parties to implement information security plans. The National Institute of Standards and Technology (NIST) Cybersecurity Framework defines those plans for civilian federal agencies, further clarified and solidified by Executive Orders (EO), Special Publications (SP), and Federal Information Processing Standards (FIPS).

While FISMA is the law, compliance is a much more complex, interwoven, and continually changing goal post. We will walk you through the evolution of authentication standards and how YubiKey fits in.


Frameworks (e.g. NIST Cybersecurity Framework)
Compliance Programs (e.g. FedRamp)
Standards (e.g. FIPS & SP)
Laws, Regulations, EOs (e.g. FISMA, DFARS)

NIST

The NIST framework suggests strong authentication, including a multi-factor combination of something a user *owns*, *knows*, and *is*. Let's take a look at the specific guidelines for identity proofing and authentication in NIST.

Standard	NIST SP | FIPS	YubiKey capabilities	YubiKey certification level
Digital identity guidelines define authenticator assurance level (AAL)	SP 800-63	• Multiple-protocol support OTP, OATH, HOTP, U2F, PIV, Open PGP • 2FA and MFA options • Multi-factor cryptographic device • PIV/CAC module access controls • Hardware-based authenticator • Touch-button test of user presence	AAL3
Guidelines for PKI credentials used for PIV cards	SP 800-157	• Approved for use in DOD Non-Classified and Secret Classified Environments	
Guidelines for the protection of controlled unclassified information	SP 800-171	• Hardware-backed MFA access controls • PIV/CAC module access controls • YubiKey used as smart card • Centralized authorization policies to control access	
Security and privacy controls for information systems and organizations	SP 800-53	• PIV/CAC module access controls • YubiKey used as smart card • Centralized authorization policies to control access	
Interface specifications for PIV	SP 800-73	• PIV/CAC module access controls • YubiKey used as smart card • Sign / decrypt operations using a private key stored on the smart card	
Security requirements for cryptographic modules	FIPS 140-2	• Cryptographic module supports multiple protocols • YubiKey used as smart card • Touch-button test of user presence • Used as a smart card (PIV compatible) • Time or hash-based synchronous OTP • FIDO U2F • Made in the USA	• Overall Level 1 #3907 • Overall Level 2 #3914 • Physical Security Level 3 #3517

Meeting AAL3 with YubiKey PIV smart card functionality

The YubiKey offers an option for meeting SP 800-63 AAL3 leveraging the YubiKey as a Cryptographic Authenticator, with the authentication process occurring without the user acting as a bridge between the authenticator and endpoint.

Using the YubiKey as a Multi-Factor Cryptographic (MF Cryptographic) device–a PIV smart card–identifies and authenticates the user when logging into a site or service. The user authentication certificates stored on the PIV smart card function of the YubiKey would be validated by a Certificate Authority server controlling access to the service, and confirmed to originate from a trusted CA. If the user is inactive for 15 minutes, they must re-authenticate again.

The YubiKey PIV smart card function must have a PIN at least 6 characters in length, and contain a user authentication certificate issued by a FIPS 140-2 validated Certificate Authority linked to the service being authenticated to.

FedRAMP | YubiKey meets FedRAMP high

The Federal Risk and Authorization Management Program (FedRAMP) is a certification program for Cloud service providers to supply their solution to federal agencies.[19] FedRAMP follows the controls for data integrity laid out in NIST SP 800-53 with consideration for the difference of cloud systems and platforms. The FedRAMP Security Controls Baseline document defines strong authentication as resistant to replay attacks. It also states that any MFA requires devices separate from information systems gaining access, such as hardware tokens providing time-based or challenge-response authenticators. This is to reduce the likelihood of compromising authentication credentials stored on the system.

DFARS

The Defense Federal Acquisition Regulation Supplement (DFARS) defines standards required of contractors by the DoD. Under DFARS, DoD contractors and subcontractors must implement controls that are specific in the NIST SP 800-171. These requirements are set in place to protect controlled unclassified information in nonfederal information systems and organizations.

Hardware-backed MFA access controls

PIV/CAC module access controls

YubiKey used as smart card

Centralized authorization policies to control access

> “YubiKey approved for use as a multi-factor authentication (MFA) token for DoD unclassified and secret classified information systems and applications.
>
> **Department of Defense Memo, August 2018[20]**

OMB Memo 19-17

Authentication for contractors / citizens

OMB Memo 20-19

Authentication for new /remote workers

OMB Memo 22-09

Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

OMB memos on authentication

The Office of Management and Budget (OMB) reports directly to the President and provides guidance to Federal agencies on matters of privacy, including oversight of FISMA.

These OMB memos have laid the groundwork for federal agencies to seek out and adopt other strong authentication as alternatives to the PIV and CAC. While the 2019 memo (19-17) dealt mostly with the "edge" cases where PIV and CAC were not appropriate for modern needs,[21] OMB Memo 20-19 was a response to COVID-19 and the need to support new or remote employees.[22] OMB Memo 22-09 specifically calls for phishing-resistant MFA for internal employee access, and for cititzen-facing digital services.[23]

CMMC

Cybersecurity Maturity Model Certification (CMMC) combines various security standards (NIST, ISO, AIA and DFARS) into one standard for implementing cybersecurity for DoD contractors.[24] The new standard consists of 17 domains and five maturity levels. As the Federal space loves self-referential standards, Level 3 CMMC maturity also meets the requirements of NIST 800-171.

An estimated 70,000 DoD contractors were required to become CMMC certified in 2021, with certifications now also being rolled out new RFIs and RFPs.[24]

CMMC capability	YubiKey certification level	YubiKey capabilities
Access Control (AC) C001 Establish system access requirements	Level 1 AC.1.001	• PIV/CAC module access controls • YubiKey used as smart card • Centralized authorization policies to control access
AC C002 Control internal system access	Level 1 AC.1.002 Level 2 AC.2.007 | AC.2.008 Level 3 AC.3.018 | AC.3.019	• Hardware-backed access controls • PIV/CAC module access controls • YubiKey used as smart card • Centralized authorization policies to control access • Smart card policy can lock OS when YubiKey is removed

YubiKey meets CMMC Level III

The CMMC domain—Identification and Authentication (IA.3.083) in particular lists the requirement for MFA. The YubiKey meets this level III requirement by providing highest-assurance MFA through a number of protocols for local and network access. YubiKeys support multiple authentication protocols including smart card PIV/CAC, FIDO U2F, FIDO2 and OTP (HOTP, TOTP, YubiOTP). Specific to smart card PIV/CAC, a user is required to enter a PIN to unlock the secure element on the YubiKey as one factor, and the second factor is the possession of the private key securely stored on the YubiKey, which is used in the authentication workflow.

CMMC capability	YubiKey certification level	YubiKey capabilities
Asset Management (AM) C006 Manage asset inventory	Level 4 AM.4.226	• Can be managed as an asset in a CMS • Firmware information can be retrieved and stored
Audit and Accountability (AU) C009 Identify and protect audit information	Level 2 AU.3.049 | AU.3.050	• PIV/CAC module access controls • YubiKey used as smart card • Centralized authorization policies to control access
Identification and Authentication (IA) C015 Grant access to authenticated entities	Level 3 IA.3.083 | 1A.3.084	• MFA through multiple protocols - Something you know PIN (FIDO2, PIV, CAC) - Something you have (Private key stored on the YubiKey) • Support password / PIN for MFA (FIDO U2F, FIDO2 or OTP) • Replay attack resistant • Possession of the physical YubiKey • Time or hash-based synchronous OTP
Maintenance (MA) C021 Manage maintenance	Level 2 MA.2.113	• MFA through multiple protocols - Something you know (FIDO2, PIV, CAC) - Something you have (Private key stored on the YubiKey) • Support password / PIN for MFA (FIDO U2F, FIDO2 or OTP) • Replay attack resistant • Possession of the physical YubiKey • Time or hash-based synchronous OTP • Portable for third-party remote access
Media Protection (MP) C023 Protect and control media	Level 3 MP.3.123	• Cannot store media

Case study: New York Air National Guard

The New York Air National Guard often faces situations where personnel have legitimate needs to access DoD networks, but who are not eligible for a PIV credential or CAC. Retired military personnel, reservists, and members of the Army and Air Force National Guards often serve only part-time. In some cases, Reserve and Guard members have a CAC, but are not issued government-furnished equipment (GFE), so lack a CAC reader.

To meet the needs of National Guard personnel and others, the Defense Department has approved the use of three alternate multi-factor authentication (MFA) solutions when PKI is infeasible. And that's where Yubico's YubiKey fits in. It makes it possible for personal non-GFE devices in a bring-your-own approved-device (BYOAD) environment to be authenticated to DoD networks.

The New York Air National Guard began rolling out YubiKey in a test program in 2021 to let senior guard members authenticate to a New York State emergency management system, and progressively to DoD CAC credential-enabled sites with personnel, financial, and healthcare services. "We need to figure out ways for them to work securely without having to physically go to a base," notes Ali, Remote Piloted Aircraft Cyberspace Officer, New York Air National Guard, "We need a virtual base."

Aside from supporting the millions of retired members who continue to access medical and financial systems, YubiKey can serve as an alternate authenticator to CAC by supporting derived credentials (DISA Purebred).

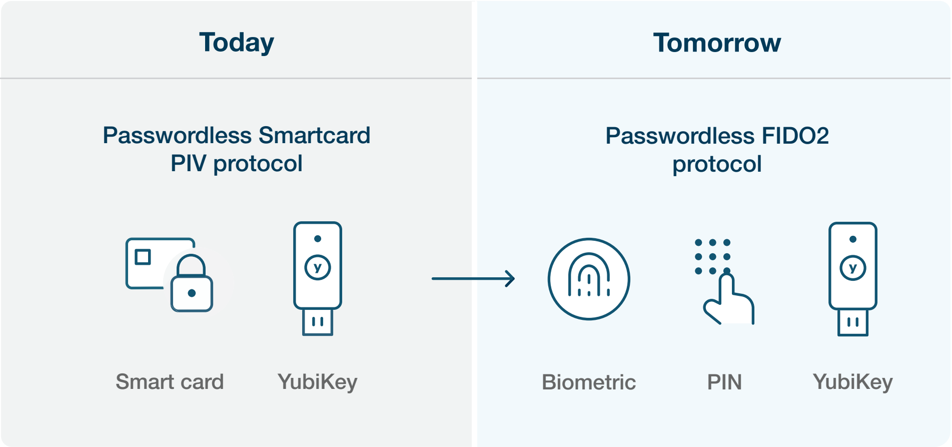
YubiKey has USB-A, USB-C, NFC and lightning form factors that don't require a specialized reader, and can be mailed directly to residential addresses across more than 30 countries.

> "The DoD's secure system with the CAC works well but moving forward we need better authentication, especially for people who are no longer actively serving in the military and lose the ability to use a CAC. With the YubiKey,they would be able to better secure their accounts with strong multi-factor authentication.
>
> **–Maj. Liaquat "Rocket" Ali, Remote Piloted Aircraft Cyberspace Officer at the New York Air National Guard**

YubiKeys offers the Federal Government a bridge to modern passwordless

While PIV and CAC offer a passwordless authentication experience, traditional smart cards may be somewhat complex for administrators to implement and manage, and involve having a good strategy in place to implement at scale.

With modern authentication protocols such as FIDO2/WebAuthn, government agencies can modernize their approach to passwordless using the YubiKey. The lowest hanging fruit for the federal government to modernize passwordless is in fact where PIV and CAC don't come into play—citizen-facing digital services. Relying on usernames and passwords for citizen-facing digital services creates security risks, leaving PII and sensitive financial information up for grabs. Government agencies can put an end to account takeovers now using the phishing-resistant YubiKey as a second factor on top of a password. The same YubiKey can be deployed as a passwordless security key when digital services are primed to support FIDO2.


Today
Tomorrow
Passwordless Smartcard PIV protocol
Passwordless FIDO2 protocol
Smart card
YubiKey
Biometric
PIN
YubiKey

Summary

As President Biden's Executive Order on Improving the Nation's Cybersecurity demonstrates, Federal agencies face "persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector."[26] The combination of major cyber attacks and a global pandemic has reshaped the risk landscape.

Recognizing this new reality, federal government agencies are working to fast track secure easy-to-use authentication to ensure that remote workers are securely connecting to government networks and that cloud-hosted services do not leave open doorways for cyber criminals to exploit.

The YubiKey is the only hardware authenticator to meet DoD contractor security requirements under DFARS and meets FIPS 140-2 certification requirements at the highest level of assurance (AAL3). Trust the YubiKey to secure your agency—and your supply chain.

YubiKey trust framework

Yubico, founded in 2007, was built on open standards like the Fast Identity Online (FIDO) standard in collaboration with industry-leading organizations and companies.

Supply chain

Yubico's hardware-backed authenticators rely on a global supply chain. We source our most sensitive component, the secure element, from a trusted and industry-leading vendor. Sensitive operations, like programming, take place at our facilities in the United States. We also built a robust chain of trust that starts with our vendor assurance program and ends with programmatic validation of components.

Product security

Security is embedded in our software and hardware development lifecycle at Yubico. Our engineering teams employ secure development practices that include security training, design reviews and threat modeling. Our dedicated security team provides automated static and dynamic analysis and performs a manual code review and penetration test for major releases. We also work with trusted and independent third parties to review the security of our products and services.

Data security & privacy

Although the amount of data we handle is minimal, Yubico leverages disk encryption, Pretty Good Privacy (PGP), Hardware Security Modules (HSMs), and a variety of platform security solutions offered by Google Cloud Platform (GCP), and Amazon Web Services (AWS).

Transport Layer Security (TLS) is used for encryption to protect information in transit. Where possible, TLS connections are mutually authenticated, to ensure that the identity of both the server and the client are verified prior to allowing access to that data. Multi-factor authentication with YubiKeys is used anywhere an employee can interact with systems handling customer data.

Sources

[1] Jason Miller, DoD plans to bring CAC cards to an end, (June 15, 2016), https://federalnewsnetwork.com/defense/2016/06/dod-plans-bring-cac-cards-end/

[2] Russell T. Vought, M-19-17, (May 21, 2019), https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

[3] Jason Miller, DoD plans to bring CAC cards to an end, (June 15, 2016), https://federalnewsnetwork.com/defense/2016/06/dod-plans-bring-cac-cards-end/

[4] · THALES, 2020 Data Threat Report - Federal Edition, (Accessed June 1, 2021), https://cpl.thalesgroup.com/federal-data-threat-report

[5] · Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021), https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

[6] Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021), https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

[7] Charlie Osborne, DarkSide explained: The ransomware group responsible for Colonial Pipeline attack, (May 14, 2021), https://www.zdnet.com/article/darkside-the-ransomware-group-responsible-for-colonial-pipeline-cyberattack-explained/

[8] Collin Eaton and Dustin Volz, Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom, (May 19, 2021), https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

[9] DHS, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators, (May 27, 2021), https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators

[10] CISA, Cyber Resource Hub, (Accessed May 27, 2021), https://www.cisa.gov/cyber-resource-hub

[11] Jon Porter, White House now says 100 companies hit by SolarWinds hack, but more may be impacted, (February 18, 2021), https://www.theverge.com/2021/2/18/22288961/solarwinds-hack-100-companies-9-federal-agencies

[12] Isabella Jibilian & Katie Canales, The US is readying sanctions against Russia over the SolarWinds cyber attack, (April 15, 2021), https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

[13] White House, FY2022 budget, (Accessed June 1, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/05/ap_12_it_fy22.pdf

[14] NSA, Selecting Secure Multi-factor Authentication Solutions, October 2020, https://media.defense.gov/2020/Sep/22/2002502665/-1/-1/0/Multifactor_Authentication_Solutions_UOO17091520_V1.1%20-%20Copy.PDF

[15] The White House, Executive order on Improving the Nation's Cybersecurity, (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[16] David Treece, Quick Take: Executive Order on Improving the Nation's Cybersecurity, (May 13, 2021), https://www.yubico.com/blog/quick-take-executive-order-on-improving-the-nations-cybersecurity/

[17] The White House, Executive order on Improving the Nation's Cybersecurity, (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[18] FedRAMP, (Accessed May 31, 2021), https://www.fedramp.gov/

[19] Essye B. Miller, Interim Digital Authentication Guidelines for Unclassified and Secret Classified DoD Networks and Information Systems, (August 20, 2018), https://www.yubico.com/wp-content/uploads/2020/09/2018-08-20-DoD-PDCIO-Memo-Interim-Digital-Authentication-Guidelines-1-1.pdf

[20] Russell T. Vought, M-19-17, (May 21, 2019), https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

[21] Margaret M. Weichert, M-20-19, (March 22, 2020), https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-19.pdf

[22] The White House, M-22-09 (January 26, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[23] OUSD (A&S), CMMC Model and Assessment Guides, (December 10, 2020), https://www.acq.osd.mil/cmmc/draft.html

[24] Kim Koster, NIST 800-171 and CMMC Compliance for Government Contractors, (January 31, 2020), https://unanet.com/blog/nist-800-171-and-cmmc-compliance-for-government-contractors; Jerome Becquart, Ready for CMMC? Here's how you can get there, (December 30), https://federalnewsnetwork.com/commentary/2020/12/ready-for-cmmc-heres-how-you-can-get-there

[25] The White House, Executive order on Improving the Nation's Cybersecurity, (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

yubico

About Yubico

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts.

The company's core invention, the YubiKey, delivers strong hardware protection, with a simple touch, across any number of IT systems and online services. The YubiHSM, Yubico's ultra-portable hardware security module, protects sensitive data stored in servers.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed and loved by 9 of the top 10 internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.