yubico

WHITE PAPER

Modernizing authentication across the Department of Defense with phishing-resistant MFA

Meet NSM-8 requirements and support modern use cases with a DOD-approved solution that compliments the CAC



Contents

Authentication challenges across the Department of Defense 2

The cyberattack landscape adds pressure to protect credentials 4

New regulations mandate phishing-resistant MFA 5

YubiKey offers FIPS-validated phishing-resistant MFA 7

- YubiKey for CAC 9
- YubiKey for derived credentials 10
- A future-proof solution 10

Common authentication scenarios across the DOD 10

- Non CAC-eligible employees & contractors 11
- Coalition & mission partners 12
- Cloud-based software / productivity software 12
- Privileged access / high-security applications 13
- Workstation login 13
- Air-gapped networks & SCIFS 13
- Mobile devices 14
- Government teleworkers 14
- Tactical 15
- Multi-credential 15
- Supply chain and DIB 15
- Retired Personnel 15
- Legacy systems 16
- RSA SecureID replacement 17
- Authentication backup 17

Ready to get started? 17



Executive Summary

Using the Common Access Card (CAC) for authentication is not practical or possible for every Department of Defense (DOD) agency employee. Guidance such as the White House Executive Order 14028 and National Security Memorandum/ NSM-8 have put pressure on the DOD to deploy phishing-resistant authentication as part of a Zero Trust Architecture and created requirements to modernize authentication across the DOD.

There is a growing need for cost-effective, turnkey solutions to address the needs of today and future-proof against the authentication needs of tomorrow—including those currently under policy review by the DOD.

The phishing-resistant and FIPS 140-2 validated YubiKey from Yubico provides the highest levels of security needed to protect against modern day attacks along with the flexibility to secure even the most complex scenarios—from air-gapped networks to remote work and cloud services—all from a single key. With multi-protocol support for SmartCard, FIDO U2F, FIDO2, OTP and OpenPGP, the YubiKey supports both legacy and modern architectures with a single solution, and offers a future-proofed bridge to modern FIDO authentication standards. The YubiKey is a DOD-approved alternative authenticator that enables the DOD in its Mission to deploy strong cybersecurity to the War Fighter.

Authentication challenges across the Department of Defense

The critical need to address gaps in CAC authentication

> 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.[1]"
>
> **Terry Halvorsen** | former CIO of the DOD



Phishing-resistant multi-factor authentication (MFA) leveraging the Fast Identity Online (FIDO) standard is well-suited for DOD agencies to extend the benefits of PKI to a wider number of applications, domains and devices—all the areas where traditional CAC deployments have proven difficult or impossible.

The DOD is still primarily reliant on public key infrastructure (PKI) and the Common Access Card (CAC), the DOD's Personal Identity Verification (PIV) credential, for identification and access, leaving gaps for modern use cases where the CAC is not suitable. The CAC is issued to verified active duty personnel, Reserve and National Guard members, DOD civilian employees and eligible contractor personnel consistent with Homeland Security Presidential Directive 12 (HSPD 12),[2] the Department of Defense Instruction (DODI) 5200.46,[3] and the Federal Information Processing Standards (FIPS) 201-3.[4]

The CAC provides multi-factor authentication (MFA) to DOD facilities and information and communications technology (ICT) systems, meeting the needs for traditional perimeter-based and desktop authentication requirements. While CAC meets the highest assurance of MFA when using DOD PKI, there are a growing number of scenarios that have the same assurance requirements where CAC is not available or practical. These include access to cloud services, BYOAD (Bring Your Own Approved Devices), non-CAC eligible coalition and mission partner environments, air-gapped/isolated networks, and tactical scenarios where relying on a CAC may inadvertently reveal identities. This is particularly important to address in situations where the traditional fallback authentication method has been just a username and password.

The need for highest-assurance authentication is not new. 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."[5] These cases spurred several memos, such as "Interim Digital Authentication Guidelines for Unclassified and Secret Classified DOD Networks and Information Systems" in August 2018, that specifically address the need for DOD-approved MFA when either a system or application does not support authentication using DOD-approved PKI credentials, or a portion of the system or application's subscribers are unable to obtain DOD approved PKI credentials.[6] In civilian agencies, the Office of Management and Budget (OMB) issued two memos (M-19-17[7] and M-20-19[8]) that laid the groundwork for federal agencies to seek out and adopt other strong authentication alternative to the PIV.

As the need for mobility became more prevalent, the difficulties of using smart card technology with mobile devices drove the DOD to look for alternatives to CAC. The DOD needed a solution to provision credentials that was more practical for a mobile device and derived from a user's existing credentials. To meet this requirement, the Purebred solution was developed.

The Defense Information Systems Agency's (DISA) Purebred solution is a government-owned credentialing process for mobile devices and approved external authenticators, providing strong PKI authentication when CAC and PIV are not practical. While the number of derived credential use cases continues to expand, including the push during COVID-19 to create a Derived Alternate Credential (DAC) to support remote work, this has resulted in users having multiple derived credentials, one for each government-owned device.

As DOD agencies look to support the growing number of authentication requirements that CAC does not support, or that require derived credentials, they require a cost-effective, secure solution for highest-assurance authentication.

The cyberattack landscape adds pressure to protect credentials

200%+

increase of breaches on the DOD and DIB since 2015[9]

The DOD and the nation's defense industrial base (DIB) are under persistent cyberattack from threat actors, including nation-states, who leverage sophisticated technologies that often combine different techniques including malware, phishing and/or hacking to gain access to systems and information. The DOD faces a number of risks stemming from these attacks, including risk to military operations, inappropriate access to sensitive information, and threats to national security.

A Government Accountability Office report found that breaches on the DOD or the DIB have more than doubled since 2015.[9] The 2021 attack on five U.S. defense and technology firms by Chinese hackers leveraged stolen passwords[10] and the 2020 SolarWinds attack, one of the worst cyber-espionage incidents on record, was traced back to supply chain and privilege abuse.[11] In 2023, more than 100 documents containing classified military information were leaked to social media from a high security IT specialist in the Massachusetts Air National Guard, adding pressure to improve how the DOD manages identity controls.[12]

With almost every breach, you'll find credentials, keys, and secrets abused. These attacks are not compromising the CAC, instead they are compromising forms of legacy MFA (passwords, mobile-based authentication) that are being used in instances where CAC does not fulfill an authentication need. Accounts using MFA that are not based on phishing-resistant protocols are susceptible to having credentials stolen. Once a credential is compromised, all additional controls become moot.

The evolving attack landscape has triggered increased federal attention on modernizing the nation's cybersecurity defenses and strengthening supply chain security, with an increased focus on protecting credentials with phishing-resistant MFA such as the White House Executive Order (EO) 14028, "Improving the Nation's Cybersecurity,"[13] and the National Security Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems (NSM-8),[14] which sets forth an expectation that the DOD adopt cybersecurity requirements that "are equivalent or exceed" those set forth in the EO.



New regulations mandate phishing-resistant MFA

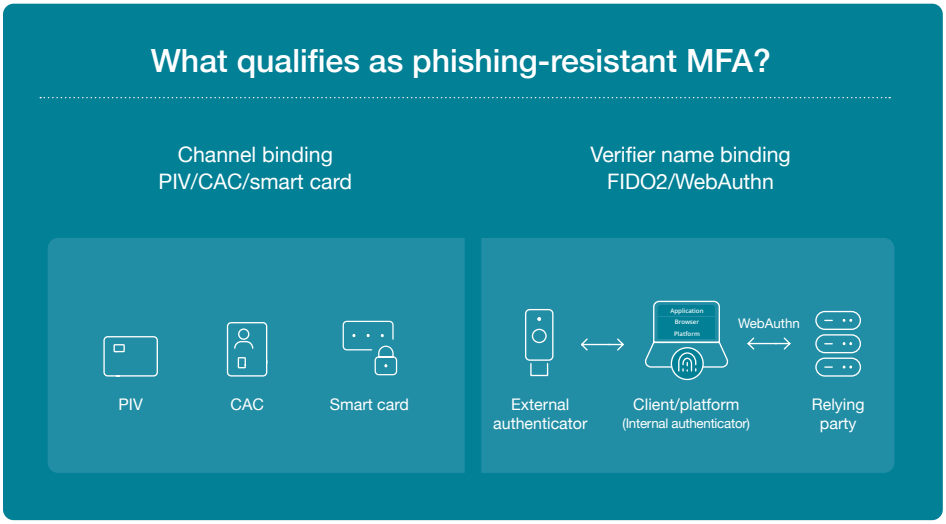
> Although DOD has determined PKI should be the primary authentication technology, not all DOD users have or can easily obtain PKI certificates and not all applications can use them."
>
> **DOD ICAM** | March 2020[15]

> The DOD must deploy alternate PKI and non-PKI authenticator technologies to support mobile devices and other form factors. The DOD must also remain committed to credential quality by driving the innovation and leveraging of new capabilities in hardware key storage, biometrics, and quantum resistant crypto-graphic algorithms. The DOD must ensure it is able to readily and securely interoperate with its subscriber base in a diverse environment and evolving threat."
>
> **DOD ICAM** | March 2020[16]

The White House has made cybersecurity a top priority for the federal government, both Civilian Agencies with EO 14028[17] and National Security Systems (NSS) with NSM-8.[18] NSM-8 requires that agencies implement standards that are "equivalent to or exceed cybersecurity requirements for Federal Information Systems set forth within Executive Order 14028," requiring DOD agencies to be familiar with EO 14028 and associated memoranda requirements to advance toward Zero Trust Architecture and adopt phishing-resistant MFA.[19]

The DOD Identity, Credential, and Access Management (ICAM) Strategy[20] outlines the need to expand credentials and authenticators to support all types of users and all environments in line with risk-based guidelines and the DOD's revised Zero Trust Reference Architecture.[21] As the ICAM states, the DOD remains committed to credential quality, a quality that can be fulfilled by phishing-resistant MFA.

The draft National Institute of Standards and Technology (NIST) Digital Identity Guidelines (SP 800-63-4), designed to guide agencies with digital identity assurance and authentication, outlines the technical requirements for phishing-resistant authentication, recognizing two methods: channel binding and verifier name binding.



Channel binding relies on a protected channel commonly used on internal network, e.g. PIV/CAC smart cards. Verifier name binding relies on a domain (URL/website) for the verification of a registered device, with the assumption that the domain you registered with is in control of the domain you want to do business with, e.g. WebAuthn/FIDO2–now commonly referred to as a passkey.

NIST SP 800-63-4

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63 *Digital Identity Guidelines* is currently in public review for a revision that would update all four volumes of the standard.[22] The draft SP 800-63-4 guidelines retain the basic organizational structure and assurance level models, but introduce several changes which are designed to reflect the current and emerging attack landscape, including a re-working of authentication assurance levels (AALs) that are also referenced by the DOD.

Under this new model, AAL3 provides very high confidence that the claimant controls one or more authenticators bound to the subscriber account—in plain language, that the person authenticating can, by proof of possession, prove they are who they are claiming to be:

AAL1	AAL2	AAL3
Single-factor authentication Verifier must be FIPS 140 validated	Two-step or two-factor authentication Approved cryptographic techniques Phishing-resistant authenticator encouraged, not required Authenticator must be FIPS 140 validated	Hardware-based authenticator Phishing-resistant authenticator required (channel or verifier name binding) Must be FIPS 140 validated
		PIV/Smart card  FIDO 



The YubiKey is:

FIPS 140-2 validated to AAL 3 requirements

Overall Level 1 (Certificate #3907) and Level 2 (Certificate #3914), Physical Security Level 3

CMMC Level III compliant

DFARS / NIST SP 800-171 compliant

Manufactured securely in the US

The YubiKey offers FIPS-validated phishing-resistant MFA

Yubico offers the phishing-resistant FIPS 140-2 validated YubiKey, a DOD-approved[23] hardware security key that offers highest-assurance multi-factor and passwordless authentication in accordance with Homeland Security Presidential Directive 12 (HSPD 12)[24]. The YubiKey is approved for use as an MFA authenticator for DOD unclassified and secret classified information systems.[25] A single YubiKey can provide both PKI and FIDO2 (WebAuthn) phishing-resistant authentication, housing multiple of each credential.

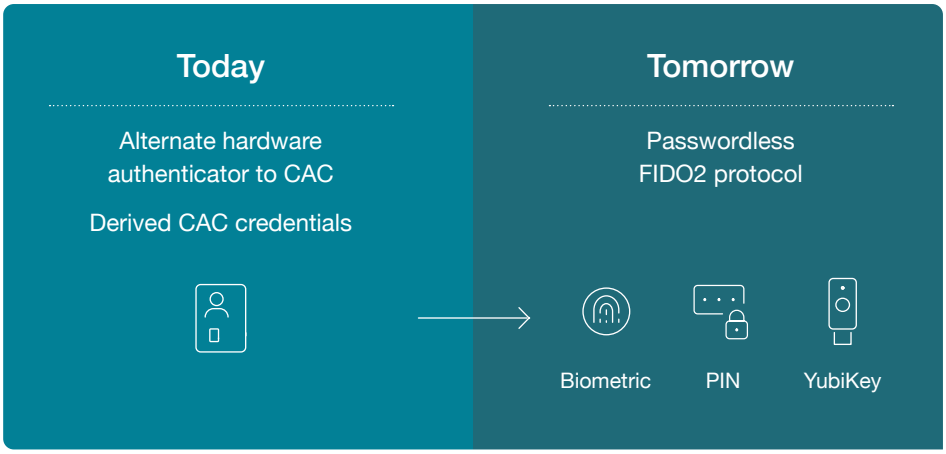
By meeting DOD mobile PKI credential storage requirements,[26] a YubiKey can hold either DOD PKI credentials, issued by Purebred, or an organization can host their own PKI to provide credentials to non-CAC eligible personnel, or for air-gapped and other accepted networks, e.g. mission partner environments. In scenarios where resources are cloud-based, or a FIDO2 capable ICAM is in use, DOD organizations can now leverage recent approval of FIDO2/WebAuthn and an alternative. FIDO2 can work extremely well to provide non-CAC eligible personnel, partners, and foreign nationals secure authentication. The YubiKey has already been successfully deployed, using PIV/PKI and FIDO2, across DOD and 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) and more.

Hardware security keys such as the YubiKey are an ideal option for strong phishing-resistant MFA because they don't require additional hardware or software, external power or batteries, or a network connection—a single key secures 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.

As a portable hardware root of trust, the YubiKey is proven to reduce risk against phishing attacks and account takeovers by 99.9%[27] and offer a seamless path to meet new zero trust and MFA requirements. As a result, 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

The YubiKey is a DOD-approved phishing-resistant authenticator that can meet use cases where PIV/CAC are not available nor practical, by leveraging derived PIV/CAC credentials.



> “I have this notion of—this little mantra of—I want to kill the CAC as the primary authentication mechanism for the department.”
>
> **Air Force Lt. Gen. Robert Skinner** | DISA Director and Commander | Joint Forces Headquarters, DOD Information Networks[29]

YubiKey for CAC

HSPD-12 identifies four criteria for secure and reliable forms of identification, including but not limited to, a PKI-based smart card credential such as the CAC. Alternatively, agencies can use one-time PIN mobile applications for phishing-resistant non-PKI authenticators, such as FIDO2, supported on the YubiKey.

The YubiKey is one of only three DOD CIO government-approved alternate authenticators that meet the DOD’s rigorous cybersecurity requirements for non-classified and secret classified environments.[28]

A single YubiKey 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. Unlike managing multiple certificates across mobile devices and CAC cards, a YubiKey with one certificate can be used as a portable root of trust across multiple devices including mobile and BYOD/BYOAD.

The YubiKey has out-of-the-box native integration for the Microsoft environment including Azure Active Directory (AD) and Microsoft 365. Leveraging certificate-based authentication (CBA) or FIDO2/WebAuthn, a user can leverage their YubiKey as a smart card to access applications and desktops protected with Azure AD or AD Federation Services (FS).





YubiKey for derived credentials

The YubiKey includes a secure built-in chip that accommodates DISA Purebred derived CAC requirements for secure credentialing. While derived credentials stored on a device are a security risk, credentials stored on YubiKeys cannot be extracted or tampered with. The YubiKey becomes a strong hardware-based identity token that is tied to a master identity record in Azure AD, which ties into CBA.

As a portable root of trust, the YubiKey can support multiple devices, services or secure offices, reducing hardware costs and solving use cases around BYOAD, cloud services, remote work and even isolated/secure networks.

The YubiKey looks and acts like a CAC for both the system and the user, making it a light IT project with minimal end user training requirements. As a side benefit, if a mobile or computer device is lost or stolen, or a new device issued, the YubiKey can be used as an easy method to establish or re-establish trust with online accounts and re-register the internal authenticator on a new device.

A future-proof solution

FIDO2 is an open authentication standard based on public key cryptography. FIDO2 enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments. The FIDO2 specifications are the World Wide Web Consortium’s (W3C) Web Authentication (WebAuthn) specification and FIDO Alliance’s corresponding Client-to-Authenticator Protocol (CTAP). The YubiKey is a multi-protocol solution that can support PIV/CAC as well as FIDO2/WebAuthn, helping DOD agencies transition to newer FIDO-based and passwordless authentication without the high overhead or usability challenges associated with CAC.

Common authentication scenarios across the DOD

While CAC remains the primary means of identification and authentication to federal systems, facilities and secured areas, the shift to managing identity supports a more comprehensive set of use cases. With the YubiKey, agencies can deploy highest-assurance, phishing-resistant MFA to support a variety of authentication scenarios across the DOD, including:

- Non CAC-eligible employees & contractors
- Coalition & mission partners
- Cloud-based software
- Privileged access
- Workstation login
- Air-gapped networks & SCIFs
- Mobile devices
- Government teleworkers
- Tactical
- Multi-credential
- Supply chain and DIB
- Retired Personnel
- Legacy systems
- RSA SecureID replacement
- Authentication backup



Phishing-resistant authentication options

Access points		Offers WebAuthn support	Offers CAC support	YubiKey (WebAuthn/ FIDO and/or CAC)
On premise (active directory)	Windows 10+ Login	✓ / 3rd party	✓	✓
	Earlier versions of Windows Login	3rd party	✓	✓
	macOS Login on a Windows domain	3rd party	✓	✓
	VPN Access	Varies	✓	✓
	Secure Proxy Gateways	✓	Varies	✓
Cloud platforms	Microsoft Azure	✓	Preview / Federation	✓
	Amazon Web Services (AWS)	✓	✓ / Federation	✓
	Google Cloud	✓	Federation	✓
	Oracle Cloud	✓	Federation	✓
	IBM Cloud	✓	Federation	✓
IDPs	Okta	✓	✓	✓
	Ping	✓	✓	✓
	DUO	✓	N/A	✓
	ForgeRock	✓	✓	✓

Non CAC-eligible employees & contractors

There are personnel without credentials who have a legitimate need to access DOD systems but either lack a CAC or require an alternate token that works without additional smart card hardware or software. This group can include Reservists and members of the Army and Air Force National Guards who may only serve part-time or who may not be issued government-furnished equipment (GFE) or short-term contract workers not eligible for CAC.

To meet the needs of National Guard personnel and others, the DOD approved the use of three alternate MFA solutions when PKI is infeasible—including the YubiKey, a FIPS 140-2 validated alternative to the PIV or CAC that allows non-CAC personnel or personal non-GFE devices in a BYOAD environment to securely authenticate to DOD networks.

Many commonly used access points such as VPNs, IdPs (Identity Provider), cloud platforms, desktop login, and web access offer support today either for WebAuthn, PIV/ CAC, or both. The chart above shows an example of common access points that support phishing-resistant MFA using either WebAuthn/FIDO2, or PIV/CAC, as well as YubiKey support.

Retired Personnel

Retirees historically only get plastic cards with barcodes to enter military installations or use as identification for military benefits such as healthcare, billeting and recreation services, but these personnel and their families lack credentials to support access to online systems for healthcare, pension, survivor benefits or other services.

The YubiKey is a phishing-resistant MFA alternative to using username and password for retirees to access personnel, financial and healthcare services.

CASE STUDY

AIR NATIONAL GUARD

New York Air National Guard leverages the YubiKey for high-assurance network authentication

The New York Air National Guard (NY ANG) often faces situations where personnel have legitimate needs to access DOD networks, but who are not eligible for a CAC. The New York Air National Guard began rolling out YubiKeys 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. The YubiKey was also critical to supporting the 30% of the workforce who want to continue to work remotely.



> “I think sometimes we only focus on the 650,000 people we have currently in the total force, and forget about the millions of people that are already retired and their family members that need access to secure medical information, paychecks, and digital transactions. 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 | New York Air National Guard

Coalition & mission partners

Coalition and Five-Eyes (FVEY) mission partners use PKI credentials to authenticate to DOD systems, but are not CAC-eligible. YubiKey is a solution that is easily onboarded and offboarded to support access to the data needed to conduct a mission, supporting non-DOD PKI credentials for access to DOD systems as well as FIDO2 credentials for access to cloud-based systems.

Cloud-based software / productivity software

For select DOD groups, YubiKey can authenticate to existing Identity and Access Management (IAM) and SSO solutions (Microsoft, Google, Okta, Duo, Ping) to provide federated access to authorized cloud services, providing additional AAL3 capabilities to traditional IdP solutions in accordance with the DOD cloud computing security requirements.[30]

Microsoft users, either Azure, Azure Active Directory (Azure AD), or Microsoft 365, can take advantage of native support for the YubiKey. With Azure AD Cloud Native CBA and YubiKeys, agencies can leverage the YubiKey to access Azure directly without the need for a third-party IAM product or the need to build certificate authentication for the cloud.

Privileged access / high-security applications

Privileged access to classified, secret and personal information places key government officials and security, network and database admins at risk of compromise. Any unauthorized access to ICT systems or data, including defense plans, budgets, and strategic planning docs, can place missions and national security at risk and compromise the security of coalition and FVEY partners.

YubiKeys bridge legacy MFA to modern protocols such as FIDO2/WebAuthn. The YubiKey's hardware design enables the authentication secret to be stored on a separate secure chip built into the YubiKey, so it cannot be copied or stolen, offering the highest security for authenticating privileged users.

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.

Workstation login

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

Air-gapped networks & SCIFs

Air gap networks are closed off from the outside, making it difficult to authenticate users using data sent over a network. Many air-gapped systems still use a username and password or a combination of passwords and a digital identity.

YubiKeys don't need any network connectivity, cellular connection or batteries to work. YubiKeys ensure that air gap networks stay secured against breaches by providing a multi-factor authentication solution that works well in isolated network and mobile restricted environments. YubiKeys are compatible with Cross Domain Solution (CDS) and Multi-Level Security (MLS), and users can be authenticated without transfer of information.

Mobile devices

bring your own device (BYOD) | bring your own approved device (BYOAD) | approved mobile device (AMD) | government furnished equipment (GFE)

The federal government has acknowledged that there are benefits associated with the use of non-GFEs, not the least of which is a reduction in cost, but that such benefits must be weighed against security risks. On August 10, 2022, a DOD memorandum outlined the minimum requirements for the use of non-government owned mobile devices, including the need for authentication with a CAC or DOD-approved authenticator such as the YubiKey.[31]

Whether BYOAD or GFE, PIV/CAC authentication is not practical, and storing credentials on that device further introduces security concerns if it is lost or stolen. With the YubiKey as a portable root of trust, government workers, contractors and DIB partners can authorize their personal mobile devices to access approved DOD services. Devices need to be authorized only a single time, with optional support for users to re-authenticate (step-up authentication) to specific government apps and services.

As the number of devices per employee increases, having a single portable external authenticator that can work across all computing devices helps make these transitions seamless.

Government teleworkers

To support government teleworkers, DOD agencies need to provision each worker with a CAC reader. If a reader is ever forgotten, end user productivity grinds to a halt. While password-based authentication may simplify remote access, relying on single-protocol authentication as part of federal ICAM strategies does not cater to zero trust security and phishing-resistant authentication requirements. Modern government use cases such as telework heighten the need for future-proofed identity strategies that are stronger than what is in use today.

The YubiKey works with leading IAM and IdP solution providers to enable remote and hybrid employees to work without the hassle or security risks associated with legacy authentication solutions such as SMS and mobile authenticators. Further, in cases where VPN and Identity-Aware Proxies (IAP) solutions are still in use (as agencies shift to Zero Trust), the YubiKey provides a strong hardware-backed AAL3 token to help support what's in place today as a bridge to more modern architecture.

In cases where remote and hybrid workers are sent GFE devices, the YubiKey can be used as a portable root of trust to ensure the device hasn't been compromised en route.

Tactical

The CAC is not purpose-built for field work or the front line. In tactical situations, the YubiKey can provide a need for a military-grade authentication solution that does not rely on cellular connectivity or battery life and is waterproof, crush-resistant and dustproof. For scenarios where an identity-based CAC could compromise user identity and security, the YubiKey can be used as a portable root of trust.

Multi-credential

The YubiKey can be used to store credentials for more than one government network, supporting multi-credential requirements such as National Guards or Reservists or coalition network partners who have access to different government networks including DOD networks as well as State and Local services. Current policies could limit provisioning of more than one DOD-issued PIV/CAC credentials on a single external authenticator.

Supply chain and DIB

The Cybersecurity Maturity Model Certification (CMMC) was rolled out by the DOD to set minimum standards for any federal contract across the Defense Industrial Base (DIB) supply chain, including software used by the DOD.

In line with Executive Order 13873 on Securing the Information and Communications Technology and Services Supply Chain[32], as well as the directive to protect the integrity of the software supply chain in EO 14028, the DOD has been tasked with improving the chain of custody in the software supply chain. To this end, the YubiKey can be used to help ensure code and commits are cryptographically signed. Learn more in Protecting the supply chain with highest-assurance security.

For organizations looking to compete on DOD RFIs and RFPs, the YubiKey can help achieve CMMC Level III compliance.



Read the white paper → here.

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 and WebAuthn. YubiKeys act as a bridge solution, supporting smart card (PIV/CAC) as well as more modern authentication standards such as FIDO U2F, FIDO2/WebAuthn, OpenPGP, and OTP.

The YubiKey's multi-protocol functionality helps address a wide range of authentication needs including computer login and remote access, digital signatures for code signing, key escrow for email encryption, or privilege access for older operating environments.

RSA SecureID replacement

The use of one-time passcodes has been deprecated as part of EO 14028, and therefore NSM-8, with the requirement for agencies to adopt more secure phishing-resistant authentication. As organizations bridge to this requirement, the first step can be to switch to the Yubico Authenticator as a second factor in an authentication process. The Yubico Authenticator app allows you to store your credentials on a YubiKey and not on your mobile phone, so that your secrets cannot be compromised. The Authenticator App requires a YubiKey 5 Series to generate OTP codes.

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. This is particularly problematic when CAC needs to be re-issued in person.

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.

Ready to get started?

DOD agencies can leverage security as a service through Yubico solutions such as YubiEnterprise Services. 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 the insight from over 150 U.S. government implementations to date.

Plan

Ensure readiness clarify use cases and user populations.

Validate

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

Integrate

Ensure key apps and services are YubiKey-ready

Launch

Distribute keys to users with turnkey delivery services or channel partners

Adopt

Drive adoption with best practice training and support

Measure

Report on security and business value impact



Get YubiKeys as a service with YubiEnterprise Subscription

With YubiEnterprise Subscription, agencies receive a service-based and affordable model for purchasing YubiKeys with benefits such as predictable spending, upgrades to the latest offerings, customer support and more. There are distinct advantages versus a one-time perpetual YubiKey purchase, particularly for large enterprise deployments:

YubiEnterprise Subscription highlights

Lower cost to entry

Initial payments are significantly reduced in procuring YubiKeys, helping organizations maintain healthy balance sheets.

Total flexibility

Order and switch form factors within the YubiKey 5 FIPS Series over time.

Priority Technical Support

Easy access to Yubico security experts with 24x7x365 priority support.

Customer Success Manager

Customer advocate and dedicated point of contact post sale to help you in your journey.

Replacement YubiKeys

Upon subscription renewal each year, 25% of the total subscription can be replaced at no additional cost, covering lost keys, employee attrition, desire for new form factors (USB-C form factor vs. USB-A form factor), upgrading to FIPS 140-3 compliant YubiKeys, etc.

Professional Services

Accelerate your rollout; Subscription includes eligibility to apply 5% of purchase towards Professional Services, up to $75K maximum. For example, a 3-year subscription totaling $1M would entitle $50K credit to be applied to Yubico Professional Services offerings.

25% discount on any backup YubiKeys

Backup keys are highly recommended - some online services that allow security keys for multi-factor authentication require two keys during registration (for example: iCloud).



Read the solution brief → here.



Read the solution brief → here.

Leverage expert consulting services for a successful YubiKey deployment

Yubico's Professional Services team is here to help you with a successful implementation. Yubico offers a wide variety of advisory services in support of your YubiKey implementation and deployment, including best practices workshops, technical implementation packages, ondemand consulting resources and custom engagements. Our Professional Services team is comprised of trained and accredited security professionals with experience gained from hundreds of customer implementations across a wide range of industries and the government sector. From standard implementations to complex enterprise rollouts, Professional Services has the skills and expertise to help guide you through all facets of your YubiKey implementation and deployment.

Contact us
yubi.co/contact

Learn more
yubi.co/ps yubi.co/yes

Sources

[1] Jason Miller, DOD plans to bring CAC cards to an end, (June 15, 2016)

[2] Homeland Security, Homeland Security Presidential Directive 12, (August 27, 2004)

[3] Department of Defense, Number 5200.46, (November 2, 2020)

[4] NIST, FIPS PUB 201-3, (January 2022)

[5] Jason Miller, DOD plans to bring CAC cards to an end, (June 15, 2016)

[6] DOD, Interim Digital Authentication Guidelines for Unclassified and Secret Classified DOD Networks and Information Systems, (August 20, 2018)

[7] Russell T. Vought, M-19-17, (May 21, 2019)

[8] Margaret M. Weichert, M-20-19, (March 22, 2020)

[9] GAO, DOD Cybersecurity, (November 2022)

[10] Robert Falcone, et al, Targeted Attack Campaign Against ManageEngine ADSelfService Plus Delivers Godzilla Webshells, NGLite Trojan and KdcSponge Stealer, (November 7, 2021)

[11] Isabella Jibilian & Katie Canales, The US is readying sanctions against Russia over the SolarWinds cyber attack, (April 15, 2021)

[12] Lara Seligman, 'I'm sick to my stomach': Pentagon officials shocked by intel leaks, (April 10, 2023)

[13] White House, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, (January 26, 2022)

[14] White House, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems/NSM-8, (January 19, 2022)

[15] DOD, Identity, Credential, and access Management (ICAM) Strategy, (March 30, 2020)

[16] DOD, Identity, Credential, and access Management (ICAM) Strategy, (March 30, 2020)

[17] White House, Executive order on Improving the Nation's Cybersecurity, (May 12, 2021)

[18] White House, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems/NSM-8, (January 19, 2022)

[19] Shalanda D. Young, Office of Management and Budget, M-22-09, (January 26, 2022)

[20] DOD, Identity, Credential, and access Management (ICAM) Strategy, (March 30, 2020)

[21] DOD, Zero Trust Reference Architecture, (July 2022)

[22] NIST, Pre-Draft Call for Comments: Digital Identity Guidelines, (June 2020)

[23] DOD OCIO, Memo, (December 20, 2019)

[24] Homeland Security, HSPD 12, (January 27, 2022)

[25] DOD Office of the CIO (OCIO), Memo, (August 20, 2018)

[26] DOD OCIO, Memo, (December 20, 2019)

[27] Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)

[28] DOD Office of the CIO (OCIO), Memo, (August 20, 2018)

[28] C. Todd Lopez, "DISA Director Says Common Access Card Showing Age", (October 8, 2021)

[29] C. Todd Lopez, "DISA Director Says Common Access Card Showing Age", (October 8, 2021)

[30] DISA for the DOD, Department of Defense Cloud Computing Security Requirements Guide Version 1, Release 4, (January 14, 2022)

[31] DOD, Use of Non-Government Owned Mobile Devices, (August 10, 2022)

[32] White House, EO 13873, (May 15, 2019)

yubico

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.