



yubico




How the YubiKey helps department of defense contractors meet the cybersecurity maturity model certification

The Cybersecurity Maturity Model Certification (CMMC) is the Department of Defense’s (DoD) unified standard for implementing cybersecurity across the defense industrial base, consisting of fourteen domains and three maturity levels. This document addresses the specific CMMC domains and capabilities that the YubiKey meets or exceeds pertaining to the following domains—Identification and Authentication, Access Control, Audit and Accountability, Maintenance, and Media Protection.

CMMC Model 2.0		
	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-171 and 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110+ practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Triennial self-assessment for select programs
LEVEL 1 Foundational	15 practices	Annual self-assessment & annual affirmation

The CMMC domain—Identification and Authentication (IA. L2-3.5.3) in particular lists the requirement for multi-factor authentication. The YubiKey, a hardware security key that is designed to stop account takeovers, meets this level 2 requirement by providing highest-assurance phishing-resistant multi-factor authentication 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. The

YubiKey can also be used in conjunction with passwords or PIN to provide multi-factor authentication leveraging the FIDO U2F, FIDO2 and OTP (HOTP, TOTP, YubiOTP) protocols.



The YubiKey is the only FIPS-validated security key (Certificate #3517 Overall Level 2, Physical Security Level 3) that is made in the USA, complies with the Trade Agreements Act (TAA), and meets the most stringent secure supply chain requirements.

The tables below showcase how the YubiKey helps DoD contractors and sub-contractors meet CMMC for Identification and Authentication, Access Control, Audit and Accountability, Maintenance, and Media Protection domains.



YubiKeys deployed in:

9 of the top 10
global technology
companies

4 of the top 10
U.S. banks

5 of the top 10
global retailers

Domain: Access Control (AC)		
Capacity	Levels	Response
<p>C001</p> <p>Establish system access requirements</p>	<p>Level 1</p> <p>AC.L1-3.1.1</p> <p>Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).</p> <ul style="list-style-type: none"> • FAR Clause 52.204-21 b.1.i • NIST SP 800-171 Rev 1 3.1.1 • CIS Controls v7.1 1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11 • NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17 • AU ACSC Essential Eight 	<p>Access can be controlled and limited by the YubiKey leveraging the PIV module. Using the YubiKey as a smart card, authorization policies are centralized and access is tightly controlled.</p>
<p>C002</p> <p>Control internal system access</p>	<p>Level 1</p> <p>AC.L1-3.1.2</p> <p>Limit information system access to the types of transactions and functions that authorized users are permitted to execute.</p> <ul style="list-style-type: none"> • FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 Rev 1 3.1.2 • CIS Controls v7.1 1.4, 1.6, 5.1, 8.5, 14.6, 15.10, 16.8, 16.9, 16.11 • NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17 <p>Level 2</p> <p>AC.L2-3.1.5</p> <p>Employ the principle of least privilege, including for specific security functions and privileged accounts.</p> <ul style="list-style-type: none"> • NIST SP 800-171 Rev 1 3.1.5 • CIS Controls v7.1 14.6 • NIST CSF v1.1 PR.AC-4 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-6, AC-6(1), AC-6(5) • UK NCSC Cyber Essentials <p>AC.L2-3.1.6</p> <p>Use non-privileged accounts or roles when accessing nonsecurity functions.</p> <ul style="list-style-type: none"> • NIST SP 800-171 Rev 1 3.1.6 • CIS Controls v7.1 4.3, 4.6 • NIST CSF v1.1 PR.AC-4 • NIST SP 800-53 Rev 4 AC-6(2) • UK NCSC Cyber Essentials <p>AC.L2-3.1.7</p> <p>Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.</p> <ul style="list-style-type: none"> • NIST SP 800-171 Rev 1 3.1.7 • NIST CSF v1.1 PR.AC-4 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-6(9), AC-6(10) <p>AC.L2-3.1.11</p> <p>Terminate (automatically) user sessions after a defined condition.</p> <ul style="list-style-type: none"> • NIST SP 800-171 Rev 1 3.1.11 • CIS Controls v7.1 16.7, 16.11 • NIST SP 800-53 Rev 4 AC-12 	<p>Access can be controlled and limited by the YubiKey leveraging the PIV module. Using the YubiKey as a smart card, authorization policies are centralized and access is tightly controlled.</p> <p>AC.L2-3.1.11—Terminate (automatically) user sessions after a defined condition.</p> <p>A smartcard policy can be implemented in such a way that when the YubiKey is removed from the computer, the OS is locked.</p>

Domain: Audit and Accountability (AU)

Capacity	Levels	Response
<p>C009</p> <p>Identify and protect audit information</p>	<p>Level 2</p> <p>AU.L2-3.3.8</p> <p>Protect audit information and audit logging tools from unauthorized access, modification, and deletion.</p> <ul style="list-style-type: none"> • NIST SP 800-171 Rev 1 3.3.8 • CERT RMM v1.2 MON:SG2.SP3 • NIST SP 800-53 Rev 4 AU-6(7), AU-9 <p>AU.L2-3.3.9</p> <p>Limit management of audit logging functionality to a subset of privileged users.</p> <ul style="list-style-type: none"> • NIST SP 800-171 Rev 1 3.3.9 • CERT RMM v1.2 MON:SG2.SP2 • NIST SP 800-53 Rev 4 AU-6(7), AU-9(4) 	<p>Access can be controlled and limited by the YubiKey leveraging the PIV module. Using the YubiKey as a smart card, authorization policies are centralized and access is tightly controlled.</p>

Domain: Identification and Authentication (IA)

Capacity	Levels	Response
<p>C015</p> <p>Grant access to authenticated entities</p>	<p>Level 2</p> <p>IA.L2-3.5.3</p> <p>Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.</p> <p>NIST SP 800-171 Rev 1 3.5.3</p> <ul style="list-style-type: none"> • CIS Controls v7.1 4.5, 11.5, 12.11 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 IA-2(1), IA-2(2), IA-2(3) • AU ACSC Essential Eight <p>IA.L2-3.5.4</p> <p>Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.</p> <ul style="list-style-type: none"> • NIST SP 800-171 Rev 1 3.5.4 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • NIST SP 800-53 Rev 4 IA-2(8), IA-2(9) 	<p>The YubiKey can provide multifactor authentication through a number of protocols for local and network access. By default, PIV and FIDO2 based authentication provide multifactor authentication by having the user enter a PIN to unlock the secure element on the YubiKey as one factor (something you know). The second factor would be the possession of the private key that is used in the authentication ceremony. The private key does not leave the YubiKey (something you have).</p> <p>The YubiKey can also be used in conjunction with passwords to provide multifactor authentication leveraging FIDO U2F, FIDO2 or OTP (HOTP, TOTP, YubiOTP) based protocols.</p> <p>IA.L2-3.5.4</p> <p>YubiKeys are resistant to replay attacks by leveraging standards that take this into account. PIV and FIDO2 required possession of the physical YubiKey. OTP based protocols are time or hash based synchronous.</p>

Domain: Maintenance (MA)

Capacity	Levels	Response
<p>C021 Manage maintenance</p>	<p>Level 2 MA.L2-3.7.5</p> <p>Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.</p> <ul style="list-style-type: none"> • NIST SP 800-171 Rev 1 3.7.5 • NIST CSF v1.1 PR.MA-2 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 MA-4 	<p>The YubiKey can provide multifactor authentication through a number of protocols for local and network access. By default, PIV and FIDO2 based authentication provide multifactor authentication by having the user enter a PIN to unlock the secure element on the YubiKey as one factor (something you know). The second factor would be the possession of the private key that is used in the authentication ceremony. The private key does not leave the YubiKey (something you have).</p> <p>The YubiKey can also be used in conjunction with passwords to provide multifactor authentication leveraging FIDO U2F, FIDO2 or OTP (HOTP, TOTP, YubiOTP) based protocols.</p> <p>Given the portability and standard form factors, YubiKey's can easily be given to third parties that perform remote access to internal systems.</p>

Domain: Media Protection (MP)

Capacity	Levels	Response
<p>C023 Protect and control media</p>	<p>Level 2 MPL2-3.8.8</p> <p>Prohibit the use of portable storage devices when such devices have no identifiable owner.</p> <ul style="list-style-type: none"> • NIST SP 800-171 Rev 1 3.8.8 • NIST CSF v1.1 PR.PT-2 • CERT RMM v1.2 MON:SG2.SP4 • NIST SP 800-53 Rev 4 MP-7(1) 	<p>Even though the YubiKey interfaces with the computer via a USB port, it is not a portable storage device. It does not have the capacity to store media. YubiKeys can also be identified by their USB identifier.</p>



WATER RESISTANT



CRUSH RESISTANT



MADE IN USA



Contact us

yubi.co/contact-us
yubi.co/contact-sales



Learn more

yubi.co/federal