yubico

Press Release
04 June 2026 20:35:00 CEST

Yubico Achieves FIPS 140-3 Validation for YubiHSM 2 FIPS, Strengthening Hardware Root of Trust for Critical Infrastructure

YubiHSM 2 FIPS delivers high-assurance cryptographic protection for keys, secrets and non-human identities in modern enterprise and operational technology environments

Yubico, the pioneer of phishing-resistant authentication and creator of the YubiKey, today announced that YubiHSM 2 FIPS has achieved FIPS 140-3 validation with Certificate #5302, published by the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP). Following the YubiKey 5 FIPS Series also becoming FIPS 140-3 validated, this milestone reinforces Yubico's commitment to delivering modern hardware-backed security for organizations protecting critical infrastructure, manufacturing systems, government environments and high-assurance enterprise workloads.

As cyberattacks increasingly target cryptographic keys, machine identities and software supply chains, organizations require stronger hardware roots of trust to secure sensitive systems and operations. YubiHSM 2 FIPS is purpose-built to protect cryptographic keys and perform secure cryptographic operations inside a tamper-resistant hardware security module (HSM), helping organizations reduce exposure to key theft, credential compromise and unauthorized access.

"AI-driven cyber threats are accelerating attacks against software, identities and cryptographic infrastructure," said Albert Biketi, chief product and technology officer at Yubico. "YubiHSM 2 FIPS delivers a hardware-backed root of trust for organizations securing sensitive workloads, manufacturing systems, operational technology and critical infrastructure. Achieving FIPS 140-3 validation reinforces Yubico's commitment to delivering modern, high-assurance cryptographic security built for today's evolving threat landscape."

As U.S. Government agencies and regulated enterprises accelerate Zero Trust adoption, the FIPS 140-3 validation of Yubico's YubiHSM 2 Cryptographic Module under NIST CMVP Certificate #5302 strengthens a critical hardware-backed foundation for modern identity, data protection and AI security. NIST SP 800-207 defines Zero Trust around granular, least privilege, per request access decision in environments where the network is assumed compromised. CISA's Zero Trust Maturity Model, and the NSA Zero Trust Implementation Guides, translate those principles into maturity and implementation guidance across identity, devices, application and workloads, data, automation and analytics.

Anthropic's latest paper on Zero Trust for AI agents extends this same model to AI agents, emphasizing cryptographically rooted identities, task scoped permissions and breach ready architectures. YubiHSM helps organizations protect cryptographic keys, certificates and credentials while supporting continuous verification, least-privilege access, and cryptographically rooted trust for mission-critical systems and emerging AI agent workflows.

The YubiHSM 2 FIPS 140-3 validated module meets Overall Level 3 security requirements and

provides advanced physical security protections for safeguarding cryptographic material and sensitive operations. The validation aligns with the latest FIPS 140-3 cryptographic framework and international ISO/IEC 19790 standards, helping organizations meet evolving global security and compliance expectations.

For more information on YubiHSM 2 FIPS and FIPS 140-3 validation, visit: https://www.yubico.com/products/hardware-security-module/

For more information contact:

Karin Muskopf
Global Communications
press@yubico.com

About Yubico

Yubico (Nasdaq Stockholm: YUBICO), the inventor of the YubiKey, offers the gold standard for phishing-resistant multi-factor authentication (MFA), stopping account takeovers in their tracks and making secure login easy and available for everyone. Since the company was founded in 2007, it has been a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO2, 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 175 countries.

Yubico's solutions enable passwordless logins using the most secure form of passkey technology. YubiKeys work out-of-the-box across more than a thousand consumer and enterprise applications and services, delivering strong security with a fast and easy experience.

As part of its mission to make the internet more secure for everyone, Yubico donates YubiKeys to organizations helping at-risk individuals through the philanthropic initiative, Secure it Forward. The company is headquartered in Stockholm and Santa Clara, CA, and Singapore. For more information on Yubico, visit us at www.yubico.com.

Attachments

Yubico Achieves FIPS 140-3 Validation for YubiHSM 2 FIPS, Strengthening Hardware Root of Trust for Critical Infrastructure