Yubico Announces Upgraded YubiKey 5 FIPS Series, Now FIPS 140-3 Validated

YubiKey 5 FIPS Series uniquely recognized in DoD guidance for hardware-based FIDO2 passkeys, bridging modern authentication with existing identity systems

SANTA CLARA, Calif. & STOCKHOLM--(BUSINESS WIRE)-- Regulatory News:

Yubico (NASDAQ STOCKHOLM: YUBICO), the pioneer of phishing-resistant authentication and creator of the most secure hardware-backed passkey, the YubiKey, today announced the certification of the next generation of its YubiKey 5 FIPS Series – now FIPS 140-3 validated with Certificate #5291. Published by the National Institute of Standards and Technology (NIST), this milestone represents the latest evolution in cryptographic module validation and reinforces Yubico's leadership in delivering hardware-backed phishing-resistant authentication. The YubiKey 5 FIPS Series supports Zero Trust and modern cybersecurity mandates, and is trusted by governments, defense organizations and the world's most security-conscious enterprises.

"Yubico is setting a new standard for high-assurance authentication, combining government-grade compliance with hardware-backed passkeys," said Albert Biketi, chief product and technology officer at Yubico. "YubiKey 5 FIPS Series is the only authenticator authorized by the U.S. Government to hold both DoD PKI credentials and FIDO2 passkeys – giving government and regulated organizations a secure bridge to passwordless. With the transition from FIPS 140-2 to FIPS 140-3, government agencies and regulated organizations are moving to a new global standard for cryptographic security – and Yubico is leading this shift with the upgraded YubiKey 5 FIPS Series."

For organizations responsible for protecting sensitive information – including U.S. federal agencies, defense contractors and regulated industries – transitioning to FIPS 140-3 is a foundational requirement to maintain compliance and security assurance. As the only authenticator authorized by the U.S. Department of Defense to hold both DoD PKI credentials and FIDO2 passkeys, this unique dual capability simplifies deployments while strengthening phishing-resistant security – allowing organizations to leverage a single hardware device to support FIDO2/WebAuthn, PIV/Smart Card authentication, OpenPGP and OATH OTP.

The FIPS 140-3 framework aligns closely with the international ISO/IEC 19790:2012 cryptographic standard, helping global enterprises and government agencies adopt a unified, modern security baseline across their operations. The upgraded YubiKey 5 FIPS Series meets FIPS 140-3 Overall Level 2, with Physical Security Level 3 – providing high-assurance authentication designed for the most demanding security environments. Additionally, the devices enable compliance with NIST SP 800-63B Authenticator Assurance Level 3 (AAL3) requirements.

Powerful Enterprise-Grade Features for Regulated Environments

Featuring the latest YubiKey 5.7.4 firmware, the YubiKey 5 FIPS Series addresses high assurance enterprise authentication requirements, spanning PKI and modern passkey use cases.

- **Expansion and Enhancement of Public Key Algorithms**: Support for larger RSA keys (RSA-3072 and RSA-4096) and Ed25519, enhancing key management functions and flexibility for organizations – aligning with DoD memo requirements on stronger public key algorithms.
- **Restricted NFC Usage During Transit**: NFC capable YubiKeys have restricted NFC usage to prevent manipulation during transit.
- **Enhanced PIN Complexity:** Enabled by default across all YubiKey applications, including FIDO2, PIV and OpenPGP.
- **FIDO Client to Authenticator Protocol (CTAP) 2.1 implementation:** Improvements around the FIDO2 PIN, including Force PIN Change and Minimum PIN Length – addressing PIN requirements in "enroll on behalf" scenarios.
- **Expanded Passkey and Passwordless Storage Capabilities**: Accommodating up to 100 device-bound passkeys (up from 25), 64 OATH seeds (up from 32) and 24 PIV certificates.
- **Enterprise Attestation**: Facilitates the retrieval of unique identifiers during FIDO2 registration and streamlining asset tracking by allowing identity providers to read the serial number from the YubiKey during FIDO2 registration.
- **New secure channel protocol:** The addition of SCP11, which is based on asymmetric cryptography.

The YubiKey 5 FIPS Series will be available in a wide range of form factors – including USB-A, USB-C, NFC, Lightning and Nano – ensuring seamless compatibility across modern laptops, mobile devices and secure closed-network environments.

For more information on the YubiKeys 5 FIPS Series and 140-3 Validation, read Yubico's blog here or visit: https://www.yubico.com/products/yubikey-fips/

About Yubico

Yubico (Nasdaq Stockholm: YUBICO) is a modern cybersecurity company on a mission to make the digital world safer for everyone. As the inventor of the YubiKey, we set the gold standard for modern phishing-resistant, hardware-backed authentication, stopping account takeovers and making secure login simple.

Since 2007, we've helped shape global authentication standards, co-created FIDO2, WebAuthn, and FIDO U2F, and introduced the original passkey. Today, our passkey technology secures people and organizations in over 160 countries—transforming how digital identity is protected from onboarding to account recovery.

Trusted by the world's most security-conscious brands, governments, and institutions, YubiKeys work out of the box with hundreds of apps and services, delivering fast, passwordless access without friction or compromise.

We believe strong security should never be out of reach. Through our philanthropic initiative, Secure it Forward, we donate YubiKeys to nonprofits supporting at-risk communities.

Headquartered in Stockholm, Sweden; Santa Clara, California; and Singapore, Yubico is proud to be recognized as one of TIME's 100 Most Influential Companies and Fast Company's Most Innovative Companies. Learn more at www.yubico.com.

Contacts

Yubico
Yubico Communications Team
press@yubico.com

Source: Yubico