yubico

Preparing for FIPS 140-3

Your Top 10 Compliance Questions Answered

As cyber threats grow more sophisticated—accelerated by automation and AI—organizations responsible for protecting sensitive systems and data are raising the bar for identity assurance. At the same time, regulatory frameworks are evolving, with the transition from FIPS 140-2 to FIPS 140-3 establishing a new global benchmark for cryptographic security.

1 What is the FIPS standard?

FIPS 140-3 is a U.S. government standard that defines security requirements for cryptographic modules used in hardware and software systems, adopted by many global organizations. It is administered through the Cryptographic Module Validation Program (CMVP) managed by the National Institute of Standards and Technology (NIST).

The standard helps validate that cryptographic functions—such as encryption, key generation, authentication, and secure storage—meet rigorous security requirements for sensitive environments.

2 What is FIPS 140-3 validation?

FIPS 140-3 is the latest NIST standard for validating the security of cryptographic modules used in hardware and software systems. It defines how encryption, key management, authentication, and secure operations must be implemented and protected.

In identity security, FIPS 140-3 helps ensure that authentication systems and credentials are protected against tampering, theft, and unauthorized access.

3 Why is FIPS validation important for identity security?

Modern identity systems depend on trusted cryptography to: protect credentials, secure authentication flows, defend against phishing attacks, and establish trusted access to systems and applications.

FIPS 140-3 validation helps organizations verify that the cryptographic components supporting authentication are independently tested against recognized security standards. This is especially important in regulated and high-assurance environments.

4 Who typically requires FIPS 140-3 validated solutions?

Organizations are increasingly transitioning from FIPS 140-2 validated products to FIPS 140-3 validated solutions. These include highly regulated industries such as federal agencies, defense contractors, financial institutions, healthcare organizations, critical infrastructure providers, and other regulated enterprises.

Additionally, many procurement policies and compliance frameworks require FIPS-validated cryptography for sensitive systems and user authentication.

5 What is the difference between FIPS 140-3 and FIPS 140-2?

The Federal Information Processing Standard (FIPS) 140-3 represents the latest evolution in cryptographic module validation. FIPS 140-3 introduces more rigorous cryptographic and operational requirements while aligning closely with the international ISO/IEC 19790 standard—enabling governments and global enterprises to adopt a unified security baseline.

6 What is the deadline for the transition from FIPS 140-2 to FIPS 140-3?

FIPS 140-2 validated modules will move to Historical status after September 21, 2026, leaving FIPS 140-3 as the active validation standard moving forward.

7 What steps should organizations take today to prepare for the FIPS 140-3 future?

Organizations that are currently using FIPS 140-2 validation solutions and/or looking to upgrade to FIPS 140-3 validated solutions should:

- Inventory existing FIPS-dependent systems
- Assess passwordless readiness
- Evaluate identity modernizationn plans and align procurement requirements
- Build migration timelines ahead of compliance deadlines

8 What is the YubiKey 5 FIPS Series?

Yubico is meeting this moment with the next generation of YubiKey 5 FIPS Series security keys, now FIPS 140-3 validated. The YubiKey 5 FIPS Series provides high-assurance, phishing-resistant authentication that helps organizations stop account takeovers, meet stringent regulatory requirements, and accelerate their transition to modern passwordless security.

9 What sets Yubico apart for the Department of Defense?

Yubico's leadership in high-assurance authentication has been recognized by the U.S. Department of Defense, which named the YubiKey 5 FIPS Series the sole authenticator authorized to hold both DoD PKI credentials and FIDO2 passkeys in its memo on Multi-factor Authentication from October 24, 2025.

This recognition underscores the YubiKey's unique ability to support both legacy PKI infrastructure and modern phishing-resistant authentication in a single hardware device. For federal agencies and defense organizations undergoing identity modernization, this dual capability simplifies deployments while strengthening security posture.

10 What are the top 5 things to know about this lineup?

With the YubiKey 5 FIPS Series, now FIPS 140-3 validated, Yubico is setting a new standard for high-assurance authentication.

- Next-generation FIPS 140-3 validation: The YubiKey 5 FIPS Series meets the latest U.S. government cryptographic standard (Levels 1 & 2, Physical Security Level 3), helping organizations maintain compliance as FIPS 140-2 is fully deprecated in 2026
- Recognized by the U.S. Department of Defense: The YubiKey FIPS Series is the only authenticator authorized to hold both DoD PKI credentials and FIDO2 passkeys, uniquely enabling secure identity modernization for federal and defense environments
- Phishing-resistant security for the AI threat era: Hardware-backed passkeys help eliminate account takeovers and protect against modern threats—including AI-driven phishing, credential theft, and social engineering attacks
- A bridge from legacy authentication to passwordless: Multi-protocol support—including FIDO2/WebAuthn, PIV, OpenPGP, OATH, and OTP—allows organizations to secure legacy systems while accelerating adoption of modern passwordless authentication
- Flexible deployment across devices and environments: Available in multiple form factors—including USB-A, USB-C, NFC, Lightning, and Nano—the YubiKey 5 FIPS Series enables high-assurance authentication for government, defense, and regulated industries worldwide

To explore YubiKey 5 FIPS Series upgrade options with YubiKey as a Service, Compliance Tier, reach out to your sales or channel representative.

Learn More at yubi.co/fips