Kiteworks

Protecting Sensitive Data:

Critical Role of FIPS 140-2 and -3 Compliance

Data breaches have become a harsh reality that organizations across sectors face on a regular basis. As cybersecurity threats continue to grow in scale and sophistication, it is more important than ever for organizations to implement robust protections for sensitive data. This is where standards like the Federal Information Processing Standards (FIPS) come into play. In this eBook, we explore what FIPS is, why FIPS 140-2 compliance and validation matter, and how organizations can leverage FIPS to strengthen data security.

What Is FIPS?

FIPS refers to a set of standards published by the National Institute of Standards and Technology (NIST) that specify requirements for cryptography, computer security, and interoperability standards for hardware, software, and firmware used by the U.S. federal government and contractors working with the federal government. FIPS standards aim to ensure that sensitive data remains confidential and integral as it is collected, stored, processed, and communicated across information systems.

The standards provide guidance on which cryptographic algorithms federal agencies should adopt to protect sensitive data and specify how to implement those algorithms correctly. FIPS compliance helps federal agencies and contractors meet regulatory obligations and demonstrate due diligence in protecting sensitive government data from internal and external threats.

While FIPS compliance is mandatory for U.S. federal agencies and contractors, private sector organizations also stand to benefit, as the standards promote best practices in data security.

Quantum Encryption Is the Future

Spin Quantum Tech's and AnniQ's CEO and Entrepreneur Jean Phillip Bernier spells out real-world applications of quantum computing, including AI-enabled algorithm acceleration and an encryption method known as entropic encryption in this Kitecast episode. The latter offers a fresh perspective by harnessing the inherent chaos and entropy of quantum states.

Listen to the Podcast

The Evolution of FIPS

1970s

The origins of FIPS date back to the early 1970s when there was growing concern about the vulnerability of sensitive electronic data in computer systems. To address these concerns, the National Bureau of Standards (now NIST) published the first FIPS standards between 1972-1981 to promote confidentiality and integrity of data processed by federal computer systems.

1980s - 1990s

Early FIPS publications provided standards for encoding data, developing passwords, managing cryptographic keys, utilizing encryption algorithms, and more. As technology advanced rapidly, NIST updated the FIPS standards accordingly over the years. Significant milestones include FIPS 46 Data Encryption Standard in 1977, FIPS 81 DES Modes of Operation in 1980, and FIPS 140-1 Security Requirements for Cryptographic Modules in 1994.

2000s

In 2001, NIST published FIPS 140-2, a major update to the FIPS cryptographic standards that remains one of the most critical and widely adopted standards. As cyber threats have grown exponentially in recent decades, the role of FIPS compliance in protecting sensitive data continues to be as crucial as ever.

Why Is FIPS 140-2 Validation Important?

FIPS 140-2 defines security requirements for cryptographic modules used to secure sensitive data. Cryptographic modules can include hardware, software, and firmware that implement cryptographic algorithms, generate keys, and perform encryption/decryption. FIPS 140-2 specifies four levels of security requirements for cryptographic modules, with Level 1 being the lowest and Level 4 being the highest. The different levels account for factors like physical security, key management protocols, algorithm strength, and more.

For organizations dealing with highly sensitive data, it is critical that the cryptographic modules they utilize meet the higher levels of FIPS 140-2 validation. This third-party validation provides assurance that the modules offer strong protections against vulnerabilities and meet industry security standards.

Some key reasons why FIPS 140-2 validation matters:

- Validates that encryption algorithms are robust and secure against external attacks
- Ensures proper management of cryptographic keys and PINs/passphrases
- Modules undergo third-party testing to analyze security mechanisms
- Higher levels mandate physical security mechanisms to prevent tampering
- Provides visibility into a module's security policy for administrators
- Validation must be renewed every few years to maintain assurance

For federal agencies and contractors handling government data, FIPS 140-2 validation is a mandatory compliance requirement. But beyond just meeting regulatory obligations, FIPS 140-2 validation demonstrates an organization's commitment to implementing state-of-the-art encryption that safeguards sensitive data.

FIPS 140-2 for Federal Agencies, Defense Contractors, and Other Industry Sectors

FIPS 140-2 validation addresses the federal government and entities that transmit sensitive content with federal agencies. Following are some examples of how organizations can leverage FIPS 140-2 to enhance data protections:

- **Government Agencies:** Secure sharing of sensitive data like financial records, health data, and classified documents with federal partners and contractors.
- **Defense Contractors:** Secure critical systems that process classified Defense information and controlled unclassified information (CUI).
- **Healthcare Providers:** Secure protected health information (PHI) sent and shared with the federal government by securing databases, communication channels, and devices.
- **Financial Institutions:** Use certified cryptographic modules to encrypt personally identifiable information (PII) sent and shared with the federal government.

As these examples demonstrate, validating compliance with FIPS 140-2 provides a strong foundation for end-to-end data security across diverse environments.

FIPS 140-2 Validation Accelerates HIPAA and PCI DSS Compliance

While FIPS 140-2 validation is not an explicit requirement of the Health Insurance Portability and Accountability Act (HIPAA) or Payment Card Industry Data Security Standard (PCI DSS), it provides a standardized way for organizations to demonstrate their encryption meets adequacy standards. Specifically, the HIPAA Security Rule requires covered entities to implement technical safeguards to protect electronic protected health information (ePHI), including encryption. It states encryption must be addressed in a risk analysis and implemented if reasonable and appropriate. However, HIPAA does not prescribe any particular encryption algorithms or strength. This is left to the discretion of the organization. Obtaining FIPS 140-2 validation provides evidence that the encryption used meets government standards for security and integrity.

Similarly, the PCI DSS requires the use of strong cryptography for encryption of cardholder data. It also recommends FIPS 140-2 validated encryption modules. By using FIPS 140-2 validated cryptographic modules, merchants can simplify and streamline their PCI DSS compliance process. The PCI Security Standards Council recognizes FIPS 140-2 as an acceptable encryption standard.

The Future of FIPS: FIPS 140-3

As cybersecurity threats continue to evolve, NIST is advancing the FIPS 140 standards to incorporate new technologies and strengthen cryptographic protections. In March 2019, NIST officially released the FIPS 140-3 standard that will eventually replace the current FIPS 140-2 standard.

FIPS 140-3 introduces new requirements to keep up with modern security needs, including:

- Support for current cryptographic algorithms like AES, SHA-3, and ECC that provide strong protection against attacks by quantum computers in the future
- Expanded testing requirements for cryptographic modules to validate security mechanisms under a wider range of conditions
- Addition of secure firmware updates for software and firmware modules to fix vulnerabilities without exposing sensitive data
- Enhanced physical security requirements for high security levels, including complete opacity of cryptographic operations
- Tamper-detection mechanisms to erase keys/critical data when physical integrity is lost
- Improved key management standards for generating, storing, and transferring keys

The transition period from FIPS 140-2 to FIPS 140-3 allows time for vendors to update their products and services. NIST will continue accepting FIPS 140-2 validations until September 2026. As the definitive industry benchmark for cryptography, the FIPS 140-2 standard will continue evolving to meet modern data security needs. FIPS 140-3 represents the next step, promoting best practices for robust encryption, key management, algorithm testing, firmware updates, and physical protections. Organizations that leverage FIPS 140-2 to secure sensitive data can ensure they are keeping pace with the latest security standards endorsed by NIST.

Kiteworks FIPS 140-2 Validation

Kiteworks offers a content collaboration platform that enables secure sharing of sensitive content within and across organizations. The Kiteworks-enabled Private Content Network meets the criteria for FIPS 140-2 validation, which Kiteworks first attained in 2014.

Kiteworks leverages FIPS 140-2 certified technologies in several components of its platform:

- The Kiteworks Key Management Server (KMS) utilizes FIPS 140-2 validated technology to generate, manage, and store encryption keys.
- The Kiteworks Content Processing Server uses FIPS 140-2 compliant mechanisms to encrypt and decrypt content.
- TLS-based communications for content uploads, downloads, and previews in Kiteworks are FIPS 140-2 compliant.
- Hashing algorithms used for data integrity checks are FIPS 140-2 approved.

Kiteworks also allows granular access controls, detailed activity tracking/auditing, and other security capabilities to help organizations manage their sensitive content. With its robust encryption validated under FIPS 140-2 standards, Kiteworks enables organizations to collaborate securely on confidential data across applications, networks, and devices while ensuring regulatory compliance. The certified cryptographic modules provide assurance that customer data is safeguarded with industry-best encryption strength.

By opting for technology solutions like Kiteworks that carry trusted FIPS 140-2 validation, organizations can fulfill their ethical and legal responsibilities in protecting sensitive information that has been entrusted to them by customers, partners, and regulatory agencies. The Kiteworks codebase is currently being validated in NIST's FIPS 140-3 process.

Kiteworks

www.kiteworks.com

October 2023