WHITE PAPER

FIPS 140-2 Security and Encryption

FIPS 140-2 (Federal Information Processing Standard Publication 140-2) represents a critical US government standard that defines security requirements for cryptographic modules used to protect sensitive information. Established by the National Institute of Standards and Technology (NIST), this standard provides a comprehensive framework for evaluating and certifying the security effectiveness of cryptographic hardware and software components.

FIPS 140-2 serves as the benchmark for ensuring that cryptographic implementations meet rigorous security criteria across four distinct security levels, ranging from basic production-grade requirements to the highest level of physical tamper evidence and response capabilities.

PATTON®
Let's Connect!™

50000160 Rev. A0

Contents

Authored by

Bob Mohr
Federal Sales Director
Patton LLC

and

Walter Glendon Flowers
Product Marketing Manager
Patton LLC

Printed in the USA.

Introduction To FIPS 140-2

Technical Overview

FIPS 140-2 defines security requirements for cryptographic modules across the following categories:

- Cryptographic module specification
- Finite state model
- Physical security
- Electromagnetic interference/ electromagnetic compatibility
- Self-tests
- Design assurance
- Mitigation of other attacks
- Key management

The FIPS standard defines four progressive security levels:

Level 1 requires basic security features and production-grade components.

Level 2 adds requirements for tamper-evident coatings, role-based authentication, and enhanced physical security.

Level 3 introduces tamper-resistant capabilities and identity-based authentication with a high probability of detecting physical tampering.

Level 4 provides the highest level of security. This level requires tamper-responsive features that immediately zeroize critical security parameters when a module detects physical intrusion.

Each level builds upon the previous level while addressing increasingly sophisticated attack scenarios.

FIPS 140-2 in industry

In the private sector, FIPS 140-2 compliance has become essential for organizations that either a) operate in regulated industries, or b) handle sensitive data that requires government-grade security.

Financial institutions rely on FIPS 140-2 validated cryptographic modules for securing payment processing systems and ATM networks, as well as customer data protection.

Healthcare organizations implementing electronic health record systems frequently require FIPS 140-2 compliance to meet HIPAA security requirements for protecting patient information.

Cloud service providers and technology companies seeking government contracts or serving regulated clients often pursue FIPS 140-2 validation as a competitive differentiator:

FIPS compliance demonstrates commitment to robust security practices that meet federal standards.

FIPS 140-2 in State and Local Governments

State and local governments have increasingly adopted FIPS 140-2 requirements as part of their cybersecurity frameworks—especially for systems that handle sensitive citizen data, law enforcement information, and critical infrastructure operations.

Many states mandate FIPS 140-2 compliance for IT procurement processes, requiring vendors to provide validated cryptographic solutions for government applications.

Local governments, especially larger municipalities and counties, often incorporate FIPS 140-2 requirements into their security policies for systems that manage voter registration databases, property records, court systems, and emergency services communications. This adoption reflects a growing recognition that state and local governments face security challenges similar to federal agencies and therefore benefit from implementing the same cryptographic standards.

JITC/APL Processes

JITC and APL. The Joint Interoperability Test Command (JITC) and Approved Products List (APL) processes have historically incorporated FIPS 140-2 validation as a fundamental requirement for cryptographic products that seek department of Defense (DoD) approval.

JITC testing procedures evaluate commercial off-the-shelf (COTS) and government off-the-shelf products against stringent interoperability and security standards. FIPS 140-2 compliance serves as a prerequisite for JITC use of cryptographic components.

APL processes ensure approved products maintain validation status throughout their operational lifecycle. APL requires vendors to demonstrate continued compliance with evolving security FIPS requirements. This integration helps DoD organizations confidently select cryptographic solutions that meet both functional requirements and security mandates while ensuring interoperability across diverse operational environments.

Retirement of Older Releases

NIST regularly reviews and updates its cryptographic standards library. FIPS 140-2 releases and associated validation certificates that no longer meet current security requirements must be retired. This retirement process reflects the evolving threat landscape. Advances in cryptographic research may reveal vulnerabilities in previously-accepted algorithms or implementation practices.

Organizations that use products validated under retired standards must transition to newer FIPS 140-2 validations or risk operating with cryptographic modules that no longer meet current federal security requirements. The retirement process typically provides adequate transition periods, but requires vigilance. Organizations must monitor their cryptographic inventory and plan timely upgrades to maintain compliance with current standards.

FIPS Compliance

What does it mean to be "FIPS compliant"?

In 2002, the Computer Security Division (CSD) of the National Institute of Standards and Technology (NIST) developed the Federal Information Security Management Act of 2002 (FISMA) as a data-security and computer-system standard.

According the the standard, Federal government organizations in the United States must reduce information-technology risk to an acceptable level at a fair cost.

The Federal Information Security Modernization Act of 2014 (FISMA2014)—replaced FISMA in 2014. The updated standard—changed its original provisions to reflect evolving cybersecurity requirements and the need for supervision.

To be considered FIPS compliant, a US government agency's and government contractor's computer systems must satisfy the criteria cited in FIPS publications numbered FIPS 140, FIPS 180, FIPS 186, FIPS 197, FIPS 198, FIPS 199, FIPS 200, FIPS 201, and FIPS 202. This paper covers FIPS 140.

Security Requirements for Cryptographic Modules

The combination of hardware, software, and firmware that implements such security features as algorithm execution and key creation is called a *cryptographic module*. The techniques for testing and validating such modules are specified in the FIPS-140 standard. FIPS-compliant organizations must follow the standard when creating, implementing, and operating cryptographic modules.

The security standards cover an extensive set of topics, including the following:

- Cryptographic module interfaces
- Software and firmware security
- Operating environment
- Physical security
- Security parameter management

- Self-tests
- Attack mitigation
- Roles
- Services
- Authentication

The cryptographic modules used by Federal departments and agencies must pass testing to ensure they meet these requirements before they may be used.

FIPS Compliance Levels

FIPS 140-2 specifies four security levels:

FIPS Level 1 specifies fundamental security requirements for the cryptography module and its algorithms. Beyond the fundamental necessity for production-grade components, a Level 1 cryptographic module does not include any physical security features specified in higher levels. PC encryption boards are an example of a Security Level 1 cryptographic module.

FIPS Level 2 certification requires the module to provide additional physical security mechanisms in addition to those required by Security Level 1. A level 2 cryptographic module must provide mechanisms that detect tampering. Such elements may include:

- **Tamper-evident coatings**
- **Physical seals** that must be broken to gain access to internal cryptographic keys and critical security parameters (CSPs)
- **Pick-resistant locks** on covers or doors that prevent unauthorized physical access.

FIPS Level 3 specifies physical security mechanisms designed to prevent intruders from gaining access to CSPs stored within the cryptographic module —in addition to the tamper-evident physical security measures required in Level 2. Level 3 mechanisms detect and react to an intruder's attempt to 1) gain physical access, 2) use, or 3) modify the cryptographic module.

Two examples of Level 3 physical security measures are:

1. Strong enclosures
2. Tamper-detect-and-respond circuitry that zeroes all plain-text CSPs when the removable covers/doors of the cryptographic module are opened

FIPS Level 4 offers the highest level of security. Level 4 physical-security

mechanisms surround the cryptographic module completely, serving as a barrier against unauthorized attempts at physical access. Should a malicious actor attempt to breach the enclosure of the cryptographic module, the module will detect the intrusion delete all CSPs that include plain text.

Cryptographic modules certified at Security Level 4 are useful in locations that lack physical protection. Attackers may employ voltage and temperature deviations outside the normal operating ranges to circumvent a cryptographic module's defenses. Security Level 4 shields the cryptographic module from such security breaches.

To meet Level 4 requirements, the module must ensure fluctuations outside of the normal operating range do not jeopardize its security by deleting any rogue CSPs. To ensure this level of protection, a cryptographic module must undergo rigorous environmental failure testing or include special environmental protection features.

Utilizing FIPS 140-2 Validated Solutions to Secure Enterprise Data-At-Rest

Enterprises store, transact, and analyze large volumes of data and have an obligation to keep this data private and secure. During its lifecycle, as data journeys through an enterprise and its network of suppliers and partners, it exists in three states:

1. at-rest
2. on-transit
3. in-use

Data at-rest and in-use can greatly benefit from FIPS 140-2 validated encryption.

Securing Data-at-Rest. Applying FIPS 140-2 validated encryption to data-at-rest (stored and not in active use) ensures unauthorized entities cannot read the data should they gain access to the data files. Employing FIPS 140-2 validated encryption guarantees the strength of underlying security algorithms.

Securing Data-in-Use. Although data-in-use encryption is a new discipline, we now have techniques that can keep valuable data encrypted even while database applications are actively using it.

FIPS 140-2 validated encryption-in-use is now available for various databases, enterprise search platforms, object stores, and file shares.

Why is FIPS Compliance Crucial?

For such industries as government contracting, finance, healthcare, and telecommunications, FIPS compliance is not just a technical requirement, it is a *legal*

obligation. For businesses that serve federal clients—or when processing regulated data—non-compliance can result in loss of contracts, fines, and damaged reputation.

Moreover, as organizations adopt such complex systems as cloud services, mobile applications, and IoT devices, the need for FIPS-compliant cryptographic solutions becomes critical for the following reasons:

Regulatory Compliance: Certain industries must comply with specific regulatory frameworks:

- HIPAA (for healthcare)
- PCI DSS (for payment processing)
- FISMA (for federal information security)

Many of these federally regulated industries are required to use FIPS-approved cryptographic modules to secure sensitive data.

Data Integrity: FIPS-certified modules protect data from tampering, which is critical for industries where trust and confidentiality are paramount. FIPS-certified modules ensure data remains secure during storage and transmission.

Government Contracts: Any business that works with the US Federal Government must certify their cryptographic systems are FIPS-compliant. The government mandates FIPS-certified solutions within its operations. This requirement also extends to government contractors.

Public Trust and Security Assurance: Achieving FIPS compliance demonstrates commitment to the highest standards of security, instilling confidence in stakeholders and clients that their data is managed securely.

The Importance of FIPS Compliance

All users should educate themselves about the importance of information security and organizations must make it a management priority. Data security needs vary from application to application, so each enterprise should identify their information resources and assess the sensitivity to and potential impact of data loss. The selection of security controls should be based on probable risks. Such controls may include:

- administrative policies and procedures
- environmental and physical controls
- information and data controls
- software development and acquisition controls
- backup and contingency planning

Case Study: Salt Typhoon

Salt Typhoon is an advanced and persistent threat. The actor, China's Ministry of State Security (MSS) has conducted high-profile cyber espionage campaigns against the United States and is believed to operate the threat. MSS operations target United States counterintelligence entities and steal corporate intellectual property (data theft). The group has also infiltrated secure targets in dozens of countries on every continent.

In July 2025, the DHS reported Salt Typhoon hacked the National Guard network for almost a year.

In a recent call with news outlets, the FBI revealed a state-sponsored cyber-attack on AT&T and Verizon is ongoing: The bad guys are still in these networks, with access to millions of customers' private phone data. Officials say it is "impossible to predict a time frame on when we'll have full eviction."

The FBI and CISA indicated that the attack, dubbed "Salt Typhoon," is worse and more pervasive than we all thought. The agencies urged Americans to not trust their sensitive information to such telecom companies AT&T and Verizon's networks, and to use data encryption to prevent China from intercepting communications.

"Our suggestion is not new: Encryption is your friend," said Jeff Greene, executive assistant director for cybersecurity at the Cybersecurity and Infrastructure Security Agency. Whether it's a phone call, text message, or email, using encrypted communication ensures that even if an adversary intercepts the data, it remains unreadable. Encryption converts the information into ciphertext, rendering it inaccessible without the decryption key.

Patton and FIPS-140 Compliance

Patton's FIP-140-2 software release for SmartNode and Tone Commander products utilizes the most current OpenSSL and active NIST Cryptographic Module.

Patton's has built its updated FIPS release on the most recent version of OpenSSL (3.0) using the most up-to-date cryptographic algorithms, ciphers, hash functions, and key lengths. Patton is also ready now for the upcoming release of FIPS 140-3

This enhancement further establishes Patton as a trusted government solution provider, for Federal, State and Local Agencies, as well as contractors and such government-related or government-regulated organizations as educational, financial and medical institutions.

Implementing FIPS 140 into communication technologies ensures sensitive data remains secure and confidential. FIPS represents a US

standard established by the National Institute of Standards and Technology (NIST) for validated cryptography.

Many government bodies are required to adhere to FIPS 140-2 and comply with the Federal Information Security Management Act (FISMA). Organizations required to adhere to HIPAA requirements must also use FIPS-validated devices.

Key Advantages of Patton's FIPS 140-2 implementation

Better Security. Patton employs up-to-date authentication and strong cryptographic protection using approved algorithms and techniques, which provide robust data protection.

Reduced Risk of breaches, tampering and attacks by stringently adhering to FIPS standards. Hackers collect unencrypted data to gain unauthorized access to sensitive information. FIPS 140-2 and 140-3 incorporate physical security measures to protect against tampering and physical attacks, making it harder for malicious actors to compromise the module.

Full Compliance with FIPS

- makes it easier to demonstrate adherence to security standards.
- eases audit burdens.
- avoids penalties.
- enriches customer confidence.

Widely Deployed across the Patton SmartNode and Tone Commander product portfolio, which includes hundreds of networking and telephony (VoIP/SIP) products.

Conclusion

All users should understand the value of security awareness and the need to make information security a priority for management. **Organizations** should identify their information resources and assess their sensitivity to information loss and its potential impact. Because information security needs vary from application to application, the available controls cited in this paper should be selected based on probable risks.

List of FIPS 140-2 Compliant Patton Models

Ethernet Extenders	
CopperLink, CL1314	Long Range Ethernet Extender | up to 6 miles (10 km) over copper.
CopperLink, CL1314R	Industrial Grade, Long Range Ethernet Extender | up to 6 miles (10 km) over copper.
CopperLink, CL1314MDE	Ruggedized Multi-Drop Ethernet Extender & Repeater | up to 6 miles (10 km) over copper.
CopperLink, CL2300	Long Range-Bonding Wire-Bonding Ethernet Extender | up to 6 miles (10 km) over copper.
CopperLink, CL2300E	Industrial Grade, Long Range-Bonding Wire-Bonding Ethernet Extender | up to 6 miles (10 km) over copper.
G.SHDSL Products	
ForeFront, FF3310P	24 port wire bonding G.SHDSL DSLAM.
OnSite, OS2300	G.SHDSL.bis EFM CPE
OnSite, OS3300	G.SHDSL.bis Wire-Bonding EFM Router
Analog VoIP Gateways	
SmartNode, SN200	Analog Telephone Adapter (ATA) & VoIP Gateway
SmartNode, SN200R	Ruggedized Analog Telephony Adapter (ATA)
SmartNode, SN4140	Analog VoIP Gateway | 2, 4 or 8 analog ports for up to 8 phone or fax calls
SmartNode, SN4140E	Rugged Military-Grade Industrial VoIP Gateway | 2, 4 or 8 Analog Ports
SmartNode, SN4740	Analog High Density Gateway | 16 to 128 ports
ISDN VoIP Gateways	
SmartNode, SN4150	Analog & BRI VoIP Gateway | 2 BRI/2 FXS-FXO or 4 BRI/4 FXS-FXO ports for up to 8 phone or fax calls
SmartNode, SN4130	BRI VoIP Gateway | 2, 4 or 8 S0 ISDN ports for up to 16 simultaneous phone or fax calls
T1/E1 VoIP Gateways	
SmartNode, SN4170	PRI VoIP Gateway | One T1/E1/PRI interface for up to 30 simultaneous phone or fax calls

SmartNode, SN4970A	PRI VoIP Gateway | 1 or 4 T1/E1/PRI interface for up to 120 simultaneous phone or fax calls
SmartNode, SN4980A	PRI VoIP Gateway-Router | 1 or 4 T1/E1/PRI interface for up to 120 simultaneous phone or fax calls
SmartNode, SN5570	eSBC + Router | 1 or 2 T1/E1/PRI interface for up to 30 simultaneous phone or fax calls
Session Border Controllers (eSBCs)	
SmartNode, SN500	Low Cost eSBC for SME/SOHO | 2x 10/100/1000 up to 30 SIP sessions
SmartNode, SN5300	eSBC + Router + IAD | Up to 60 SIP Sessions with optional G.SHDSL
SmartNode, SN5480	eSBC + Router | Up to 64 Transcoded Calls
SmartNode, SN5490	eSBC + Router + IAD | Up to 60 SIP Sessions with optional G.SHDSL, ADSL/VDSL, X.21, Fiber
SmartNode, SN5500	eSBC + Router | 2 Ethernet ports for up to 200 SIP to SIP calls
SmartNode, SN5530	eSBC + Router | 2 to 8 BRI ports for up to 16 simultaneous phone or fax calls
SmartNode, SN5540	eSBC + Router | 2, 4 or 8 analog ports for up to 8 phone or fax calls
SmartNode, SN5550	eSBC + Router | 2FXS/2S0 or 4FXS/4S0 ports for up to 8 phone or fax calls
SmartNode, SN5570	eSBC + Router | 1 or 2 T1/E1/PRI interface for up to 30 simultaneous phone or fax calls
SmartNode, SN5600	Session Border Controller | 2 Ethernet ports for up to 1000 SIP to SIP calls
SmartNode, VSN	Virtual CPE: Software SBC, IP Access Router and VPN Server
TSG & JITC Certified SIP Phones	
Tone Commander, 7810-TSG	TSG-6 SIP Phone, AS-SIP, 10 Lines with PoE.
Tone Commander, TC7910-TSG	Tone Commander 7910-TSG TSG-6 SIP Phone with GigE and Fiber SFP Support, AS-SIP, 10 Lines with PoE
JITC Certified non-TSG SIP Phones	
Tone Commander, 4101	IP Phone, AS-SIP, Single Line with POE, Switched PC Port. TAA Compliant.
Tone Commander, 7810	SIP Phone, AS-SIP, 10 Lines with PoE.

Tone Commander, TC7910	Tone Commander 7910 SIP Phone with GigE and Fiber SFP Support, AS-SIP, 10 Lines with PoE
US Made Commercial Secure SIP Phones	
Tone Commander, TC7010	Tone Commander 7010 US Made Secure SIP Phone, 10 Lines with POE
Tone Commander, TC7110	Tone Commander 7110 US Made Secure SIP Phone with GigE/POE and Fiber SFP Support

www.patton.com

PATTON®
Let's Connect!™