

Ingrian Networks, Inc.

Federal Information Processing Standard (FIPS)

White Paper



INGRIAN
NETWORKS

INGRIAN NETWORKS AND FIPS

Introduction: Drivers of Market Opportunity

The demand for security on the Internet is increasing rapidly, driven by increasing frequency and severity of security breaches and the resulting financial and loss-of-privacy costs to businesses and consumers. According to IDC, secure traffic on the Internet is expected to reach 33% of overall traffic by 2004. This increase is significant given that total Internet traffic is growing exponentially. Businesses are increasingly using the Web to provide more products and services, enlarging their customer base and improving their bottom line.

A number of federal regulations govern the implementation of security standards for several business sectors. For instance, financial and healthcare businesses must comply with data privacy and security requirements set by GLBA (Gramm-Leach-Bliley Act) and HIPAA (Health Insurance Portability and Accountability Act). These acts require companies to bolster the security of their network infrastructure to ensure the safety and privacy of confidential data. In the past, the focus of security innovation was limited to protecting data in transit across the network, but given the increase in hackers' attacks to backend databases, the focus is quickly expanding to include the protection of data at rest, or data stored in backend servers and databases.

Secure Sockets Layer (SSL) is the de-facto protocol for securing traffic over the Internet. In certain markets, including financial services, over 75% of the Web traffic is encrypted. Cryptography is used to secure the data in transit. In addition, cryptography is used to secure the data in backend databases, and various types of authentication and authorization schemas are employed to protect data and network resources. Every cryptographic algorithm uses a key for encryption of data. The SSL protocol relies on the use of public and private keys to authenticate the sender and receiver of messages or transactions and protect the data in transmission.

The integrity of any security system is based on protection of the keys, integrity and robustness of the key generation, and reliability of the device that provides the security. To ensure that the sensitive data exchanged and stored as a result of confidential transactions, companies must implement additional levels of security beyond those provided by the SSL protocol.

There are number of vendors who claim to have products providing security. However, the claims may not have been verified by an independent body. This is where regulatory validation performs an important role in helping companies sort through vendor claims and qualify products.

This paper provides a brief overview of the FIPS 140-1 standard and explains how the secure networking products of Ingrian Networks have achieved compliance for this strict security standard for key management.

What is FIPS?

Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS). In the absence of voluntary industry standards, NIST develops FIPS when there are compelling Federal government requirements for computer security and interoperability.

FIPS 140-1 establishes the security requirements for cryptographic modules. In order for a cryptographic product to be marketable to the United States government, it must be evaluated and certified as meeting this standard. Given the absence of an industry standard, many companies and other governments seek products that are validated for FIPS 140-1 standard.

This provides them with the assurance of top-flight, validated security and competitive advantage. Protection of a cryptographic module within a security system assures the confidentiality and integrity of information protected by the module.

FIPS 140-1 covers areas related to the secure design and implementation of a cryptographic module. These security areas include physical security, self-tests, cryptographic algorithms and authentication. Each area is evaluated at validation levels one through four (1 is lowest, 4 is highest) with the overall level of the module equaling the lowest rating received. In terms of cryptographic algorithms, FIPS 140-1 requires that only FIPS-validated cryptographic algorithms be employed to provide security in a cryptographic module. These algorithms are specified in other FIPS (for example, FIPS 180-1 [FIPS95] specifies how SHA1 is to be implemented). Other non-FIPS-approved algorithms may be used as well, but as long as the FIPS validated algorithms are used, the product or module is validated for this standard.

NIST has developed a FIPS 140-1 approval program called the Cryptographic Module Validation Program (CMVP) that enables vendors of security products to submit their cryptographic modules to be tested by NIST-accredited laboratories for conformance to FIPS 140-1. Certificates are issued to indicate the security level that a vendor's product achieves, but if the software in the module is changed, the module must be revalidated.

FIPS 140-1 specifies 11 security areas that must be met by a cryptographic module used inside a security system that protects unclassified information such as medical records, tax information, personnel records, etc.—information that needs to be protected during transmission or storage.

These areas include:

- ?? Cryptographic Module Design and Documentation
- ?? Module Interfaces
- ?? Roles and Services
- ?? Finite State Machine Model
- ?? Physical Security
- ?? Software Security
- ?? Operating System Security
- ?? Cryptographic Key Management
- ?? Cryptographic Algorithms
- ?? Electromagnetic Interference/Electromagnetic
- ?? Compatibility (EMI/EMC)
- ?? Self Tests

Vendors of security products who submit their products for CMVP testing will receive a security rating from 1 to 4 for the areas listed above. The cryptographic module itself will also receive a single overall rating between 1 and 4.

FIPS 140-1 sets out to achieve a means of defining the structure of cryptographic modules in computer and telecommunications systems. A cryptographic module can be hardware, firmware or software that carries out cryptographic functions like encryption, decryption, digital signatures, authentication techniques or random number generation. Within a security product, cryptographic modules encrypt and decrypt data, authenticate users' identities and rely on digital signatures, private key management and other services. Independent testing labs assign a security level rating depending on how many FIPS 140-1 requirements the cryptographic module meets. The higher levels encompass the lower levels. That is, a Level 4 certified device meets all Level 1, 2 and 3 requirements.

Basically, the levels require:

Level 1: The lowest level of security. No physical security mechanisms are required in the module beyond the requirement for production-grade equipment.

Level 2: Tamper-evident physical security or pick-resistant locks. Level 2 provides for role-based authentication. It allows software cryptography in multi-user timeshared systems when used in conjunction with a C2 or equivalent trusted operating system.

Level 3: Tamper resistant physical security. Level 3 provides for identity-based authentication.

Level 4: Physical security provides an envelope of protection around the cryptographic module. Also protects against fluctuations in the production environment.

Benefits to a customer:

Customers benefit significantly by selecting a FIPS 140-1 validated product. They are assured that they are purchasing a product that:

- ?? Is built to adhere to strict security standards developed by NIST and issued by the US government.
- ?? Has security features validated by an independent third party.
- ?? Substantiates the security level claims made by the vendor.
- ?? Provides protection in areas that are not covered by traditional security products like firewalls or IDS.

Ingrian Networks secure networking device meets FIPS 140-1 Level 2 Certification Requirements for Key Management

The Ingrian Networks secure networking products protect data in transit and in storage. For secure networking products that perform cryptographic operations, the following areas are the most relevant:

- ?? Physical security of the keys
- ?? Cryptographic algorithms
- ?? Cryptographic key management
- ?? Roles and services

Today, there are a number of network devices that try to address the problems associated with secure traffic (SSL) by adding hardware cards. When security is added as an afterthought, it can be difficult to ensure that software defects or physical accessibility of the network devices are not allowing keys stored in them to be accidentally or maliciously disclosed. This issue is critical because any compromise of the private keys could result in eavesdropping and spoofing of legitimate Web identities. Failure to protect the keys could also result in data theft, loss of privacy, and damages to brand credibility and customer confidence. A thief with your private key could conduct fraudulent business in your name.

This is why Ingrian Networks secure networking products are designed with built-in FIPS level security. The Ingrian secure networking products feature multi-layered protection for private keys and fine-grained access control of the keys within the network security infrastructure. With the Ingrian device, private keys are stored in encrypted form within a tamper-resistant hardware security module (HSM). Keys stored in tamper-resistant HSM are protected from logical attacks and cannot be stolen by stealing the card itself.

In contrast to typical network configurations where private keys are stored insecurely on multiple Web servers, Ingrian devices protect the private keys in our hardware with multi-level security perimeters. The Ingrian Networks products use cryptographic algorithms that are FIPS validated for encryption of the keys and data. This is accomplished by using a FIPS validated cryptographic module.

Smart Card Based Key Management and Recovery

In the secure networking product from Ingrian Networks, private keys are stored internally inside tamper-resistant cards. The product encrypts private keys using a key known only to a small, predefined group of Ingrian Networks devices. These group keys are transported and backed up by smart cards. If a backup file was created on one of this small group of Ingrian devices, then only an Ingrian device that is part of this predefined group of Ingrian device can reload the backup file. The device also supports k -out-of- n secret sharing of the group key for increased security.

This means that the Ingrian device requires smart cards for backup and restoring of the private keys. For example, if the key information is distributed across a group of five smart cards (n), preferences can be set so that group data can be accessed after inserting three smart cards (k) into the smart card reader. Any attempt to access the data with less than three smart cards will fail. Using a k of n schema ensures data safety. If a single card is stolen, the thief will not be able to access the configuration data stored on the tamper resistant card because the thief does not have enough cards to meet the k of n criteria set above.

Secure Key Backup

A weak link in the security of many networks is the backup process. Often, private keys and certificates are archived along with the data from the backend Web servers. The backup files may be stored in a clear text file protected only by an administrator's password. A hacker could launch a simple dictionary attack and obtain the private keys and certificates.

Ingrian Networks has designed a secure backup system where:

- ?? Private keys are never exported from the device in clear text.
- ?? The backup file is password protected and then encrypted using an internal Ingrian key.

The Ingrian key makes it impossible for a dictionary attack to expose an administrator's password.

Secure Role-Based Management and Administration

Ingrian Networks devices allow customized security procedures to be established and enforced for accessing the devices based on roles and functions. Individual administrators can be authorized to perform specific duties, such as network management, security and back-ups. Each administrative function can be protected by a separate password, thereby limiting security risk to the entire network.

Remote administration via the Web interface is secured with 128-bit encryption via SSL to protect administrator commands. Advanced users can use the command-line interface, protected via a Secure Shell connection. For increased security, remote administration can be disabled, either globally or granularly.

Administrators can generate and manage certificates through the Web or command-line interface, reducing the chance of error. To easily manage a large number of keys, the interface provides for convenient key lifecycle management—for secure creation, storage, importing, back up, restoration, and removal—for a variety of applications.

Secure Architecture

In addition to the security design requirements of FIPS 140-1, the Ingrian Networks products have a number of other security features.

- ?? The products use common design principles for security systems such as well-defined security perimeters (often called “security rings”). The objective here is to ensure that attackers who succeed in breaching one or more security perimeters are still severely limited in the damage they can inflict.
- ?? The components of the system are partitioned and have separate management facilities. Placing partitions between the components of complex security systems considerably strengthens such systems. Consequently, a compromise of a single component minimizes the likelihood of unauthorized access to of the entire system.
- ?? Ingrian Networks devices runs a hardened security operating system. The following are some of the characteristics of its hardened operating system:
 - ?? A stripped down operating system with no unnecessary services. Security risks generated by the various services running in the background have been reduced. All non-essential services and executables have been removed from the devices.
 - ?? No standard shell on the devices. The only shell is Ingrian Networks’ own proprietary command line interface.
 - ?? Built-in defense against Denial of Service (DoS) overloads such as SYN floods.
 - ?? Read-only file system to prevent accidental software changes. This is another feature for minimizing operator error.

For more details on the security architecture of the Ingrian Networks device, refer to the “Ingrian Security Architecture” white paper.

Summary

Since its inception, Ingrian Networks has recognized the need for FIPS compliant cryptographic module within its secure networking products. With Ingrian Networks, customers can meet the stringent security requirements of FIPS. By purchasing an Ingrian Networks product, customers lower their security risk and protect valuable corporate assets and customer information. Importantly, Ingrian Networks’ customers will realize these benefits without any loss in performance or availability of their secure network.

Ingrian Networks is currently the only vendor who provides devices with FIPS validated key management for secure networking that also integrate security, caching and switching. Due to the device’s extensibility, customers can deploy new secure services and secure their existing Web applications easily at a low cost of ownership.

For more information on Ingrian Networks, please visit www.ingrian.com or call us toll-free at 866-464-7426.