Netop

NETOP™
RemoteControl
Secure Remote Management and Support

FIPS ENCRYPTION Standards

Concerned about security compliance for your remote access solution?
Here is how Netop helps you meet even the toughest standards.

What are FIPS?

The Federal Information Processing Standards (FIPS) publications are guidelines that set best practices for software and hardware computer security products to support The Federal Information Security Management Act (FISMA)

Why are FIPS important?

In many situations, U.S. government agencies can only purchase FIPS-compliant products.

This is true for almost every federal agency, with the exception of the military and the CIA, which often have more extensive security practices. Many private companies are required by U.S. government regulation to use FIPS-compliant products. For example, the Controlled Substances Ordering System (CSOS) regulations (regulations on electronic ordering of controlled substances) require FIPS standards for wholesale, health-care and pharmaceutical companies.

Canada, Australia and several other European countries also require FIPS compliancy.

Many private financial companies require FIPS-compliant products. ANSI and ISO are working through the process of adopting some FIPS publications. Some large companies are starting to take the approach that all security products must be FIPS-compliant and that they are always used in FIPS mode.

NIST

The FIPS publications are created by the National Institute of Science and Technology (NIST).

NIST is a non-regulatory federal agency within the U.S. Department of Commerce with approximately 3,000 employees and an estimated annual budget of $771 million. NIST works with the industry to develop and apply technology, measurements and standards.

What does “FIPS Mode” mean?

Products that support one or more FIPS standards can be set into a mode where the product only use FIPS approved algorithms and methods. In other words, security toolkits typically support both FIPS approved and non-FIPS approved functions. In FIPS mode, the product is incapable of using any non-FIPS approved methods.

Netop Remote Control runs in FIPS mode by default.

Key FIPS Standards

- 140-2 standard for Security Requirements for Cryptographic Modules
- 180-3 Secure Hash Standard SHA-1 plus SHA-256, SHA-384, SHA-512
- 197 Advanced Encryption Standard (AES)
- 198-1 The Keyed-Hash Message Authentication Code (HMAC)

Algorithms used by Netop Remote Control

TYPE	ALGORITM	FIPS 140-2 APPROVED
Key Exchange	Diffie-Hellman	Yes - SP 800-56 A
Symmetric Key	AES (Key sizes: 128-256)	Yes – FIPS 197
Digest	SHA-1 SHA-256 SHA-512	Yes – FIPS 180-3 Yes – FIPS 180-3 Yes – FIPS 180-3
Message Authentication Code	HMAC SHA-1 HMAC SHA-256 HMAC SHA-512	Yes – FIPS 198-1/FIPS 180-3 Yes – FIPS 198-1/FIPS 180-3 YES – FIPS 198-1/FIPS 180-3

continued >>

Encryption

Data transmitted between Windows, Linux, Solaris and Mac OS X modules can be encrypted using the Advanced Encryption Standard (AES – FIPS 197) with key lengths up to 256-bits.

Integrity and Message Authentication

Verified using the Keyed-Hash Message Authentication Code HMAC SHA-1 (FIPS 198-1/FIPS 180-3) or HMAC SHA-256 (FIPS 198-1/FIPS 180-3) based on the Secure Hash Standards SHA-1(FIPS 180-3) or SHA-256 (FIPS 180-3).

Key exchange

Encryption keys for encrypted data transmissions are exchanged using the Diffie-Hellman method (SP 800-56 A) with key lengths up to 2048 bits and up to 256-bit AES (FIPS 197) and up to 512-bit SHA HMAC (FIPS 198-1/FIPS 180-3) verification.

RSA CERTIFIED

www.netop.com/secure