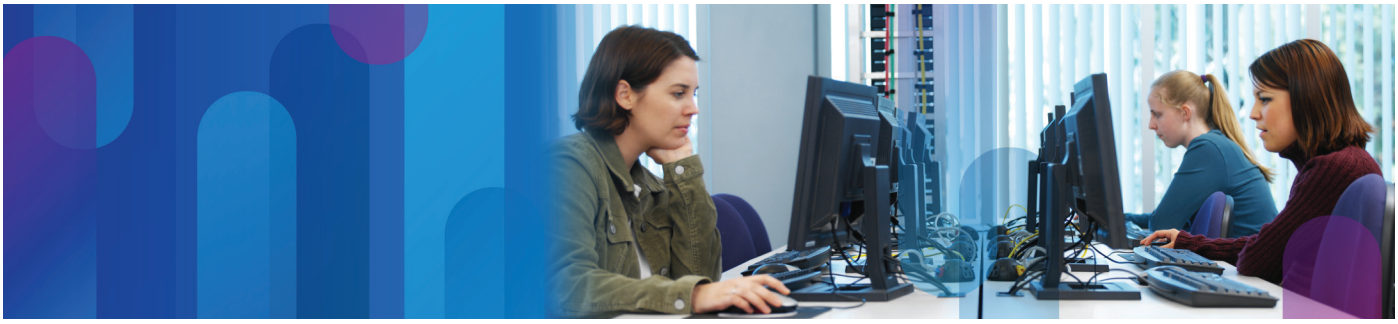
Cisco Next-Generation Cryptography: Enable Secure Communications and Collaboration



What You Will Learn

The Suite B set of cryptographic algorithms has become the preferred global standard for ensuring the security and integrity of information shared over non-trusted networks. This white paper, intended for public sector IT professionals, explains that:

Powerful benefits

- Suite B combines four well-established public domain cryptographic algorithms
- The Internet Engineering Task Force (IETF) has established open standards for commercial products using Suite B, helping organizations adopt it with confidence
- Cisco has introduced an IPsec-based implementation of Suite B cryptography in its VPN products

Opportunity: Secure Collaboration Over Public Networks

In 2005, the U.S. National Security Agency (NSA) identified a set of cryptographic algorithms that, when used together, are the preferred method for assuring the security and integrity of information passed over public networks such as the Internet. The NSA called the set of algorithms "Suite B." Today, Suite B is globally recognized as an advanced, publicly available standard for cryptography. It provides a security level of 128 bits or higher, significantly higher than many commonly used standards.

Integrated into IETF standards, Suite B algorithms make it easier to collaborate in environments where costs or logistics traditionally hindered information sharing. Secure sharing of information over the Internet and other non-trusted networks supports a variety of missions at all levels of government. For example, intelligence agencies can rapidly transmit information to state and local governments for improved disaster response. Military troops can share information in the field with a higher level of assurance that the data will not be tampered with or decrypted. And in the private sector, companies can increase the security of transmitting sensitive content such as intellectual property or private customer and employee information.

Another advantage of Suite B is that it helps public and private sector organizations meet compliance requirements, including Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Processing Standards (FIPS), and others.

What Is Suite B?

As described in RFC 4869, Suite B cryptography secures information travelling over networks using four well established, public-domain cryptographic algorithms:

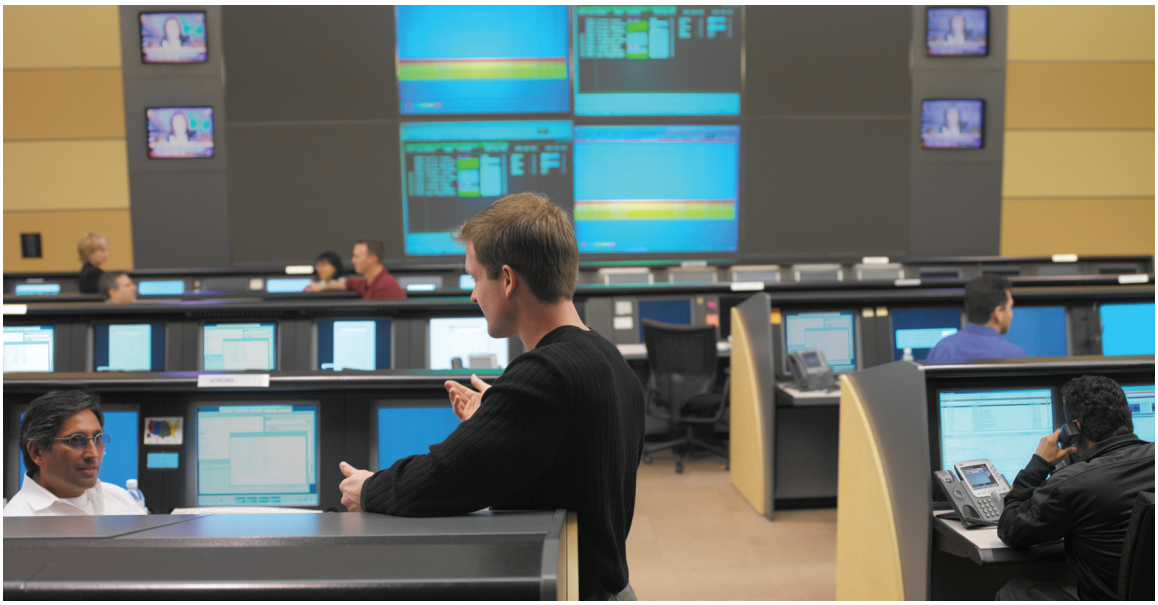
- Encryption based on the Advanced Encryption Standard (AES) using 128- or 256-bit keys
- Digital signatures with the Elliptic Curve Digital Signature Algorithm using curves with 256- and 384-bit prime moduli
- Key exchange, either pre-shared or dynamic, using the Elliptic Curve Diffie-Hellman method
- Hashing (digital fingerprinting) based on the Secure Hash Algorithm-2 (SHA-2)

The NSA has stated that these four algorithms in combination provide adequate information assurance for classified information. NSA Suite B cryptography for IPsec has been published as standard in RFC 4869, and has gained acceptance in the industry.

Commercial Suite B devices do not require the special handling requirements traditionally associated with government-specific cryptographic devices. This simplifies adoption, strengthens the overall architecture security, and minimizes operational costs.

Confidence in Commercial Suite B Products

To confidently adopt Suite B, public and private sector organizations need assurance about the integrity of the cryptographic algorithm deployed, the stability of the platform performing the cryptography, and interoperability with other agencies' Suite B–compliant products. To provide this assurance, commercial products that support the Suite B algorithms are subject to the same compliance and certification requirements as traditional IPsec products, including FIPS and Common Criteria. Organizations that use Suite B products validated by a certification or compliance program can have confidence in the integrity of the information they are transmitting and the stability of their platforms. They also benefit from ongoing global technology innovation stimulated by open standards.



Suite B: Natural Evolution of Cryptography

Suite B–compliant solutions are a natural evolution for Cisco, which has a 20-year history of innovation in cryptography (Table 1).

Cisco has long been committed to the success of Suite B and the use of efficient and secure cryptographic methods. Since 2004, Cisco led the design and standardization of the Galois/Counter Mode (GCM) of operation for AES that is used for symmetric encryption in Suite B. GCM provides both confidentiality and authentication, and is efficient even at very high data rates, above 1 Gbps. More recently, Cisco contributed to standards on practical implementation methods of the Elliptic Curve Cryptography (ECC) algorithms that provide the public key cryptography for Suite B.

Table 1 – Evolution of Cryptology in Cisco Solutions
Suite B technologies are shown in blue.

Encryption	Digital Signature	Hashing	Key Exchange
Cisco Encryption Technology	Short RSA Keys	MD5	Diffie-Hellman
IPsec: 56-bit Digital Encryption Standard (DES)	2048-bit RSA Keys	SHA-1	Elliptic Curve Diffie-Hellman (using P-256 and P-384 curves)
168-bit Triple DES (3DES)	Elliptic Curve Digital Signature Algorithm	SHA-256	
128-bit AES (Galois/Counter Mode [GCM] and Galois Message Authentication Code [GMAC])		SHA-384 and SHA-512	
256-bit AES (GCM and GMAC)			

By integrating Suite B cryptography standards into its VPN products, Cisco has taken the first step to using the network as the platform for Suite B information assurance. Organizations that use Cisco solutions for Suite B gain additional security, scalability, and operational efficiencies not available in Suite B products from other vendors.

For example, Cisco IOS® Software is well-proven, currently operating on millions of active systems. It includes built-in security technologies such as the IPsec standards, as well as integrated solutions that build on top of those standards, such as Dynamic Multipoint VPN (DMVPN). Both IPsec and DMVPN can use Suite B cryptography to provide strong data authentication, data confidentiality, entity authentication services, and anti-replay services.

By using IPsec in combination with other Cisco IOS Software capabilities, agencies can build VPNs that are secure, reliable, and able to prioritize latency-sensitive traffic, such as voice and video. The latter capability enables government agencies to build "medianets"—networks optimized to deliver an excellent video experience. Organizations with medianets can use Suite B to conduct classified voice and videoconferences.

"Open and freely implementable cryptography standards are indispensable to global information security. By not asserting patent rights with the Galois/Counter Mode of operation, Cisco has taken an active role in helping Suite B standards remain open."

David McGrew
Cisco Fellow

Currently Available Suite B-Compliant Solutions

Second-generation Cisco® Integrated Service Routers are the first Cisco products supporting Suite B cryptography. These routers support a variety of VPN architectures, including site-to-site, remote-access, and DMVPN. Integrating Suite B requirements into commercially available products is part of Cisco's commitment to enabling borderless collaboration between public and private sectors, anytime, anywhere.

For More Information

To learn more about Cisco Integrated Service Routers supporting Suite B cryptography, visit http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_vpn_ipsec.html.

To read about other Cisco solutions for federal government, visit www.cisco.com/go/federal.

To arrange a demonstration of Cisco technologies at a Cisco Center of Excellence, contact your local Cisco account team.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**