Envisioning the Future of Secure Communications

Using Suite B Cryptography to Increase Collaboration, Save Time, and Optimize Budgets

Table of Contents

List of Figures

Overview

The U.S. Federal Government manages many of the most sophisticated communications networks in the world, and within those networks, agencies create, share, and protect vital national security information. Historically, these systems have been designed and deployed to meet the stringent and specific requirements prescribed by the National Security Agency/Central Security Service (NSA/CSS), whose primary mission is to lead the Federal Government's programs for cryptology and secure computer network operations "to gain a decision advantage for the Nation and our allies under all circumstances."[1]

During the 60 years NSA has been in operation, most of the cryptologic devices—even those in place today—were purpose-built for NSA use only. Before they can be trusted for use with live network traffic from U.S. military, civilian, and intelligence agencies, as well as traffic from allied forces around the globe, these government off-the-shelf (GOTS) devices require multiyear development, testing, and implementation phases. These devices are strictly controlled and functionally prohibit collaboration among those who do not have access to these proprietary devices, including allied and coalition partners, as well as law enforcement authorities in state, local, and tribal governments. These unpublished algorithms have been categorized as "Suite A" cryptography, and they are incorporated into tightly controlled "Type 1" encryption products which are exclusively sold to the U.S. Government.

Under the current operating model, national security officials are unable to introduce new, more powerful GOTS devices at a pace that keeps up with the rapid evolution of commercial technology. In response to user requirements for faster performance and more scalable systems, and given the built-in constraints associated with GOTS development, NSA has become increasingly focused on ways to introduce robust new commercial off-the-shelf (COTS) tools and techniques into its operating environments, while maintaining the utmost end-to-end system security. In early 2005, in an effort to explore proactive ways the Federal Government might leverage the many benefits of COTS, NSA announced the establishment of a new security protocol that opens the door to the deployment of innovative, yet secure, alternatives to single purpose GOTS encryption devices in the form of a new protocol named Suite B Cryptography.

What is Suite B Cryptography?

Suite B is a set of unclassified cryptographic algorithms, initially released by the NSA in 2005, to encourage industry investment in commercial communications security technology. NSA created Suite B as part of its Cryptographic Modernization Program, while preserving its unpublished Suite A algorithms which are employed to protect the most sensitive communications and authentication systems.

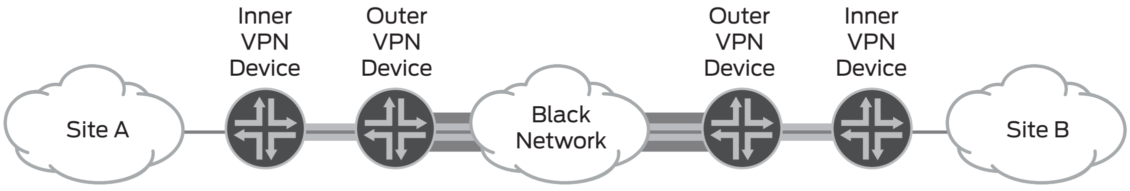
The National Information Assurance Glossary[2] offers the following definition for Suite B:

> *A specific set of cryptographic algorithms suitable for protecting both classified and unclassified national security systems and information throughout the U.S. Government and to support interoperability with allies and coalition partners.*

Suite B may be used to share Sensitive But Unclassified (SBU) information, as well as classified data at the Secret level or below, providing end users with more flexible, cost-effective, and COTS-based alternatives to the strictly controlled, and far more expensive, encryption devices that use Suite A algorithms.

It is worth noting that although designed to meet the rigorous protection requirements for national security information processing, Suite B Cryptography also has tremendous value for organizations beyond the law enforcement, intelligence, and Department of Defense (DOD) communities. Other public sector agencies, as well as security conscious commercial concerns, may choose Suite B to protect data stores of financial data, intellectual property, and other private information.

Suite B makes use of layered encryption that enables vendor neutral integration of diverse devices .[3]



Two IPsec tunnels protect data across a black network

Figure 1: Suite B layered encryption enabling vendor neutral integration

[1] NSA/CSS Mission Statement, www.nsa.gov/about/values/index.shtml
[2] The National Information Assurance Glossary, published by the Committee on National Security Systems, CNSS Instruction No. 4009; 26 April 2010, p. 74
[3] Diagram from p. 8 of the *Commercial Solutions for Classified (CSFC) Multi-Site Virtual Private Network Capability Package*, Version 1, August 17, 2012, published by the NSA Information Assurance Directorate

Essential Suite B components include:

- Advanced Encryption Standard (AES 128/256) for confidentiality/symmetric encryption
- Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signature
- Elliptic Curve Diffie–Hellman (ECDH) for key transport and agreement or exchange/establishment
- Secure Hash Algorithm 2 (SHA 256) for integrity/hashing

A summary of the *Approved Suite B Algorithms* (which are subcategorized into Suites 1 and 2) is published in the NSA Information Assurance Directorate's *Commercial Solutions for Classified (CSfC) Multi-Site Virtual Private Network Capability Package*.

Table 1: Approved Suite B Algorithms[4]

Security Service	Algorithm Suite 1	Algorithm Suite 2	Specifications
Overall level of security	128 bits	192 bits	
Confidentiality (encryption)	AES-128	AES-256	FIPS PUB 197
Authentication (digital signature)	ECDSA over the curve P-256 with SHA-256	ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-3
Key exchange/ establishment	ECDH over the curve P-256 (DH Group 19)	ECDH over the curve P-384 (DH Group 20)	NIST SP 800-56A IETF RFC 6379 Suite B Cryptographic Suites for IPsec (IKEv2)
Integrity (hashing)	SHA-256	SHA-384	FIPS PUB 180-4
Protection coverage	Up to Secret	Up to Top Secret	

Why Establish a Suite B Alternative?

NSA established its Commercial Solutions for Classified (CSfC) program to leverage the benefits of rapidly emerging technologies for use with classified data used by National Security Systems (NSS). There are numerous advantages to be gained by the U.S. Government from developing metho ds that allow for the use of COTS hardware and software wherever possible. Agencies stand to benefit from significant potential cost savings in product development, replacement, and maintenance. Equally important, the time to field new commercially-based products is substantially faster than that for proprietary or controlled government technologies.

One of the compelling arguments for using Suite B Cryptography is the opportunity it provides for improving collaboration between government agencies, allies, and across jurisdictional boundaries. Because Suite B relies on affordable COTS devices that are not Controlled Cryptographic Items (CCI)[5], a much broader community of partners are able to use this method for sharing controlled or classified information in a timely and secure manner. By removing the barriers to collaboration that traditionally have been included in the security management requirements of encryption devices using Suite A algorithms, Suite B delivers critically important operational flexibility to:

- Federal agencies
- Law enforcement and other officials in state, local, and tribal governments
- Military coalition partners

How Suite B Solutions Compare to Suite A

Encryption devices using Suite A algorithms are certified by the NSA for use in securing Federal Government information that has been classified, and typically are called "Type 1" products or devices. The National IA Glossary[6] offers the following definition for a Type 1 product:

> *Cryptographic equipment, assembly, or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed. Developed using established NSA business processes and containing NSA approved algorithms. Used to protect systems requiring the most stringent protection mechanisms.*

[4] NSA Information Assurance Directorate's Commercial Solutions for Classified (CSfC) Multi-Site Virtual Private Network Capability Package (Version 1.0 issued August 17, 2012), page 22, *Approved Suite B Algorithms*

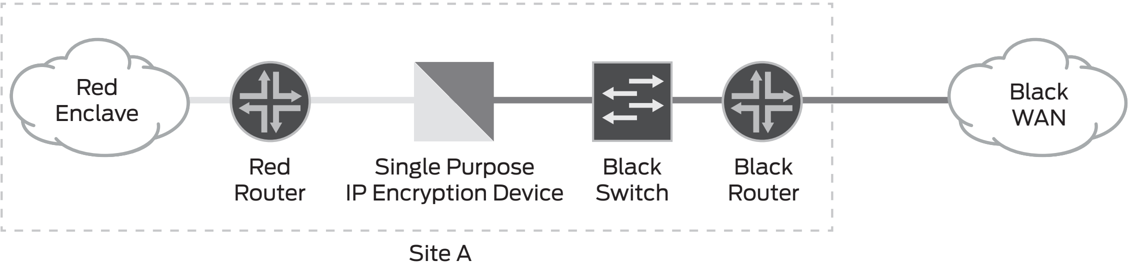
[5] Controlled Cryptographic Item (CCI)—Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements www.fismapedia.org/index.php?title=Term:Controlled_Cryptographic_Item

[6] The National Information Assurance Glossary, published by the Committee on National Security Systems, CNSS Instruction No. 4009; 26 April 2010, p. 81

Before a product is eligible to receive this certification, it must undergo rigorous testing and analysis to ensure the integrity and ability of the device to maintain the security standards set by NSA. As this can be an expensive and time-consuming process for the government and industry alike, the NSA has been motivated to identify a means for secure communications that does not require Type 1 certification for all classified processing.

Type 1 encryption environments generally are considered complicated and difficult to manage because the CCI requirements and processes for device and algorithm protection are significant. By comparison, given the ability to peel away the CCI constraints with Suite B, network managers are able to simplify device management and handling, as well as introduce new methods for seamless and significantly unencumbered information sharing.

The following diagram shows how a typical Type 1 encryption environment relies on a single purpose encryption device.



Type 1 encryption environment – multiple single purpose devices

Figure 2: Type 1 encryption environment

The following summarizes the distinguishing characteristics of Type 1 from Suite B cryptographic solutions.

Table 2: Key Characteristics Comparison—Suite A versus Suite B Cryptography

	Suite A (Type 1 Device)	Suite B (COTS Device)
Cryptographic algorithms	NSA unpublished/classified	IPsec/open standard
Key management	NSA approved	Public Key Infrastructure (PKI)
Handling restrictions	Yes, CCI	No
Classification protection	All levels	Up to top secret with the appropriate key lengths and NSA approval
Availability	Federal/federally sponsored	Commercial
Certification process	Multiyear review	One year or less
Certification	NSA	Federal Information Processing Standard (FIPS), National Information Assurance Partnership (NIAP)

(See Appendix 1, Table 3 for a feature-by-feature comparison of Juniper Networks' Suite B capable router versus the alternative single purpose Suite B encryptor.)

What Can Suite B Do For Your Organization?

Suite B solutions provide a cost-effective alternative for customers who today rely on standard Type 1 encryption devices. There are ***several fundamental cost savings opportunities with Suite B***, and the savings can be significant when compared to Type 1 encryption configurations:

- Reduced total cost of ownership (TCO) that comes with the use of COTS vs. GOTS hardware and software.
- Savings of CapEx and OpEx as Suite B is installed on singular, multifunction devices that deliver a number of network management and security services. (Type 1 devices provide encryption only, and additional devices are needed to provide additional network and security operations services.)
- Simpler network operations based on proven firewall, switching, routing, and VPN devices with encryption that meets Suite B standards.
- The reduced networking complexity and corresponding reduction in personnel training for network management and maintenance, as Suite B cryptography is standards-based and resides on familiar commercial devices.
- Network maintenance that is greatly simplified, as Suite B functionality does not rely on CCI devices and does not require the stringent handling, storage, and destruction associated with Type 1 encryptors.
- Opportunities for network innovation, collaboration, and additional functionality that are built into the COTS hardware and evolves with organizational infrastructures over time.

Common Sense Reasons to Consider Suite B Cryptography

Demonstrable Savings in Network Operating Costs

- Undeniable economies of scale are realized by moving to COTS devices—a primary driver for this new approach.
- Type 1 devices are purpose-built and approved for overlay security only; the COTS products that include Suite B cryptography are part of a multifunction device that is an embedded component in the overall network architecture.

Flexible, Innovative Network Architecture

- Additions and replacement of COTS-based devices can be accomplished with relative ease.
- Where GOTS products lag in innovation, performance, and scalability, COTS product development will continue to refresh and expand future product capabilities as part of its natural technical evolution.
- COTS-based Suite B devices can be tailored to meet the capacity and functionality of specific operational requirements, while Type 1 encryptors are available in only limited, predetermined configurations.
- Decreasing the number of government Type 1 devices in the network and replacing them with layered encryption offers more flexible architecture for today and tomorrow.

Why a Qualified, Trusted Partner Is Essential

Any organization managing classified information is keenly focused on information assurance and vigilant protection in accordance with national security requirements. For this reason, it is essential for Federal Government customers to implement effective Suite B encryption to provide trusted and tamper resistant mission-critical applications and communications. To do this, the commercial provider of Suite B solutions must have the consummate networking expertise to ensure that new devices function properly and reliably when they are installed into certified architectures processing classified data.

For this reason, Suite B implementation is best managed by proven networking professionals with an established track record of delivering compliant and certified technologies to support critical government missions. When evaluating options for secure networking partners, consider the following essential qualities to ensure successful outcomes:

- Networking is the primary business of the partner—not a secondary area of expertise
- Possesses personnel with an in-depth understanding of current Type 1 encryption requirements as well as an operating knowledge of Suite B functionality
- Ability to comply with security requirements for hardware and software—built into the current network devices
- Compliance with FIPS 140-2, Security Requirements for Cryptographic Modules
- Proven past performance in network technology engineering
- Reputation for optimized and secure network performance
- Ability to design and implement Suite B with existing network architectures to enable phased and staged introduction of this new technology

Future-Proofing Secure Network Operations—A Compelling Case for Suite B

The following schematic shows how a multifunction device with Suite B can decrease network complexity by eliminating single-use components with one multifunction device. The net effect of this single transformation is a significant reduction not only in initial capital investment—moving from GOTS to COTS—but an even more significant decrease in operations and maintenance over the device lifecycle.

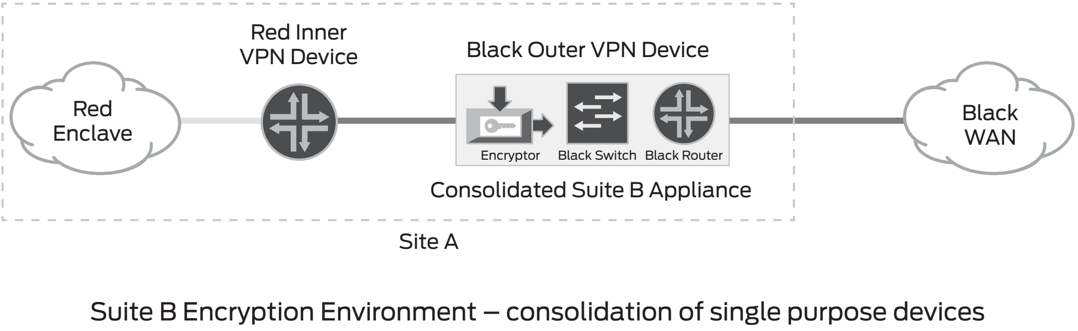

Red Inner VPN Device
Black Outer VPN Device
Red Enclave
Encryptor
Black Switch
Black Router
Black WAN
Consolidated Suite B Appliance
Site A
Suite B Encryption Environment – consolidation of single purpose devices

Figure 3: Suite B enables consolidation of single purpose devices

Having a trusted network technology partner deliver COTS-based networking appliances with Suite B embedded allows IT professionals to design secure network architectures, while consolidating hardware and dramatically reducing CapEx and OpEx.

Ready to Make the Change to Suite B?

There are no compelling technical reasons not to migrate towards a Suite B solution for processing classified information. In the near future, agencies using this type of national security data will be pushed to adopt this secure, available, and COTS-based technology. The primary reasons Suite B has not been adopted by some to date are: 1) Suite B is relatively new; and 2) many networking professionals are just now becoming familiar with the available products and the compelling arguments to use these COTS products for protection of sensitive traffic over established government networks.

For those agencies planning to migrate as part of an enterprise technology refreshment program, it is valuable to include Suite B capable devices along the way, so the option to use the technology is available when they are ready to make the move.

Evaluating Your Environment with Suite B in Mind

Technical professionals are ready to help—call toll-free 1-866-308-5692 or send your inquiry by e-mail to suiteb@juniper.net.

Appendix 1

Table 3: Leveraging Suite B Capable Routers for Multifunction Use—Single Purpose versus Multiuse Device Comparison

	Single Purpose Suite B Encryptor	Juniper Suite B Capable Router
Routing support	Static	BGP, IS-IS, OSPF/OSPFv3, RIPv1/v2, static
Interface support	Ethernet	Ethernet/serial/T1E1/DS3
Modular interfaces	No	Yes
Aggregate throughput	200 Mbps to 2 Gbps	65 Mbps to >100 Gbps
Management	Proprietary management system	CLI, WebUI, standard network management system (NMS) support
Single purpose appliance	Yes	No
Virtualization	No	VPN routing and forwarding (VRF), virtual routers, VLAN, Network Address Translation (NAT), LSYS, security zones
Ethernet switching	No	Yes
MPLS support	No	L2VPN, L3VPN, virtual private LAN service (VPLS), RSVP, circuit cross-connect (CCC), translational cross-connect (TCC)
Multicast support	No	Yes
Quality of service (QoS) support	No	Yes
Policy-based VPN	No	Yes
Stateful firewall	No	Yes
Signature-based inspection	Deep inspection (DI)	Full intrusion prevention system (IPS)
High availability	No	A/A, A/P, redundant power supply

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701