



Suite B

Highly Secure Collaboration over Wireless Networks

Benefits of Suite B:

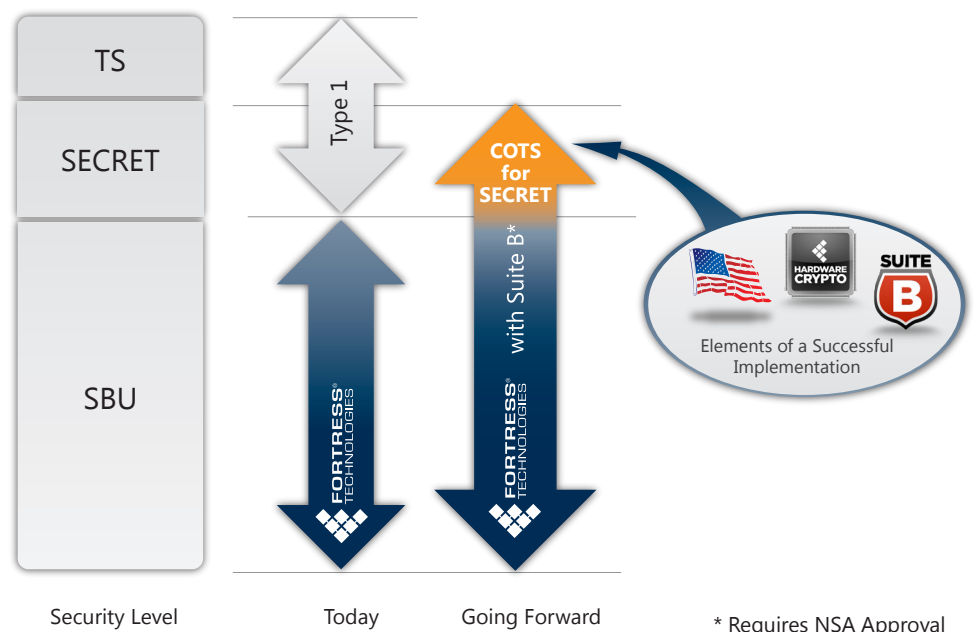
- COTS products reduce complexity and cost of deployment
- Globally recognized, publicly available standard for cryptography
- Supports inter agency and international collaboration through crypto interoperability
- Security of AES 128 or higher, significantly higher than commonly used standards

The transmission of classified information over any communications infrastructure introduces vulnerabilities if the information can be extracted, and wireless networks are perceived to be particularly vulnerable. Methods of protecting sensitive information of different levels have been developed and are implemented by defense and security bodies worldwide. These involve cryptographic algorithms in conjunction with stringent regulation. Legacy U.S. information assurance was based on Type 1 Products, highly regulated, validated, controlled and expensive components deployed to ensure privacy of classified information. In 2005, the U.S. National Security Agency (NSA) identified a set of public cryptographic algorithms that, when used together, are an acceptable method for assuring the security and integrity of information passed over public networks including wireless up to the SECRET level. The NSA called the set of algorithms "Suite B."

The secure sharing of information in the government security arena motivates the need for widespread cryptographic interoperability and the NSA initiative to approve products that meet appropriate security standards to protect classified information at the SECRET level is significant.

A Cryptographic Interoperability Strategy (CIS) was developed by the NSA to increase and assure rapid sharing of information both within the U.S. and with coalition partners through the use of a common suite of public standards, protocols, algorithms and modes.

The Commercial Solutions Partnership Program (CSPP) will enable the use of a combination of COTS information assurance products composed to form a particular application solution to protect information up to the SECRET level.





What is Suite B?

Suite B is part of a cryptographic interoperability strategy for protecting classified information. Suite B is based on a set of four well established, public-domain cryptographic algorithms and these four algorithms in combination provide adequate information assurance for classified information. Implementing Suite B will allow the layered use of COTS products that meet a robust set of security standards to protect information up to the SECRET level for classified networks, and removes the stringent handling and accountability requirements for a "Type 1" Controlled Cryptographic Item (CCI).

Open standards and the use of strong public algorithms also enable interoperability between agencies and allow DOD services, coalition partners or state and local governments to collaborate better.

Natural Evolution of Fortress Security Capabilities

Throughout the U.S. Federal Government and its coalition partners, an urgent and increasing demand for mission critical secure wireless communications is driving the need for economic, COTS-based solutions that will enable the disadvantaged user to get access to readily available information and capabilities like voice, data and video. Fortress provides this for our customers today, offering FIPS approved secure wireless products that are deployed to protect Sensitive but Unclassified (SBU)/Controlled Unclassified Information (CUI). With Suite B, Fortress' COTS-based wireless communication solutions can be used to extend the reach of the network as a common transport framework. By embracing the COTS Suite B architecture with appropriate NSA review and approval, Fortress extends the value of wireless to SECRET and below, enabling a much broader scale of classified communications.

	COTS	Fortress COTS+	Fortress COTS for SECRET	GOTS for SECRET	GOTS Type 1
Data Classification Enabled	Unclassified	SBU/CUI	SECRET	SECRET	SECRET/TS/SCI
Crypto Used	AES	AES	Suite B	Suite B	Suite A
Accreditation	None	FIPS	FIPS + CC (Device) + CSPP (Implementation)	NSA (Device)	NSA (Device)
Price Tag	Low	Medium	Medium	High	Very High
Use Restrictions	None	None	None	CCI or CHVP	CCI
Key Management	None	Commercial	Commercial/ Government	NSA Approved Source	NSA Approved Source

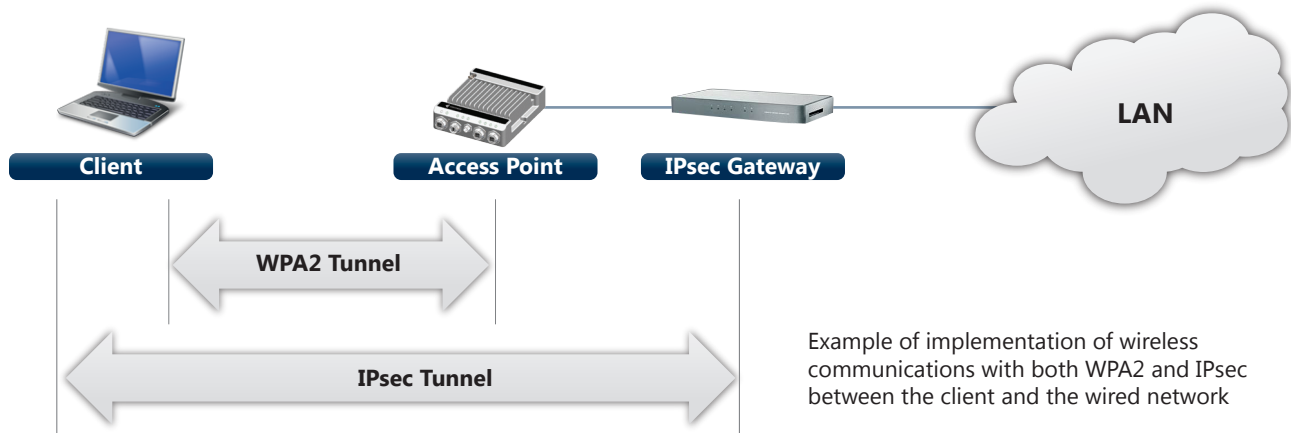
COTS for SECRET Requirements

The NSA guidelines for approval of wireless LAN implementations to support COTS for SECRET are still under development at the time this was written. It is expected the recommendations will involve a composite framework involving multiple components. To support this, Fortress solutions can implement secure 802.11 tunneling between a client and an access point using WPA2, as well as virtual private network (VPN) tunneling using L2TP and IPsec. These secure tunnels can run independently and interoperate with other vendors solutions to create multiple secure tunnels over the wireless link.

Unlike Type 1 or FIPS 140-2 where products are certified to meet a set of requirements, COTS for SECRET approval first requires the network architecture to be approved by the NSA. The actual implementation (specific solution) of composed products with FIPS and CC approval is accredited by a process simpler and faster than Type 1 accreditation.

Fortress Suite B enabled products have the following characteristics:

- Standards-based, Secure Sharing Suite (S3) compliant
- FIPS 140-2 and Common Criteria compliant
- Reconfigurable custom hardware crypto (FPGA)
- True Random Number Generator (TRNG)
- Trusted Platform Module (TPM)
- Designed and manufactured in the U.S.



Fortress Suite B Implementation

Fortress Mesh Points and client solutions implement Suite B cryptographic algorithms for IPsec as well as WPA2-EAP-TLS using hardware based crypto FPGA to implement high performance encryption and hardware TRNG that is critical to ensure security for devices that do not have other sources of entropy. By complying with interoperability standards as outlined by NSA's IPsec Minimal Essential Interoperability Requirements (IPMEIR), and meeting FIPS 140-2, Common Criteria, DODD 8100.2, and service based accreditation processes, the solution and products lend themselves to integration into a Suite B Accredited Implementation.

Suite B Going Forward

Fortress is an advocate and leader in implementing COTS Suite B Cryptography in support of the NSA's Cryptographic Interoperability Strategy as promoted by the Committee on National Security Systems Policy 15 (CNSSP-15). We continue to work closely with our customers to help them successfully leverage secure wireless communications across their operating environments and submit to the appropriate authorities for accreditation.

For assistance with developing security requirements and determining if Suite B is appropriate for your project, contact Fortress Technologies and your NSA liaison.

Specifications:

Suite B Algorithms

Confidentiality (Encryption)

Advanced Encryption Standard (AES) - FIPS PUB 197 (using key sizes of 128 and 256 bits)

Integrity (Hashing)

Secure Hash Algorithm (SHA) – FIPS PUB 180-3 (using SHA-256 and SHA-384)

Key Exchange / Establishment

Elliptic Curve Diffie Hellman (ECDH) - FIPS Special Publication 800-56A (using 256 and 384-bit prime moduli curves)

Authentication (Digital Signature)

Elliptic Curve Digital Signature Algorithm (ECDSA) - FIPS PUB 186-3 (using 256 and 384-bit prime moduli curves)

Suite B Protocols

IPMEIR

IPMEIR Version 1.0.0 Core
Elliptic Curve Cryptography Groups IPMEIR IS Version 1.0

IPsec

RFC4869:
IPsec using the Internet Key Exchange (IKE) or IKEv2: "Suite B Cryptography for IPsec"

TLS

RFC 5430:
"Suite B Cipher Suites for TLS"
RFC 5289:
"TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)"

Additional Information

http://www.nsa.gov/ia/programs/suiteb_cryptography/
<http://www.niap-ccevs.org>
<http://csrc.nist.gov/groups/STM/cmvp>
<http://www.cnss.gov>
<http://www.fortresstech.com/Technology-Article/suite-b.html>

Fortress Technologies

www.fortresstech.com
1.888.477.4822

© 2011 Fortress Technologies, Inc.
All rights reserved.