

# Suite B NSA Cryptography

## Protecting Government Communication

### Fortress Technologies and Suite B

The National Security Agency (NSA) announced Suite B cryptography at the 2005 RSA Conference. Suite B cryptography is intended to complement the existing policy for the use of AES to protect national security systems (CNSSP-15). The Suite B initiative is intended to provide industry with a common set of cryptographic algorithms that can be used to create products that meet the widest range of US Government needs. Suite B will allow vendors to deliver high-assurance security products to meet NSA approval for classified and unclassified use.

Until now, only Type 1 products are approved for classified use. Type 1 products can be burdensome because of their relatively high cost, the requirement that they only be operated by people with the appropriate security clearances, they are only available to U.S. government entities, and they have export restrictions associated with them. With prior NSA approval, Suite B products may be substituted for Type 1 products in certain applications.

### Suite B cryptography specifies use of the following algorithms:

- **Encryption:** AES-128 or AES-256, AES-256 selected by Fortress for interoperability, Defined in FIPS 197
- **Hashing:** SHA-256 or SHA-384, Defined in FIPS 180-2
- **Key Agreement:** ECC with the 256 and 384-bit prime moduli ECDH or ECMQV, Defined in NIST 800-56
- **Digital Signature:** Elliptic Curve Digital Signature (ECDSA), Defined in FIPS 186-2

While Suite B specifies the cryptographic algorithms to be used, many factors determine whether a particular device should be used to satisfy a specific requirement. These factors include:

- The quality of the implementation of the algorithm in software, firmware or hardware
- Operational requirements associated with U.S. Government-approved key and key management activities
- The uniqueness of the information to be protected (e.g. special intelligence, nuclear command and control, U.S.-Only data)
- Requirements for interoperability both domestically and internationally

## Product Datasheet



### Applications Include:

- Tactical use
- Sensor applications
- Federal cooperation with state/local agencies
- Coalition government

## Product Datasheet



Once these requirements are satisfactorily met, and NSA approval has been acquired, there are many potential applications that may be suitable for Suite B technology, including:

- Tactical use
- Sensor applications (e.g. bio/chemical sensors)
- Federal cooperation with state/local agencies (e.g. incidence response, natural disasters, terrorism)
- Foreign military or Coalition military use

Fortress Technologies' Mobile Security Protocol (MSP) is field upgradeable to Suite B mode. Fortress's Suite B implementation is notable for the following:

- Cryptography is hardware-based, improving speed and preventing side-channel attacks
- Fortress provides for True Random Number Generation
- Fortress products are field-upgradeable to Suite B security
- Fortress products are manufactured in the U.S.

### NSA Evaluation

The NSA may evaluate Suite B products on a case-by-case basis for use in protecting U.S. Government classified information. Suite B only specifies the cryptographic algorithms to be used; many factors determine whether a particular device should be used to satisfy a specific requirement:

- The quality of the implementation of the cryptographic algorithm in software, firmware or hardware
- Operational requirements associated with U.S. Government approved key and key-management activities
- The uniqueness of the information to be protected (e.g. special intelligence, nuclear command and control, U.S.-only data)
- Requirements for interoperability both domestically and internationally

**LTI DataComm**  
23020 Eaglewood Ct. #100  
Sterling, VA 20166  
[www.ltidata.com](http://www.ltidata.com)  
800-677-5050