>>Fact Sheet NSA Suite B Cryptography

Background:

The sustained and rapid advance of information technology in the 21st century dictates the adoption of a flexible and adaptable cryptographic strategy for protecting national security information. To complement the existing policy for the use of the Advanced Encryption Standard (AES) to protect national security systems and information as specified in The National Policy on the use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information (CNSSP-15), the National Security Agency (NSA) announced Suite B Cryptography at the 2005 RSA Conference. In addition to the AES, Suite B includes cryptographic algorithms for hashing, digital signatures, and key exchange.

The entire suite of cryptographic algorithms is intended to protect both classified and unclassified national security systems and information. Because Suite B is also a subset of the cryptographic algorithms approved by the National Institute of Standards, Suite B is also suitable for use throughout government. NSA's goal in presenting Suite B is to provide industry with a common set of cryptographic algorithms that they can use to create products that meet the needs of the widest range of US Government (USG) needs.

Suite B only specifies the cryptographic algorithms to be used. Many other factors need to be addressed in determining whether a particular device implementing a particular set of cryptographic algorithms should be used to satisfy a particular requirement. These include:

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

The process by which these factors are addressed is outside the scope of Suite B. Suite B focuses only on cryptographic technology, a small piece of an overall information assurance system.

Another suite of NSA cryptography, Suite A, contains classified algorithms that will not be released. Suite A will be used for the protection of some categories of especially sensitive information (a small percentage of the overall national security related information assurance market).

SUITE B includes:

Encryption:	Advanced Encryption Standard (AES) - FIPS 197 (with keys sizes of 128 and 256 bits) http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf*
Digital Signature:	Elliptic Curve Digital Signature Algorithm - FIPS 186-2 (using the curves with 256 and 384-bit prime moduli) http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf*
Key Exchange:	Elliptic Curve Diffie-Hellman or Elliptic Curve MQV Draft NIST Special Publication 800-56 (using the curves with 256 and 384-bit prime moduli) http://csrc.nist.gov/CryptoToolkit/kms/keyschemes-Jan03.pdf*
	Secure Hash Algorithm - FIPS 180-2

Hashing:	(using SHA-256 and SHA-384) http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf*

CNSSP-15 states that AES with either 128 or 256-bit keys are sufficient to protect classified information up to the SECRET level. Protecting TOP SECRET information would require the use of 256-bit AES keys[1] as well as numerous other controls on manufacture, handling and keying. These same key sizes are suitable for protecting both national security and non-national security related information throughout the USG.

Consistent with CNSSP-15, Elliptic Curve Public Key Cryptography using the 256-bit prime modulus elliptic curve as specified in FIPS-186-2 and SHA-256 are appropriate for protecting classified information up to the SECRET level. Use of the 384-bit prime modulus elliptic curve and SHA-384 are necessary for the protection of TOP SECRET information.

All implementations of Suite B must, at a minimum, include AES with 128-bit keys, the 256-bit prime modulus elliptic curve and SHA-256 as a common mode for widespread interoperability.

Testing, Evaluation and Certification of "Suite B" Products:

Creating secure cryptographic equipment involves much more than simply implementing a specific suite of cryptographic algorithms. Within the USG there are various ways to have cryptographic equipment tested or evaluated and certified. These methods include:

1. **The Cryptographic Module Verification Program (CMVP)** - this program, managed by the National Institute for Standards and Technology (NIST), tests cryptographic implementations at commercial laboratories both in the US and abroad. The testing process is derived from FIPS-140-2. Suite B products containing only cryptographic security functions may be evaluated and certified under this program. Certified products may be used to protect unclassified information throughout the USG, except national security systems. For further information on this program visit: http://csrc.nist.gov/cryptval/
2. **The Common Criteria Evaluation and Validation Scheme (CCEVS)** - this program, managed by NSA and NIST, tests information assurance (IA) products in accord with The Common Criteria for Information Technology Security Evaluation (CC), ISO/IEC 15408. Suite B Products that contain non-cryptographic IA functionality (i.e. firewalls, smart cards, operating systems etc.) should be evaluated under this scheme as well.[2] For further information on this program visit: http://www.niap-ccevs.org/cc-scheme
3. **Evaluation by the National Security Agency** - NSA will evaluate Suite B products for use in protecting classified information throughout the USG. Products accepted for evaluation would normally come into NSA through Traditional Procurements, the Commercial COMSEC Evaluation Program (CCEP) or User Partnership Agreements (UPA). Through these programs, NSA will not only evaluate a vendor's product but also provide extensive design guidance on how to make a product suitable for protecting classified information. Implementing Suite B is only one step in a complex process. For further information visit: http://www.nsa.gov/ia/industry/cep.cfm

For protecting unclassified national security information or systems, a Suite B product must be evaluated under the CMVP. If the product contains non-cryptographic information assurance functionality the product must also be evaluated under the CCEVS as well using an NSA approved protection profile.

For protecting classified information, a product must be reviewed and certified by NSA.

Intellectual Property:

A key aspect of Suite B is its use of elliptic curve technology instead of classical public key technology. NSA has determined that beyond the 1024-bit public key cryptography in common use today, rather than increase key sizes beyond 1024-bits, a switch to elliptic curve technology is warranted. In order to facilitate adoption of Suite B by industry, NSA has licensed the rights to 26 patents held by Certicom Inc. covering a variety of elliptic curve technology. Under the license, NSA has a right to sublicense vendors building equipment or components in support of US national security interests. Any vendor building products for national security use is eligible to receive a license from the National Security Agency. For

further information on Elliptic Curve Intellectual Property Licensing please contact the Business Affairs Office of the NSA/CSS Commercial Solutions Center. For further information visit: http://www.nsa.gov/ia/industry/cep.cfm

Key Management:

For key exchange, Suite B calls for the use of either an Elliptic Curve Diffie-Hellman Key Exchange (ECDH) or the use of a protocol called ECMQV[3]. ECDH is appropriate for incorporation of Suite B into many existing Internet protocols such as the Internet Key Exchange (IKE), Transport Layer Security (TLS), and Secure MIME (S/MIME). ECMQV is appropriate in many link and voice encryption applications.

We will encourage the development of commercial services to provide for Public Key Infrastructure support to the vast array of Suite B compliant products used in both government and commercially. Commercial standards will be used for the interface between devices and a commercial public key infrastructure. NSA will maintain an equivalent public key infrastructure to support Suite B products applications that need to receive key from a USG source.

---

[1] CNSSP-15 correctly states that 192-bit AES keys are sufficient for protecting even TOPSECRET information. However, Suite B uses only 256-bit keys to enhance interoperability.

[2] NSA will be involved in all CCEVS evaluations above EAL Level 4.

[3] This is the elliptic curve variant of the Menezes, Qu, and Vanstone (MQV) key exchange. NSA licensed the patents on MQV from Certicom for use in Suite B implementations.

[*] To view documents stored as Portable Document Format (PDF) files your local computer must have the Adobe Acrobat Reader application or a Web browser plug-in that supports the PDF file format.