XML Cryptographic Security and Suite B

Background:

The Department of Defense (DOD) through the leadership of the Defense Information Security Agency (DISA) is pushing forward to use the Extensible Markup Language (XML) as a key element of the DOD information sharing effort. The National Security Agency (NSA), in support of the DOD, is interested in seeing XML security evolve in a manner that provides extensive interoperability between XML systems and use cryptographic mechanisms that meet the stringent security requirements of the DOD.

The NSA has established a suite of cryptographic algorithms, drawn from published standards established by the National Institute for Standards and Technology (NIST), as a primary basis for DOD cryptographic security in the 21st century. This suite of algorithms has come to be called, "SUITE B." To promote interoperability among DOD elements and to maximize the DOD's ability to utilize commercial technology in satisfying their mission, NSA encourages all commercial vendors to incorporate Suite B in their products. In particular NSA would like to see XML standards emerge which support the use of Suite B.

Suite B Defined

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. Several years ago, the Committee for National Security Systems (CNSS) issued a policy stating that the Advanced Encryption Standard (AES) could be used to protect both classified and unclassified National Security information. However, because a single encryption algorithm could not satisfy all of the needs of the national security community, NSA created a larger set of cryptographic algorithms which could be used along with AES in the systems used by the DOD and other national security users. The NSA announced Suite B 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 NIST, Suite B is also suitable for use throughout the U.S. 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.

However, 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.

Today 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 NIST Special Publication 800-56A (using the curves with 256 and 384-bit prime moduli) http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf
Hashing:	Secure Hash Algorithm - FIPS 180-2 (using SHA-256 and SHA-384) http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

The original policy on AES use states that AES with either 128 or 256-bit keys are sufficient to protect classified information up to the SECRET level. In addition, other controls on manufacture, handling and keying are anticipated. These same key sizes are suitable for

protecting both national security and non-national security related information throughout the USG.

Consistent with this policy, 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 both the 384-bit prime modulus elliptic curve and SHA-384 is necessary for the protection of TOP SECRET information.

Intellectual Property on Suite B:

Associated with most cryptographic algorithms, even those found in standards, are patents on various ways of implementing the cryptography in particularly efficient or novel ways. Although there are some particular implementations of both the Advanced Encryption Systems and Secure Hash Algorithm that are patented, the basic algorithms are available worldwide for royalty free use.

Another key aspect of Suite B is its use of elliptic curve technology instead of classical public key technology. NSA has determined that rather than increase key sizes beyond today's current 1024-bits, a switch to elliptic curve technology is warranted.

Like the AES and SHA there are no fundamental patents on elliptic curve cryptography, however, there are a number of patents covering various aspects of elliptic curve technology and implementations. Certicom, the largest holder of elliptic curve patents, states on their company website that licensing their patents is not necessary for implementing elliptic curve cryptography. Rather, they state that they have patents on what they believe to be some of the "best ways to implement elliptic curve cryptography (ECC)."

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. While NSA offers vendors royalty free licenses for the use of these patents, NSA is not suggesting that licensing any of these patents or any other patents is necessary for implementing Suite B.

Conclusion:

To master the information space, DOD and the IC need to be able to share, analyze and secure vast amounts of information. In order to prevent all of the information in DOD networks from becoming a meaningless tower of babel, standards such as XML are critical. NSA would like to see security for XML evolve in a manner that supports the DOD's need for secure information sharing. To that end, NSA would like to see the adoption of Suite B cryptography as a security option for XML.