XML Cryptographic Security and Suite B

National Security Agency

25 September 2007

Key Point

The National Security Agency would like to see appropriate Suite B algorithms incorporated into XML Signature and XML Encryption.

The Case for Elliptic Curve Cryptography

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

NIST Recommended Key Sizes

The Case for Elliptic Curve Cryptography

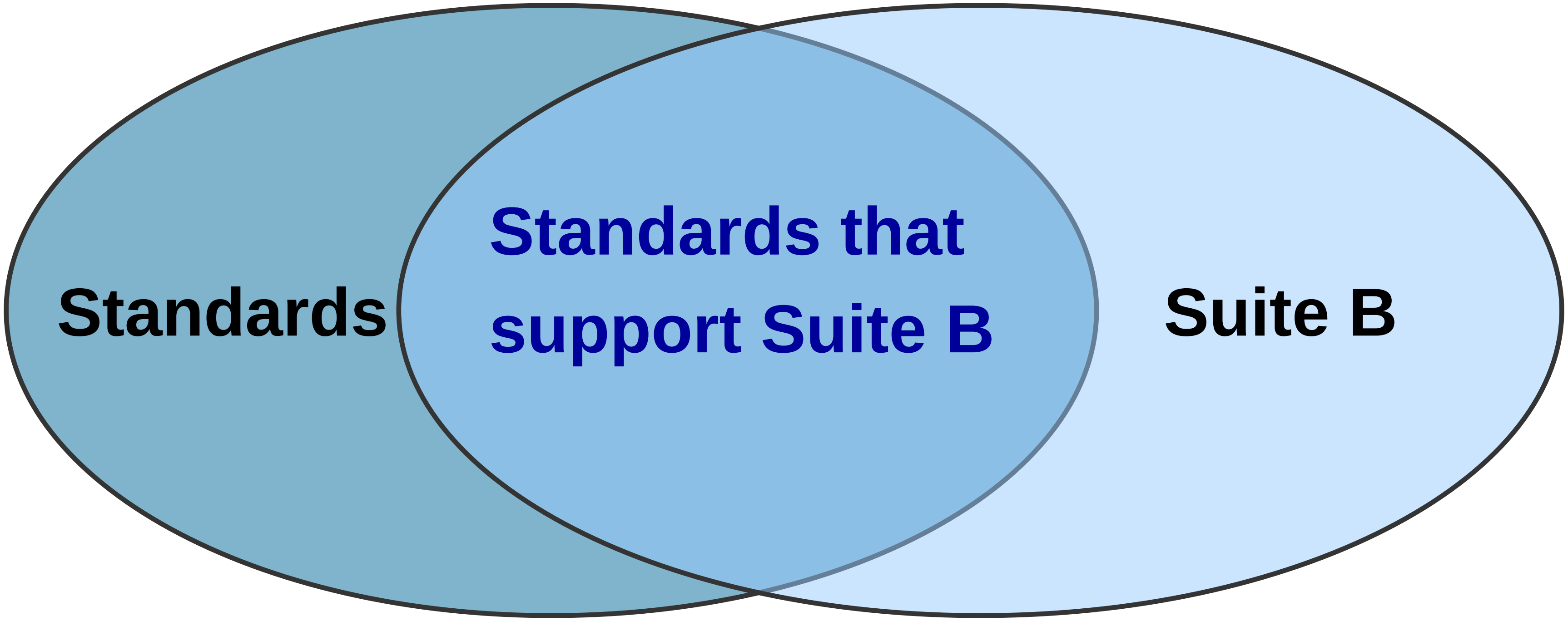
- In general, elliptic curve cryptosystems:
  - Offer more security per bit increase in key size than first generation public key systems.
  - Are more computationally efficient than the first generation public key systems.
  - Require less channel overhead to perform key exchanges and digital signatures on a communications link.

NSA’s Suite B

Suite B is comprised of:

Encryption	Advanced Encryption Standard (AES)	FIPS 197	Key sizes: 128 bits and 256 bits
Digital Signature	Elliptic Curve Digital Signature Algorithm (ECDSA)	FIPS 186-2	Curves: P-256 and P-384
Key Exchange	Elliptic Curve Diffie-Hellman	NIST Special Publication 800-56A	Curves: P-256 and P-384
	Elliptic Curve Menzes-Qu-Vanstone (ECMQV)	NIST Special Publication 800-56A	Curves: P-256 and P-384
Hashing	Secure Hash Algorithm	FIPS 180-2	SHA-256 and SHA-384

Suite B and Standards Convergence



- Current standards supporting Suite B include:
  - Suite B Cryptographic Suites for IPSec (RFC 4869)
  - Suite B Cipher Suites for TLS (Internet Draft)
  - Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME) (Internet Draft)

Next Steps

- Next steps for incorporating appropriate Suite B algorithms into XML Signature and XML Encryption could include, but are not limited to:
  - XML Signature
    - Signature Algorithms: Define ECDSA integration with XML Signature
    - Digest: Define SHA-256 and SHA-384 integration with XML Signature
  - XML Encryption
    - Key Agreement: Define ECDH integration with XML Encryption
    - Message Digest: Define SHA-384 integration with XML Encryption

Conclusion

Incorporation of appropriate Suite B algorithms into XML Encryption and XML Signature is an important next step.

Contacts

- ***NSA ECC license information:***
  - National Security Agency

    Attn: IAD Business Affairs Office

    9800 Savage Road, Suite 6740

    Fort Meade, MD 20755-6740
  - 410-854-6091
  - bao@nsa.gov

References

- FIPS 140-2, Security Requirements for Cryptographic Modules: http://csrc.nist.gov/cryptval/140-2.htm
- FIPS 197, Advanced Encryption Standard: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
- FIPS 186-2, Digital Signature Standard (Elliptic Curve Digital Signature Algorithm): http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
- Draft NIST Special Publication 800-56, Recommendation on Key Establishment Schemes (Elliptic Curve D-H or Elliptic Curve MQV): http://csrc.nist.gov/CryptoToolkit/kms/keyschemes-Jan03.pdf
- FIPS 180-2, Secure Hash Standard (SHA -256 and SHA-384): http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf
- NSA Suite B Fact Sheet: http://www.nsa.gov/ia/industry/crypto_suite_b.cfm