Suite B Interoperability

Suite B is a set of cryptographic algorithms intended to protect sensitive data communication and critical authentication systems. Suite B cryptography has been selected and approved by the National Institute of Standards and Technology (NIST) for use by the U.S. Government and specified in NIST standards and recommendations. Information on Suite B and the NIST Suite B standards and recommendations can be found at the following web site: http://www.nsa.gov/ia/programs/suiteb_cryptography/.

Suite B defines multiple levels of data security protection based on the sensitivity of the underlying data to be protected. These security levels are defined in NIST FIPS 140-3.

XML Signature 1.1 and XML Encryption 1.1 are normative specifications produced by the XML Security working group in the W3C. These specifications have required and optional normative statements on implementations, including ones related to Suite B support. The elements, algorithms, and methods marked as REQUIRED in XML Signature 1.1 and XML Encryption 1.1 support the lower NIST security levels; those marked as OPTIONAL support the higher NIST security levels.

Suite B's components are:

- Symmetric Encryption: Advanced Encryption Standard (AES) with key sizes of 128 and 256 bits. For data traffic, AES should be used with the Galois/Counter Mode (GCM) mode of operation
- Digital Signatures: Elliptic-Curve Digital Signature Algorithm (ECDSA)
- Key Agreement: Elliptic-Curve Diffie-Hellman (ECDH)
- Message Digest: Secure Hash Algorithm 2 (SHA-256 and SHA-384)

The XML Security requirements, including the Suite B components, are described in http://www.w3.org/2008/xmlsec/Drafts/xmlsec-reqs/Overview.html.

XML Signature 1.1 Suite B Implementations

All XML Signature 1.1 implementations are Suite B interoperable when they support all of the following Suite B algorithms or methods, as listed in the "Algorithm/Method" column, with their associated required values, as listed in the "REQUIRED" or "OPTIONAL" column, in the table below:

| Suite B Component | XML Signature 1.1 Element | Algorithm/ Method | REQUIRED in the XML Signature 1.1 specification | OPTIONAL in the XML Signature 1.1 specification |
|---|---|---|---|---|
| Signature | SignatureMethod | ECDSA | ECDSA-P256 with SHA-256: ECDSAwithSHA256 | ECDSA-P384 with SHA-384: ECDSAwithSHA384 |
| Key Exchange | DEREncodedKey Value | ECDH | 256-bit key: id-ecDH, ecdsa-with-SHA256, sect256r1 | 384-bit key: id-ecDH, ecdsa-with-SHA384, |

| | | | | |
|---|---|---|---|---|
| | | | | , sect384r1 |
| | KeyInfo | X509 | • http://www.w3.org/2000/09/xmldsig#X509Data<br>• http://www.w3.org/2000/09/xmldsig#rawX509Certificate | N/A |
| | KeyValue | | dsig11:ECKeyValue | N/A |
| Hash | DigestMethod | SHA | SHA-256 | SHA-384 |

Suite B does not impact the canonicalization method or the transform algorithm used by the XML Signature 1.1 implementation.

XML Encryption 1.1 Suite B Implementations

All XML Encryption 1.1 implementations are Suite B interoperable when they support all of the following Suite B algorithms or methods, as listed in the "Algorithm/Method" column, with their associated required values, as listed in the "REQUIRED" or "OPTIONAL" column, in the table below:

| Suite B Component | XML Encryption 1.1 Element | Algorithm/ Method | REQUIRED by XML Encryption 1.1 | OPTIONAL in XML Encryption 1.1 |
|---|---|---|---|---|
| Encryption | EncryptionMethod | AES-GCM | N/A | • 128-bit key: http://www.w3.org/2009/xmlenc11#aes128-gcm<br>• 256-bit key: http://www.w3.org/2009/xmlenc11#aes256-gcm |
| Key Exchange | KeyDerivationMethod | ConcatKDF | http://www.w3.org/2009/xmlenc11#ConcatKDF | N/A |
| | AgreementMethod | ECDH | http://www.w3.org/2009/xmlenc11#ECDH-ES | N/A |
| | KeyWrap | AES | 256-bit key: http://www.w3.org/2001/04/xmlenc#kw-aes256 | N/A |
| Hash | DigestMethod | SHA | SHA-256 | SHA-384 |

Suite B does not impact the canonicalization method or the transform algorithm used by the XML Encryption 1.1 implementation.