XML Cryptographic Security and Suite B

National Security Agency

25 September 2007
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

<table>
<thead>
<tr>
<th>Symmetric Key Size (bits)</th>
<th>RSA and Diffie-Hellman Key Size (bits)</th>
<th>Elliptic Curve Key Size (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>1024</td>
<td>160</td>
</tr>
<tr>
<td>112</td>
<td>2048</td>
<td>224</td>
</tr>
<tr>
<td>128</td>
<td>3072</td>
<td>256</td>
</tr>
<tr>
<td>192</td>
<td>7680</td>
<td>384</td>
</tr>
<tr>
<td>256</td>
<td>15360</td>
<td>521</td>
</tr>
</tbody>
</table>

NIST Recommended Key Sizes
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.
Suite B is comprised of:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Reference</th>
<th>Key sizes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Advanced Encryption Standard (AES)</td>
<td>FIPS 197</td>
<td>Key sizes: 128 bits and 256 bits</td>
</tr>
<tr>
<td>Digital Signature</td>
<td>Elliptic Curve Digital Signature Algorithm (ECDSA)</td>
<td>FIPS 186-2</td>
<td>Curves: P-256 and P-384</td>
</tr>
<tr>
<td>Key Exchange</td>
<td>Elliptic Curve Diffie-Hellman</td>
<td>NIST Special Publication 800-56A</td>
<td>Curves: P-256 and P-384</td>
</tr>
<tr>
<td></td>
<td>Elliptic Curve Menzes-Qu-Vanstone (ECMQV)</td>
<td>NIST Special Publication 800-56A</td>
<td>Curves: P-256 and P-384</td>
</tr>
<tr>
<td>Hashing</td>
<td>Secure Hash Algorithm</td>
<td>FIPS 180-2</td>
<td>SHA-256 and SHA-384</td>
</tr>
</tbody>
</table>
• 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
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

- NSA Suite B Fact Sheet: [http://www.nsa.gov/ia/industry/crypto_suite_b.cfm](http://www.nsa.gov/ia/industry/crypto_suite_b.cfm)