

CYGNACOM
S O L U T I O N S

Suite B Algorithms
Santosh Chokhani

May 6, 2009

-
- **Suite B Specification**
 - **Benefits of Using Suite B**
 - **Adoption Impediments**
 - **Implementation Nuances**

Suite B Algorithms

- **AES (128 Bit and 256 bit)**
- **ECDSA (P256 and P384 Curves)**
- **ECDH (P256 and P384 Curves)**
- **SHA-256 and SHA-384**

Benefits of Using Suite B

- **Payload size**
- **Performance**
 - Key generation
 - Private Key Operations
- **Security of generated keys**
 - Known domain parameters for selected curves
 - Most RSA hardware implementations do not ensure primality
 - prime number probability of not being prime is to 2^{-100} or lower
 - Meet FIPS 186-3 or ANSI X9.31
 - Specially true of smart card
 - Also true of HSMs
- **MSFT commitment to Suite B enhances interoperability**
- **NSS has Suite B**
 - Netscape, Sun, Firefox, Thunderbird PKI and Crypto API

Adoption Impediments

- **MSFT implementation on XP and earlier platforms**
 - No EC Algorithms in XP and earlier
 - **SHA-256 Support only in XP and not on Win 2K**
 - XP SHA-256 may not extend to applications such as Outlook
 - **AES Support limited in XP**
 - AES available for TLS, IPSEC, WPA
 - AES not available for Outlook
- **CA products do not support EC algorithms**
 - It is always one year away
 - “We will put it in if you want it”
- **HSMs may not be impediment, e.g., SafeNet and nCipher claim to implement**
- **Smart card products**
 - Audience poll

EC Performance

<http://www.cryptopp.com/benchmarks.html>

Crypto++ is a good C++ implementation of both RSA and EC DSA

- **Some benchmarks from above website in milliseconds per cryptographic operation:**

	Sign	Verify
1024 Bit RSA	1.48	0.07
2048 Bit RSA	6.05	0.16
P256 ECDSA	2.88	8.53
P256 ECDSA (precomp)	2.14	3.58

EC Performance (Notes)

- **RSA Public Exponent: 17**
 - NIST recommended exponent of $2^{16} + 1$ means RSA performance will be slower
- **ECDSA pre-computation uses a table of 16 pre-computed multiples of each fixed base to speed up multiplication**
- **Multiplier effect of slower public key operation**
 - Not just one public key operation, but $n + 1$ operations where n is the number of certificates in certification path
 - n can be reduced or eliminated by caching public key verification results
 - Added to software complexity
 - Security trade-off to protect cached results
 - Revocation checking – next Update or revocation notification frequency can be used as cached result time frame

-
- **Best page for ECC/TLS interop:**
<http://dev.experimentalstuff.com:8082/>
 - **Schemes and cipher suites defined in RFC 4492**
 - **Most commercial implementations support:**
 - ECDSA based client authentication scheme
 - **Most commercial implementations do not support other schemes for client authentication:**
 - Client ECDH certificate signed using RSA or ECDSA

- **Schemes and algorithm OIDs defined in RFC 3278 Bis**
 - **ECDH has only one mode: ephemeral (sender), static (recipient)**
 - Note EC MQV is not part of Suite B
 - Thus, encrypted mail alone is not authenticated (no different from RSA situation)
 - Sender authentication must be done using other means, e.g., signed e-mail
 - Sender authorization checks must be done using other means, e.g., information in signature certificate or based on signed identity
- **Expect problems:**
 - For example, a signed message from a user with Outlook 2007/Windows Vista was not readable by a user with Outlook 2003/Windows XP

- **New RFC providing subject public key information**
 - New OID for ECDH, but general EC public key OID in conjunction with key usage and extended key usage can be used
- **Suite B does not include EC MQV**
 - One must use ECDH
- **ECDH based SSL Interoperability working Group**
 - Some activity, but currently quiet
- **ECDH based S/MIME Interoperability working Group**
 - Inactive

