Certicom Proposal to Revise SEC 1: Elliptic Curve Cryptography, Version 1.0

Prepared by Daniel R. L. Brown*

January 14, 2005

Abstract

The *Standard for Efficient Cryptography (SEC) 1, Elliptic Curve Cryptography (ECC), Version 1.0* [23] is a freely available specification of selected ECC techniques. Because of many developments in ECC since its publication in September, 2000, SEC1 would benefit from a revision. This document summarizes Certicom's proposed modifications to SEC 1, v. 1.0.

1 Schedule and Version Numbering

The revision of SEC 1 shall be Version 2.0. A first draft of the Version 2.0 will be released for public comment around February 18, 2005, as Draft 1.5. Please direct any comments to the SECG mailing list.

2 Revisions to Core ECC Techniques

The revised standard will continue to serve as consolidated specification of selected ECC techniques. The revisions primarily function to increase security, and secondarily to improve performance and maintain consistency with other parallel standards efforts. The following list summarizes the revisions to the ECC techniques:

1. Key transport mechanisms where a key agreement scheme is combined with a key wrap algorithm, for consistency with NIST SP 800-56 [18].

*Certicom Research

2. Revised generation of elliptic curve domain parameters, for better security and consistency with the forthcoming ANSI X9.62-2005 [7] and ANSI X9.109 [6], including:

   (a) Verifiably random canonical base point generator G.

   (b) Disallowing composite degree binary fields.

   (c) Only two possible field representation per binary field: a canonical polynomial basis and a canonical normal basis. The latter will be optional.

   (d) Countermeasures to and discussion of Vaudenay's domain parameter attack and its relevance to ECDSA forgery.

   (e) Recommend that $n - 1$ has a large prime factor.

3. Public key validation enhancements, for better security and standards consistency:

   (a) Every public key input to an algorithm must be fully validated.

   (b) Specification of accelerated techniques for public key validation.

4. Countermeasures to certain attacks on ECIES, for better security and consistency with the forthcoming IEEE 1363A-2004 [10]:

   (a) Prevention of Shoup's *parameters shifting attack*, in which the boundaries between the ciphertext and the parameters are shifted in the MAC input.

   (b) Prevention of a *benign malleability attack*, in which the ciphertext is modified while the plaintext is not.

5. Specifications for proper key generation, similar to the directions to be taken in X9.109 [6]:

   (a) Public key validation

   (b) Proof of possession

   (c) Verifiable (and assisted) key generation

6. Allow alternative mode of ECDSA verification which uses the private key, for consistency with the new X9.62 revision.

7. Inclusion of elliptic curve Pintsov-Vanstone signature algorithm providing partial message recovery[1], consistent with IEEE 1363A [10] and forthcoming ANS X9.92 [4].

3 Revisions to non-ECC Cryptographic Techniques

It is not in the scope of SEC 1 to specify non-ECC techniques. Most ECC techniques, however, make internal use of some non-ECC cryptographic techniques such as hash functions, message authentication codes and symmetric encryption. For such internal usage of non-ECC techniques, SEC 1, v. 1.0 required certain techniques, which are specified via reference to external standards. The revision of SEC 1, v. 2.0 will modify these requirements to ensure that an adequate level of security is provided. This will still be achieved through reference to external standards. Most notable among such new non-ECC techniques are AES [15] and the new SHA2 family of hash functions [20].

To encourage interoperability, the revision of SEC 1 will also recommend certain non-ECC techniques. The recommendations applies to both internal use and external use[2] of these techniques. Only recommendations for external use of non-ECC techniques will be given; requirements apply only to internal uses. Recommendations are provided to guide implementers of ECC to use ECC with other techniques that provide an adequate level of security.

The following list summarizes the requirements and recommendations regarding non-ECC algorithms:

1. Five pre-defined security levels (80, 112, 128, 192, and 256 bits), , for consistency with the forthcoming X9.62-2005 [7] and FIPS 186-3, and NIST draft Special Publications 800-56 [18] and 800-57 [19], with required levels for data protection lifetimes:
   (a) Up to 2010: security level 80, 112, 128, 192 or 256 bits.
   (b) Up to 2030: security level 112, 128, 192, or 256 bits.
   (c) Beyond 2030: security level 128, 192, or 256 bits.
2. Certain symmetric encryption algorithms specified in other standards:

[1] Another approach is to include PV signatures in a new SECG document, such as SEC 5.

[2] An example of external use is agreeing a key with ECMQV, and then using the key with a symmetric encryption technique, which is the external usage.

(a) Block cipher for security level:

i. Two-key Triple-DES for the 80-bit security level.

ii. Three-key Triple-DES for the 112-bit security level, and lower security levels

iii. AES-128 for the 128-bit security level, and lower security levels.

iv. AES-192 for the 192-bit security level.

v. AES-256 for the 256-bit security level.

(b) Modes of operations for block ciphers specified in other standards such as the NIST SP 800-38 series, such as:

i. Encryption (such as CBC, CFB, OFB, ECB, Counter mode, as in NIST SP 800-38a [16] and ANSI X9.52 [1]).

ii. Authentication (such as RMAC in NIST SP 800-38B [17])

iii. Authenticated encryption (such as CCM in NIST SP 800-38C [21])

iv. Key wrap (such as in X9.102 [4] and S/MIME [11])

v. Random number generation (such as in forthcoming X9.82 [8])

vi. Hashing (such as the Matyas-Meyer-Oseas method in Zigbee)

(c) Stream cipher algorithms for certain exceptional circumstances (such as when block cipher not viable, or for backward interoperability with existing legacy implementations).

3. Certain hash functions specified in other standards, especially FIPS 180-2, Change Notice [20].

(a) In general, and especially for generating an ECDSA signature, a unique hash function of output length equal to twice the security level:

i. SHA-1 for the 80-bit security level

ii. SHA-224 for the 112-bit security level

iii. SHA-256 for the 128-bit security level

iv. SHA-384 for the 192-bit security level

v. SHA-512 for the 256-bit security level

(b) In special well-defined circumstances below, a hash function of output length equal to the security level:

i. Key derivation

ii. Message authentication

iii. Random number generation

(c) In the special circumstance below, SHA-1 to be used for any security level:

i. Verification of the ten verifiably random NIST-recommended elliptic curve domain parameters specified in FIPS 186-2 [14] and SEC 2 [24].

(d) Other hash functions, on an exception basis:

i. In the TLS pseudorandom function, see [13], the hash functions SHA-1 and MD5 are used in combination as a key derivation function instead of the key derivation function specified in X9.63 [3], SEC 1 [23], and NIST SP 800-56 [18].

4. Revised key derivation function specification, including:

   (a) Use of stronger hash functions than SHA-1 (such as SHA-256 in [20].)

   (b) Specifications and requirements for better consistency with the NIST SP 800-56 [18].

5. Key wrap mechanisms, for consistency with NIST SP 800-56 [18] and X9.102 [5], and to support more general key transport schemes.

6. New random number generator requirements and algorithms, for consistency with the new X9.62 [7] and X9.82 [8], including:

   (a) Methods to ensure no bias in the random numbers.

   (b) Requirements and definitions of entropy for RNG seeding.

   (c) New deterministic RNG algorithms including HMAC-based and elliptic curve based.

4 Revisions to Syntax

Corresponding to the revisions of the underlying techniques, revisions to the syntaxes used are needed to communicate use of the revised techniques. The following briefly summarizes the syntax revisions:

1. Additional ASN.1 for:

   (a) Better algorithm identification in certificates:

i. Consistency with the forthcoming X9.62-2005 [7] and [12] PKIX work in progress, including extensions for ECMQV.

(b) Better algorithm identification for with S/MIME [11].

2. Specification of PEM-like headers.

3. Tentative specifications for new data fields that can be embedded in certificates and other places, that enable acceleration of public key operations

5 Revisions to Commentary and References

For convenience, SEC 1 provides commentary and references, and will continue to do so. This helps implementers compare SEC 1 to other standards and papers about ECC.

1. Better consistency with other standards, particularly those of ANSI, NIST, IEEE, ISO, and IETF.

2. Provisions for backwards compatibility exemptions to new requirements.

3. Comparison of SEC 1 to other standards for ECC.

4. Better support for existing implementations of ECC.

5. Updated references, including new standards and new research papers.

6. Updated commentary, including discussion of new relevant research results.

References

[1] American National Standards Institute. *ANS X9.52-1998: Triple Data Encryption: Modes of Operation*, 1998. Purchasable at webstore.ansi.org/ansidocstore/default.asp.

[2] American National Standards Institute. *ANS X9.62-1998: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 1998. Revision scheduled for 2005. Purchasable at webstore.ansi.org/ansidocstore/default.asp.

[3] American National Standards Institute. *ANS X9.63-2001: Public-Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography*, 2001. Purchasable at webstore.ansi.org/ansidocstore/default.asp.

[4] American National Standards Institute. *Draft ANS X9.92-2002: Public-Key Cryptography for the Financial Services Industry: Digital Signature Algorithms Providing Partial Message Recovery: Part 1: Elliptic Curve Pintsov-Vanstone Signatures (ECPVS)*, 2002. Tentative organization: Part 1: Overview; Part 2: Entropy Sources; Part 3: Deterministic Algorithms; Part 4: Complete Systems.

[5] American National Standards Institute. *Draft ANS X9.102-2003: Symmetric Key Cryptography for the Financial Services Industry: Part 1: Wrapping of Keys and Associated Data*, 2003. Draft.

[6] American National Standards Institute. *Draft ANS X9.109: Public-Key Cryptography for the Financial Services Industry: Domain Parameter and Key Generation*, 2005. No draft available yet. Currently an approved new work item of X9F1.

[7] American National Standards Institute. *Draft ANS X9.62-2005: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 2005. Draft revision.

[8] American National Standards Institute. *Draft ANS X9.82: Random Number Generation*, 2005. Tentative organization: Part 1: Overview; Part 2: Entropy Sources; Part 3: Deterministic Algorithms; Part 4: Complete Systems.

[9] Institute of Electrical and Electronics Engineers. *IEEE Std 1363-2000: Standard Specifications for Public-Key Cryptography*, 2000. Purchasable at standards.ieee.org/catalog/olis/busarch.html.

[10] Institute of Electrical and Electronics Engineers. *IEEE Std 1363A-2004: Standard Specifications for Public-Key Cryptography — Amendment 1: Additional Techniques*, 2004. Purchasable at standards.ieee.org/catalog/olis/busarch.html.

[11] Internet Engineering Task Force. *Request for Comments 3278: Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)*, April 2002. Available at www.ietf.org/rfc/rfc3278.txt.

[12] Internet Engineering Task Force. *Internet-Draft: Additional Algorithms and Identifiers for the Use of Elliptic Curve Cryptography with PKIX*, July 2004. Available at www.ietf.org/internet-drafts/draft-ietf-pkix-ecc-pkalgs-00.txt.

[13] Internet Engineering Task Force. *Internet-Draft: ECC Ciphersuites for TLS*, December 2004. Available at www.ietf.org/internet-drafts/draft-ietf-tls-ecc-07.txt.

[14] National Institute Standards and Technology. *Federal Information Processing Standard 186-2: Digital Signature Standard (Change Notice)*, October 2001. Available at csrc.nist.gov/publications/fips/fips-186-2/fips-186-2-change1.pdf.

[15] National Institute Standards and Technology. *Federal Information Processing Standard 197: Advance Encryption Standard (Change Notice)*, October 2001. Available at csrc.nist.gov/publications/fips/fips-197/fips-197.pdf.

[16] National Institute Standards and Technology. *Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation*, December 2001. Available at csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.

[17] National Institute Standards and Technology. *Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: the RMAC Authentication Mode*, November 2002. Draft. Available at csrc.nist.gov/publications/drafts/draft800-38B-110402.pdf.

[18] National Institute Standards and Technology. *Special Publication 800-56: Recommendation on Key Establishment Schemes*, January 2003. Draft 2.0. Available at csrc.nist.gov/CryptoToolkit/kms/keyschemes-Jan03.pdf.

[19] National Institute Standards and Technology. *Special Publication 800-57: Recommendation for Key Management: Part 1: General Guideline*, January 2003. Draft. Available at csrc.nist.gov/CryptoToolkit/kms/guideline-1-Jan03.pdf.

[20] National Institute Standards and Technology. *Federal Information Processing Standard 180-2: Secure Hash Standard (Change Notice)*, February 2004. Available at csrc.nist.gov/publications/fips/fips-180-2/fips-180-2withchangenotice.pdf.

[21] National Institute Standards and Technology. *Special Publication 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, May 2004. Available at csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf.

[22] National Institute Standards and Technology. *Federal Information Processing Standard 186-3: Digital Signature Standard (Change Notice)*, 2005. Anticipated revision of FIPS 186-2.

[23] Standards for Efficient Cryptography Group. *SEC 1: Elliptic Curve Cryptography*, September 2000. Version 1.0. Document proposed for revision. Available at www.secg.org.

[24] Standards for Efficient Cryptography Group. *SEC 2: Recommended Elliptic Curve Domain Parameters*, September 2000. Version 1.0. Available at www.secg.org.