

Standards for Efficient Cryptography Group
Minutes of the 16 September 1999 Meeting

A combined total of 18 SECG members and participants attended the meeting hosted by NIST. A separate attendee list will be published by Certicom.

The meeting was launched with a review of the latest SEC 1 draft led by Simon Blake-Wilson of Certicom. The group's comments were as follows:

- SEC 1 Section 3.6 should be reviewed for compatibility with the IETF standards TLS and IPsec. Can SEC 1 support TLS?
- Section 3.8 should include a health warning concerning the use of exclusive-or.
- A new name for ECAES was recommended. Don Johnson has asked Bellare and Rogaway for their recommendations. The new ECAES name will be ECIES for Integrated Encryption Scheme.
- Table 5 of Appendix B must be extended.
- Table 6 should be clarified to state that the results are based on the number of operations required. Don Johnson will submit wording.
- Section 6.4 Add a note stating that the private key cannot be separated from the domain parameters.
- Simon reviewed Dan Boneh's and Phil Rogaway's comments on SEC 1. No significant problems with the document were found. Please see their comments on the www.secg.org.
- Simon will adjust some wording to accommodate Fujitsu's request to note that an implementation is compliant if its computations produce equivalent results as another implementation. It was noted that Fujitsu's approach was considered more risky.

Simon expects to have the final draft of SEC 1 ready in early October. Barring strong dissent from the SECG membership, it is expected to become an SECG standard by year end.

The latest GEC 1 draft was next reviewed by the group. The group's comments were as follows:

- Add the large NIST recommended curves to GEC 1.
- The group wants GEC 1 to support field sizes larger than 256 bits to accommodate the use of AES.
- Table 1 and Table 4. Change "Strength" to "Approximate Strength".
- Change the name of GEC 1 to SEC 2 to reflect the group's desire for this document to have greater force among other standards bodies, companies, and implementers.

Simon expects to have the next revision of this document in early October. Barring major dissent from the SECG membership, it is expected to become an SECG standard by year end.

GEC 2 was briefly reviewed. NIST and NSA will see if they can assist in generating test vectors as well as in verifying the existing test vectors.

Peter de Rooij, Certicom, led a review of the X.509 ECC draft produced by his working group. Comments were as follows:

- The draft is compliant with ANSI X9.62, X9.63 and PKIX. It is not necessarily compliant with ANSI X9.57.
- Health warnings should be added for key usage.
- The working group is to investigate support for hybrid certificates (certificates using containing mixed cryptosystem data)
- This document will become SEC 3.

This working group will produce the next revision by mid-October. Xcert and Diversinet will check into the availability of ASN.1 experts to assist with the ASN.1 portion of this document. They will also check its compliance with PKIX.

Proposed New Work Discussions:

Short Certificates and Implicit Certificates

Simon Blake-Wilson reviewed implicit certificates with the group and Don Johnson reviewed ANSI X9.68 and other short certificate work with the group. These presentations will be posted to the SECG web page. It was put to the group whether or not the SECG should develop a standard for implicit certificates. There was unanimous consent for this from the group. The group was also asked if work should commence on an X9.68 short certificate-type. It was decided to wait until ANSI completes their next revision of X9.68 and see if the SECG can add any value.

The next steps will be to establish a working group for implicit certificates. Bill Lattin will coordinate this.

Signatures with Message Recovery

Some discussion was had regarding whether or not the SECG should develop standardization of signature techniques with message recovery. No strong agreement was forthcoming from the group, so a call will be made to the mailing list.

Other Items:

NIST gave a short review of their standards activities. Of particular interest, they will be hosting a workshop in Q1 2000 to create a key management standard. Also, they said that FIPS 186-2, the next revision of the Digital Signature Standard which incorporates RSA, was sent to the Department of Commerce for signature. A version of FIPS 186 incorporating ECDSA is also in process. This was due to the solicitations received from industry - these included the letter from the SECG as well as many letters from SECG members.

In closing, on behalf of the SECG, I wish to thank NIST for hosting this meeting. We are close to having our first standards which will be a great milestone for the SECG.

I apologize for the delay in posting these minutes.

The next meeting will be scheduled via the mailing list.

Respectfully submitted,

Bill Lattin
SECG Chair