

Standards for Efficient Cryptography Group
18 February 1999
General Meeting Minutes

The meeting was opened by Scott Vanstone, Chief Cryptographer of Certicom

Bill Lattin of Certicom gave a brief background describing the goals of the SECG, the industry composition of its members, and the operation of the SECG. Since the group is a *de facto* organization, it was asked how it would be decided when a standard was ready for publication. Bill replied, that as SECG Chair, he would watch the secg-talk list activity for messages regarding a particular standard. As the list activity for that standard tapers off, he will declare that standard ready for general publication. Bill's presentation is posted on the SECG website.

Simon Blake-Wilson of Certicom next presented on the SEC 1 and GEC 1 draft documents. Please see the meeting minutes specifically relating to the discussions of these documents. Simon's presentations are available from the SECG website.

Next, Peter de Rooij of Certicom presented an overview of a recommended approach for specifying ECC X.509v3 certificates. His presentation is available from the SECG website. It was decided to establish a working group to focus on the development of this standard. A call for a working group chair was made with the outcome that Mr. de Rooij was appointed chair of the working group. Current members of this working group are: William Whyte - Baltimore, Don Johnson - Certicom, Adel Jaber - Diversinet, Mark Shuttleworth - Thawte, and Young Etheridge - Xcert. If others wish to join, please contact Peter at pderooij@certicom.com.

Larry Puhl of Motorola next presented on Motorola's cryptographic API and ANSI X9.68's work on short certificates. Larry's presentations are posted on the SECG web server. There was considerable group discussion on the general subject of short certificates and cryptographic APIs. It was decided to move the discussions on to the mail list. Time will be reserved at the next meeting to further discuss these topics.

The next presentation, on ECC extensions to the PKIX protocols, was made by Paul Lambert of Certicom. Paul's presentation is posted on the SECG web server. This area is one requiring considerable further research. Discussion in this area covered primarily proof of possession. Paul will solicit inputs to this effort on the mail list.

Shawn Abbott of Rainbow presented proposed ECC extensions to PKCS #11. He is chair of this working group and will solicit members on the mail list. The current plan is to develop a list of suggested modifications to PKCS #11 and to submit this list to Security Dynamics/RSA Labs for use in modifying PKCS #11. If the SECG does not get support for these modifications (or appropriate modifications) from Security Dynamics, then the SECG may make these modifications proprietary PKCS #11 extensions as allowed per

that document and publish them as an SEC standard. Shawn may be contacted at sabbott@rainbow.com.

Bill Lattin closed the meeting by thanking everyone for their support of the SECG and for making this first meeting a productive and successful event.

Next Meeting:

The SECG accepted NIST's invitation to host the next meeting at their facilities in Maryland. If possible, the group would like to align the meeting with Crypto '99 to minimize the travel burden of overseas members.

Potential new work items for this meeting include: a review of ECC use in IPsec, SMIME and TLS; alignment of TLS with SEC 1; short certificate structures; cryptographic APIs.

Attendees:

An attendee list, with contact information, will be posted separately.