

Standards for Efficient Cryptography Group

Information Technology Laboratory
ATTN: DSS/X9.31 Comments
National Institute of Standards and Technology
100 Bureau Drive Stop 8970
Gaithersburg, MD 20899-8970

3 March 1999

Subject: Request to include ECDSA in FIPS 186-1

Dear Sirs:

The Standards for Efficient Cryptography Group (SECG) is a multinational industry consortium committed to the development and use of Elliptic Curve Cryptography (ECC) for information security purposes in commercial and governmental applications.

Regarding the proposed FIPS 186-1, the SECG requests that NIST further extend FIPS 186 to include the ability to conform to ANSI X9.62 ECDSA, for the following reasons:

1. ECDSA is based on a different hard problem than RSA or DSA signatures. All three methods are recognized by ANSI X9 and are being recognized by ISO SC27, IEEE P1363, IETF, and other standards bodies. The FIPS Digital Signature Standard should encompass the same commercially-endorsed technology to ensure FIPS-conformant products will be able to use off-the-shelf technology.
2. X9.62 is the first digital signature standard to include specification of methods for domain parameter validation and public key validation - critical features for those users which wish additional assurance that:
 - (i) there was not a calculation error during key pair generation; and
 - (ii) no one was trying to use a false or spoofed set of domain parameters or a false public key that would void all intended security.
3. ECDSA offers technical advantages in the areas of key size, certificate size, and performance over other digital signature methods. Its smaller data structures and calculation efficiencies enable it to be used in specific applications in which either RSA or DSS would be very difficult or expensive to implement. As an example, the lowest cost smart cards (8-bit CPU and no cryptographic coprocessor) can be used to realize practical implementations of ECDSA, but not of RSA or DSA.

4. When the public key infrastructure model being used assumes that each user generates his or her own public/private key pair, choosing ECDSA means that more systems will be able to meet that assumption than if RSA and DSA are the only options.

5. ECDSA-enabled products and applications are currently available in the market. These include smart cards, hardware accelerators, certificate authorities, and EDI/financial applications. Elliptic Curve Cryptography is currently used in a number of commercial and government applications, including the US Postal Service IBIP program.

Members of the SECG include the following companies: 3Com, ABN-AMRO, American Express, Baltimore Technologies, Certicom, Deloitte & Touche, Diversinet, Ernst & Young, Fujitsu, Giesecke & Devrient, GlobeSet, GTE CyberTrust, Hewlett-Packard, Hitachi Ltd., Indicii Salus, Inter Clear Service Ltd., LPK Information Integrity Ltd., Motorola, NTT Electronics Corporation, Pitney Bowes, Rainbow Technologies, Thawte Consulting, Visa International and Xcert International. Additional information on the SECG may be found at our website, www.secg.org.

Should you wish any additional information, please feel free to contact the undersigned at 650/312-7991.

We thank you for your careful consideration of this matter.

Sincerely,

William L. Lattin
SECG Chair