certicom

September 24, 1999

Mr. Harold Deal
American National Standards Institute
X9 Financial Services Committee
c/o Nations Bank
1 Independence Center
NCI-001-09-10
Charlotte, NC 28255

Dear Mr. Deal:

This letter sets forth Certicom's policy with respect to its Intellectual Property in relation to ANSI X9.63 Key Agreement and Key Transport Using Elliptic Curve Cryptography.

Certicom is committed to making public-key cryptography viable in constrained devices such as wireless devices, PDA's and smart cards. In pursuing research to discover the most efficient ways to implement high-strength public-key cryptography, Certicom has generated significant intellectual property. In doing so, it has invested significant financial resources and has protected that investment by filing numerous patents on cryptographic implementation techniques, routines, algorithms, and protocols. Some of this intellectual property is embodied in currently-evolving standards and Certicom is continuing to meet its obligations to notify standards associations of patent coverage. We have attached a schedule setting out the areas of ANSI X9.63 Key Agreement and Key Transport Using Elliptic Curve Cryptography that may fall under the scope of one or more Certicom patents or patent applications.

If any of Certicom's patents are required to implement the cryptographic schemes in ANSI X9.63, Certicom is prepared to grant a license to any party to use those patents in implementing a scheme compliant with ANSI X9.63 on a nondiscriminatory basis and on reasonable terms and conditions, provided that the licensee provides a similar grant for any relevant patents under their control to Certicom.

For information of licensing terms, please contact:

Bruce MacInnis
Director of Licensing
Certicom Corp.
200 Matheson Blvd. West
Mississauga, Ontario
Canada L5R 3L7
Tel: (905) 501-3821
Fax: (905) 507-1239
bmacinnis@certicom.com

Yours truly,

Philip C. Deck
Chairman & CEO

Attachment

certicom

Attachment

An implementation conforming to the ANSI X9.63 standard may require a license from Certicom for one or more of the following items.

Certicom is the owner of the following issued patents:

1. US4745568: Computational method and apparatus for finite field multiplication, issued May 17, 1988.
2. US5761305: Key agreement and transport protocol with implicit signatures, issued June 2, 1998.
3. US5787028: Multiple bit multiplier, issued June 28, 1998.
4. US5889685: Key agreement and transport protocol with implicit signatures, issued March 30, 1999.
5. US5896455: Key agreement and transport protocol with implicit signatures, issued April 20, 1999.
6. US5933504: Strengthened public key protocol, issued August 3, 1999.

Corresponding foreign patent applications have been applied for.

In addition Certicom is an exclusive licensee to the following US patents and corresponding Canadian applications:

1. US5600725: Digital signature method and key agreement method, issued February 4, 1997.

Certicom also has patent applications that relate to the following:

1. Methods for efficient implementation of elliptic curve arithmetic over finite fields. This includes efficient methods for computing inverses.
2. Methods for point compression.
3. Methods to improve performance of private key operations.
4. Various versions of the MQV key agreement protocols.
5. Methods to thwart or mitigate small subgroup attacks.
6. Methods to improve performance of elliptic curve arithmetic; in particular, fast efficient multiplication techniques.
7. Methods to improve performance of finite field multiplication.
8. Methods for efficient implementation of arithmetic modulo n.
9. Methods to perform validation of elliptic curve public keys (including validation of elliptic curve domain parameters).
10. Methods to perform efficient basis conversion.

Finally Certicom has pending US and Canadian applications numbers US 09/070794 and CA 2236495 which include methods for performing key confirmation. To encourage use of secure methods for performing key confirmation, Certicom will grant a royalty-free license on any patent that may issue from these applications to any party implementing a key confirmation method compliant with ANSI X9.63. No license beyond the implementation of this standard is granted by or to be inferred from this statement.

Certicom Corp. 200 Matheson Blvd. West, Suite 103 Mississauga, Ontario, L5R3L7, Canada
t.905.507.4220 f: 905.507.3680 www.certicom.com