



Bill Lattin  
SECG Chair  
Certicom  
25801 Industrial Boulevard  
Hayward, CA 94545, USA

May 27, 1999

Dear Bill:

This letter is in response to the SECG Patent Policy of April 26, 1999 available from <http://www.secg.org>.

Certicom is committed to making public-key cryptography viable in the most demanding environments, particularly encountered in small 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 considerable 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 the SEC1 and GEC1 Standards that may fall under the scope of one or more Certicom patents or patent applications.

Certicom agrees upon request to grant a non-exclusive license under our patent or patents on a nondiscriminatory basis and on reasonable terms and conditions provided a similar grant under licensee's patents within the scope of the license granted to licensee is made available upon request 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  
905-507-9343  
[bmacinni@certicom.com](mailto:bmacinni@certicom.com)

Yours truly,

Philip C. Deck  
CEO  
Certicom Corp.

Attachment

This list is accurate as of May 26, 1999. An implementation conforming to the SEC1 and GEC1 standards may require a license from Certicom for one or more of the following items.

Certicom is the owner of the following issued patents:

1. 4,745,568: Computational method and apparatus for finite field multiplication, issued May 17, 1988. This patent includes methods for efficient implementation of finite field arithmetic using a normal basis representation.



2. 5,761,305: Key Agreement and Transport Protocol with Implicit Signatures, issued June 2, 1998. This patent includes versions of the MQV protocols.
3. 5,787,028: Multiple Bit Multiplier, issued July 28, 1998.
4. 5,889,865: Key Agreement and Transport Protocol with Implicit Signatures, issued March 30, 1999. This patent includes versions of the MQV protocols.
5. 5,896,455: Key Agreement and Transport Protocol with Implicit Signatures, issued April 20, 1999. This patent includes versions of the MQV protocols.

Note that corresponding foreign patent applications have been applied for.

Certicom has the exclusive North American license rights to the following issued patent:

1. 5,600,725: Digital signature method and key agreement method, issued Feb. 4, 1997. This patent includes the Nyberg-Rueppel (NR) signature method.

Certicom has patent applications that include 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 avoid the small subgroup attack.
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.
10. Methods to perform efficient basis conversion.