February 10, 2005

SECG Consortium

Dear SECG consortium,

This letter is in response to the SECG Patent Policy as posted on www.secg.org, on February 10, 2005.

Certicom is the authority for strong, efficient cryptography required by software vendors and device manufacturers to embed security in their products. 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, Certicom 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. I have attached a schedule listing the Certicom patents and patents pending that are included in the current SECG Standards. This list may not be exhaustive and will be amended from time to time.

Certicom agrees, upon request, to grant non-exclusive licenses to our 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 the licensee is made available, upon request, to Certicom.

For information of licensing terms, please contact:

Paul Carter
Director, IP Licensing & Sales Operations
Certicom Corp.
5520 Explorer Drive, 4th Floor
Mississauga, ON L4W 5L1
Canada
905-507-4220
pcarter@certicom.com

5520 Explorer Drive, 4th Floor
Mississauga, ON. L4W 5L1
Canada
Ph: 905-507-4220 Fax: 905-501-4230

Attachment:

This list has been complied as of February 10, 2005. An implementation conforming to the current SECG standards may require a license from Certicom for one of more of the following items.

Certicom is the owner of the following issued patents:

EP 0 739 105 B1 (validated in DE, FR, and the UK)
"Method for signature and session key generation"
pertains to the MQV protocol

US 5,600,725
"Digital Signature Method and Key Agreement Method"
pertains to PV signatures

US 5,761,305
"Key Agreement and Transport Protocols with Implicit Signatures"
pertains to the MQV protocol

US 5,889,865
"Key Agreement and Transport Protocol with Implicit Signatures"
pertains to the MQV protocol

US 5,896,455
"Key Agreement and Transport Protocol with Implicit Signatures"
pertains to the MQV protocol

US 5,933,504
"Strengthened public key protocol"
pertains to preventing the small-subgroup attack

US 6,122,736
"Key agreement and transport protocol with implicit signatures"
pertains to the MQV protocol

US 6,141,420
"Elliptic Curve Encryption Systems"
pertains to point compression

US 6,618,483
"Elliptic curve encryption systems"
pertains to point compression

US 6,704,870
"Digital Signatures on a Smart Card"
pertains to ECDSA

US 6,785,813
"Key agreement and transport protocol with implicit signatures"

5520 Explorer Drive, 4th Floor
Mississauga, ON. L4W 5L1
Canada
Ph: 905-507-4220 Fax: 905-501-4230

pertains to the MQV protocol

CH 693 252
"Verfahren und Vorrichtung zur Erzeugenung einer ganzen Zahl"
pertains to key generation

US 6,078,667
"Generating Unique and Unpredictable Values"
pertains to key generation

AU 758044
"Implicit certificate scheme"
pertains to bullet certificates

EP 1 066 699
"Method of generating a public key in a secure digital communication system and implicit certificate"
pertains to bullet certificates

US 6,792,530
"Implicit certificate scheme"
pertains to bullet certificates

Pertinent patent applications:
1. Methods to improve the performance of elliptic-curve arithmetic.
2. Methods to improve the performance of finite-field operations.
3. Methods to improve the performance of private-key operations.
4. Methods to improve the performance of public-key operations, including signature verification.
5. Methods to improve the performance of modular arithmetic.
6. Methods pertaining to the validation of elliptic-curve public keys.
7. Methods to thwart domain-parameter attacks.
8. Methods to perform efficient basis conversion.
9. Methods to generate keys with desirable cryptographic properties.
10. Methods pertaining to PV signatures.

5520 Explorer Drive, 4th Floor
Mississauga, ON. L4W 5L1
Canada
Ph: 905-507-4220 Fax: 905-501-4230