**Certicom IPR contribution for
RFC 4346, RFC 5246, RFC 5289, RFC 4492, RFC 2409, RFC 4306,
RFC 4754, RFC 4753, RFC 4869, RFC 4253, RFC 2633, RFC 3278,
RFC 4347, RFC 4366, RFC 4109, RFC 4252, RFC 3850, RFC 3851,
RFC 5008, draft-ietf-tls-rfc4347-bis-00, draft-rescorla-tls-suiteb-07,
draft-ietf-tls-extractor-02, draft-green-secsh-ecc-03, draft-ietf-avt-dtls-srtp-05,
draft-igoe-secsh-suiteb-00, draft-ietf-smime-3851bis-08,
draft-ietf-smime-3850bis-08, draft-ietf-smime-multisig-05,
draft-ietf-smime-sha2-09, and draft-ietf-smime-3278bis-02**

13 October 2008

It is Certicom's desire to facilitate the wide-scale adoption and proliferation of Elliptic Curve Cryptography (ECC) technology in the marketplace to replace today's aging public key systems. At this time, Certicom believes its patents and patent applications listed in Schedule A contain claims which may be necessary and essential to implementations of the following protocols:

IETF TLS:
"The Transport Layer Security (TLS) Protocol -- Version 1.1," RFC 4346 or "The Transport Layer Security (TLS) Protocol – Version 1.2," RFC 5246, or "Datagram Transport Layer Security (DTLS) – Version 1.2," draft-ietf-tls-rfc4347-bis-00.txt, or "Transport Layer Security (TLS) Extensions", RFC 4366, or "Datagram Transport Layer Security (DTLS) – Version 1.0", RFC 4347, or "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for Secure Real-time Transport Protocol (SRTP)", draft-ietf-avt-dtls-srtp-05.txt or "Keying Material Extractors for Transport Layer Security (TLS)", draft-ietf-tls-extractor-02.txt when used with either:

A. "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security(TLS)" RFC 4492, May 2006; or,
B. "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode," RFC 5289, or
C. "Suite B Cipher Suites for TLS," draft-rescorla-tls-suiteb-07.txt;

IETF IKE for IPSec:
IPsec IKE and IKEv2 Protocols:

"The Internet Key Exchange (IKE)," RFC 2409; or "Internet Key Exchange (IKEv2) Protocol," RFC 4306 when used with either:

A. "IKE and IKEv2 Authentication Using ECDSA," RFC 4754; or
B. " ECP Groups for IKE and IKEv2," RFC 4753; or
C. "Suite B Cryptographic Suites for IPsec." RFC 4869; or
D. "Algorithms for Internet Key Exchange version 1 (IKEv1)", RFC 4109

SSH:

"The Secure Shell (SSH) Transport Layer Protocol," RFC 4253 or "The Secure Shell (SSH) Authentication Protocol", RFC 4252 when used with:

A. "Elliptic-Curve Algorithm Integration in the Secure Shell Transport Layer," draft-green-secsh-ecc-03; or
B. "Suite B Cryptographic Suites for Secure Shell", draft-igoe-secsh-suiteb-00.txt.

CMS in S/MIME:

"Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.0 Message Specification," RFC 2633 or "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification, RFC 3851, or "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling", RFC 3850, or "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling", draft-ietf-smime-3850bis-08.txt, or "Secure/Multipurpose Internet Mail Extensions Specification", draft-ietf-smime-3851bis-08.txt or "Multiple Signatures in S/MIME", draft-ietf-smime-multisig-05.txt, when used with digital certificates and:

A. "Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)," RFC 3278; or
B. "Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)," draft-ietf-smime-3278bis-02.txt; or
C. "Using SHA2 Algorithms with Cryptographic Message Syntax", draft-ietf-smime-sha2-09.txt; or
D. "Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME)", RFC 5008.

Certicom will, upon request, provide a nonexclusive, royalty free patent license, to manufacturers to permit end users (including both client and server sides), to use the patents in schedule A when implementing any of these protocols, including those requiring third party certificates provided the certificate is obtained from a licensed Certificate Authority (CA). This license does not cover the issuing of certificates by a Certification Authority (CA).

The reasonable terms and conditions of this license are contained in the license document that Certicom intends to make available on its web site.

This royalty free license is restricted to the use of the protocols listed above utilizing the ECC options in the specified drafts and restricted to NIST curves P256, P384, and P521 only. The IKE and IKEv2 protocols must be used in combination with IPSec in this license grant; and CMS must be used in combination with S/MIME in this grant. Certicom will grant licenses on reasonable and non-discriminatory terms for implementations of these protocols over other named curves or explicitly defined curves. The above list of protocols will be amended from time to time in order to keep the documents current.

The license granted does not extend, either explicitly or implicitly, to other IETF protocols.

Any party wishing to request a license should contact:

Tony Rosati
VP of Intellectual Property Licensing
Certicom Corp.
5520 Explorer Drive, 4th Floor
Mississauga, ON L4W 5L1
Tel:(613)254-9265

email: trosati@certicom.com

Any party wishing to request additional information may contact:

Matthew Campagna
Director of Research
Certicom Corp.
5520 Explorer Drive, 4th Floor
Mississauga, ON L4W 5L1
Tel:(203)897-9777

email: mcampagna@certicom.com

Schedule A

(1) U.S. Pat. No. 5,761,305 entitled "Key Agreement and Transport Protocol with Implicit Signatures" issued on June 2, 1998;

(2) Can. Pat, Appl. Ser. No. 2,176,972 entitled "Key Agreement and Transport Protocol with Implicit Signature and Reduced Bandwidth" filed on May 16, 1996;

(3) U.S. Pat. No. 5,889,865 entitled "Key Agreement and Transport Protocol with Implicit Signatures" issued on March 30, 1999;

(4) U.S. Pat. No. 5,896,455 entitled "'Key Agreement and Transport Protocol with Implicit Signatures" issued on April 20, 1999;

(5) U.S. Pat. No. 5,933,504 entitled "Strengthened Public Key Protocol" issued on August 3, 1999;

(6) U.K Pat. No. 9510035 entitled "Strengthened Public Key Protocol" filed on May 18, 1995 (superseded by 8 below);

(7) Can. Pat. Appl. Ser. No. 2,176,866 entitled "Strengthened Public Key Protocol" filed on May 17, 1996;

(8) E.P. Pat. Publ. Appl. Ser. No. 0743774 entitled "Strengthened Public Key Protocol" filed on May 17, 1996 ;

(9) U.S. Pat. No. 5,999,626 entitled "Digital Signatures on a Smartcard" issued on December 7, 1999;

(10) Can. Pat No. 2202566 entitled "Digital Signatures on a Smartcard" issued on December 12, 2006;

(11) E.P. Pat. Appl. No. 97106114.8 entitled "Digital Signatures on a Smartcard" filed on April 15, 1997;

(12) U.S Pat. No. 6,122,736 entitled "Key Agreement and Transport Protocol with Implicit Signatures" issued on September 19, 2000;

(13) Can. Pat. No. 2,174,261 entitled "Key Agreement and Transport Protocol with Implicit Signatures" issued on June 12, 2007;

(14) E.P. Pat. No. 0739105 entitled "Key Agreement and Transport Protocol with Implicit Signatures" issued on October 13, 2004, registered in DE, FR, UK;

(15) U.S. Pat. No. 6,141,420 entitled “Elliptic Curve Encryption Systems" issued on October 31, 2000;

(16) Can. Pat Appl. Ser. No.2155038 entitled "Elliptic Curve Encryption Systems" filed on July 31, 1995;

(17) E.P. Pat. No. 0804758 entitled "Elliptic Curve Encryption System" issued on November 19, 2005, registered in CH, DE, FR, UK;

(18) U.S. Pat. No. 6,336,188 entitled "Authenticated Key Agreement" issued on January 1, 2002;

(19) U.S. Pat. No. 6,487,661 entitled "Key Agreement and Transport Protocol" issued on November 26, 2002;

(20) Can. Pat. No. 2174260 entitled "Key Agreement Transport Protocol" issued on June 19, 2007;

(21)-E. P. Pat. No. 0739106 entitled "Key Agreement and Transport Protocol" issued on October 15, 2003, registered in DE, FR, UK;

(22)-U.S. Pat. No. 6,563,928 entitled "Strengthened Public Key Protocol" issued on May 13, 2003;

(23) U.S. Pat. No. 6,618,483 entitled "Elliptic Curve Encryption Systems issued September 9, 2003;

(24)–U.S. Pat. No. 6,925,564 entitled "Digital Signatures on a Smartcard" issued on August 02, 2005;

(25)-U.S. Pat. No. 6,785,813 entitled "Key Agreement and Transport Protocol with Implicit Signatures" issued on August 31, 2004;

(26)-U.S. Pat. No. 6,704,870 entitled "Digital Signatures on a Smartcard" issued on March 9, 2004; and

(27) U.S. Pat. Appl. Ser. No. 10/185,735 entitled "Strengthened Public Key Protocol" filed on July 1, 2000.