Certicom IPR contribution for
RFC 3446, RFC 2409,
draft-ietf-tls-ecc-12.txt,
draft-ietf-ipsec-ike-auth-ecdsa-05,
draft-ietf-ipsec-ike-ecp-groups-02 and
other IETF specifications using ECC technology

October 06, 2006

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 TLS and IPsec IKE protocols:

IETF TLS:

"The Transport Layer Security (TLS) Protocol -- Version 1.1;" RFC 4346, when used with either:

A. "ECC Cipher Suites for TLS" draft-ietf-tls-ecc-12.txt, October 17 2005, or

B. "ECMQV in TLS" (edited by Rob Dugal, but not yet posted); and

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," draft-ietf-ipsec-ike-auth-ecdsa-05; or

B. "ECC Groups For IKE and IKEv2," draft-ietf-ipsec-ike-ecp-groups-02

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). This agreement does not require such implementations to check that a third party certificate is licensed, it is understood that no license, implied or otherwise, is granted to such implementations for the use of certificates from Certificate Authorities who are not licensed.

It is important to clarify the situation stated in the preceding paragraph regarding certificates. If a CA creates certificates that use Certicom intellectual property then Certicom would expect this entity to obtain license from Certicom, which will be granted on reasonable and non-discriminatory terms. Certificates acquired from a licensed CA may then be used in any of the above protocols on a royalty free basis, i.e. without further payment to Certicom.

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. 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.

Should those end users requesting this royalty free patent license also have patents containing claims that are necessary and essential in the implementation of the above protocols, Certicom's grant of the royalty free license will be conditioned upon the grant to Certicom of a reciprocal license under such end user's necessary and essential claim (s).

Any party wishing to request a license should write to:

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

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. Appl. Ser. No. 96201322.3 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 Appl. Ser. No. 2202566 entitled "Digital Signatures on a Smartcard" filed on April 14, 1997;

(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. Appl. Ser. No. 2,174,261 entitled "Key Agreement and Transport Protocol with Implicit Signatures" filed on April 16, 1996;

(14) E.P. Pat. Appl. Ser. No. 96105920.1 entitled "Key Agreement and Transport Protocol with Implicit Signatures"-filed on April 16, 1996;

(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. Appl. Ser. No. 95926348.4 entitled "Elliptic Curve Encryption System" filed on July 31, 1995;

(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. Appl. Ser. No.2174260 entitled "Key Agreement Transport Protocol" filed on April 16, 1996;

(21)-E. P. Pat. Appl. Ser. No. 96105921.9 entitled "Key Agreement and Transport Protocol"-filed on April 21, 1996;

(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. Appl. Ser. No. 09/434,247 entitled "Digital Signatures on a Smartcard"–filed on November 5, 1999;

(25)-U.S. Pat. Appl. Ser. No, 09/558,256 entitled "Key Agreement and Transport Protocol with Implicit Signatures" filed on April 25, 2000;

(26)-U.S. Pat. Appl. Ser. No. 091942,492 entitled "Digital Signatures on a Smartcard" filed on August 29, 2001 and published on July 18, 2002; and

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