certicom

Via facsimile
Attn: PatCom Secretary
1-732-562-1571

Friday, April 12, 2002

Secretary, IEEE-SA Standards Board Patent Committee
Institute of Electrical and Electronics Engineers, Inc.
445 Hoes Lane
Piscataway, NJ 08855 USA

Attn: PatCom Secretary

As part of our ongoing review of Certicom's intellectual property, and in order to fulfill our obligations under this standard, we wish to provide a statement of Certicom's current position.

This letter sets forth Certicom's Intellectual Property in relation to the IEEE P802.15.3 Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPAN™).

Certicom is committed to making public-key cryptography viable in the most demanding environments, and particularly those encountered in small constrained devices such as wireless communicators, PDA's, and smart cards. Certicom's active research programs have generated and continue to generate significant intellectual property based on the most efficient ways to implement high-strength public-key cryptography. Accordingly, Certicom has invested significant financial resources and continues to protect its investments by patenting 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. In particular, Certicom has patents and patent applications that relate to the following aspects of the proposed IEEE 802.15.3 standard: point compression, public-key validation, key establishment protocols, implicit certificates, digital signature schemes, hardware-and software-based computational techniques for speeding up finite-field operations and modular integer arithmetic, and other computational techniques.

Certicom Corp.
5520 Explorer Drive, 4th Floor, Mississauga, Ontario, Canada L4W 5L1
t: 905.507.4220 f: 905.507.4230 www.certicom.com

certicom

If a license is required under any of Certicom's patents or patent applications to implement the cryptographic schemes in IEEE 802.15.3, Certicom is prepared to grant a license on fair and non-discriminatory terms and on reasonable terms and conditions, to any party to use those patents in implementing a scheme compliant with IEEE 802.15.3, provided that the licensee provides a similar grant for any relevant patents under their control to Certicom.

For information of licensing terms, please contact

Hervé Séguin
Director of Licensing
Phone: +1-905-501-3827.

To assist in the evaluation of intellectual property rights, a list of Certicom's patents is enclosed.

Yours very truly,

Certicom Corp.

Ian McKinnon
President and CEO

IM/bdk

Encl: Published Certicom Patent Portfolio

cc: Dr. Bob Heile (Chair IEEE P802.15 Working Group)
Dr. John Barr (Chair IEEE P802.15.3 Task Group)

Attachment

An implementation conforming to the IEEE 802.15.3 standard may require a license from Certicom for one or more of the following items.

Certicom is the owner of the following issued patents:

	Patent No.	Date Issued	Title
1	US 6,349,318	2002 02 19	Arithmetic processor for finite field and module integer arithmetic operations
2	US 6,337,909	2002 01 08	Generation of Session Keys for ElGamal-like Protocols from low Hamming Weight Integers
3	US 6,336,188	2002 01 01	Authenticated Key-agreement Protocol
4	FR 97 12690	2001 10 19	Procédé et appareil de génération de valeurs uniques impossibles à prédire
5	FR 98 01047	2001 10 19	Protocole de vérification d'une signature numérique
6	GB 2322775	2001 09 19	Digital Signature Protocol
7	GB 2318709	2001 09 05	Generating unique and unpredictable values
8	US 6,279,110 B1	2001 08 21	Masked Digital Signatures
9	US 6,212,281	2001 04 03	Digital Signature Protocol
10	US 6,195,433	2001 02 27	Private key validity and validation
11	US 6,178,507	2001 01 23	Data Card Verification System
12	GB 2 313 272 B	2000 12 13	Digital Signature Protocol with Reduced Bandwith
13	US 6,141,420	2000 10 31	Elliptic Curve Encryption Systems
14	US 6,134,325	2000 10 17	Key Transmission System
15	GB 2 321 741	2000 10 04	Data card verification system
16	US 6,122,736	2000 09 19	Key agreement and transport protocol with implicit signatures
17	FR 97 05976	2000 09 08	Protocole de signature numérique à largeur de bande reduite
18	US 6,097,813	2000 08 01	Digital Signature Protocol with Reduced Bandwidth
19	US 6,078,667	2000 06 20	Generating Unique and Unpredictable Values
20	US 6,049,815	2000 04 11	Method and Apparatus for Finite Field Multiplication
21	UK 2 309 809	2000 03 08	Transaction Verification Protocol for Smart Cards
22	US 5,999,626	1999 12 07	Digital Signatures on a Smart Card
23	FR 98 01204	1999 10 08	Système de Vérification de Cartes de Données
24	US 5,955,717	1999 09 21	Transaction Verification Protocol for Smart Cards
25	US 5,933,504	1999 08 03	Strengthened public key protocol
26	US 5,896,455	1999 04 20	Key Agreement and Transport Protocol with Implicit Signatures
27	US 5,889,865	1999 03 30	Key Agreement and Transport Protocol with Implicit Signatures
28	US 5,787,028	1998 06 28	Multiple Bit Multiplier
29	US 5,761,305	1998 06 02	Key Agreement and Transport Protocols with Implicit Signatures
30	EPO 0 337 985 B1	1995 06 14	Computational method and apparatus for finite field multiplier
31	GB 2 176 325	1989 07 19	Computational method and apparatus for finite field multiplier
32	CA 1 242 030	1988 09 13	Computational method and apparatus for finite field multiplier
33	US 4,745,568	1988 05 17	Computational method and apparatus for finite field multiplier

Certicom is the owner of the following joint patents with Motorola:

	Patent No.	Date Issued	Title
1	US 6,230,179	2001 05 08	Finite field multiplier with intrinsic modular reduction
2	US 6,009,450	1999 12 28	Finite field inverse circuit
3	US 5,982,895	1999 11 09	Finite field inverse circuit for use in an elliptic curve processor

Certicom has the exclusive rights to the following Entrust patent:

	Patent No.	Date Issued	Title
1	US 5,600,725	1997 02 04	Digital Signature Method and Key Agreement Method

Certicom also has published patent applications that relate to the following:

	Publication Number	Publication Date	Application Name
1	WO 99/57844 (PCT) and US20010016908A1	1999 11 11 (PCT) and 2001 08 23 (US)	Authenticated Key Agreement Protocol
2	WO 99/20020	1999 04 22	Key Validation Scheme
3	WO 00/39668	2000 07 06	A Method for Accelerating Cryptographic Operations on Elliptic Curves
4	WO 00/44129	2000 07 07	A Resilient Cryptographic Scheme
5	WO 99/23781	1999 05 14	Signature Verification for ElGamal Schemes
6	WO 99/25092 and US2001/0008013 A1	WO 1999 05 20 and US 2001 07 12	Masked Digital Signatures
7	WO 01/54374 A2	2001 07 26	Customizable Public Key Infrastructure and Development Tool for Same
8	WO 99/63426	1999 12 09	Accelerated Cryptographic Operations
9	WO 00/42733	2000 07 20	Method and Apparatus for Masking Cryptographic Operations
10	WO 00/55756	2000 09 21	System and Method for Efficient Basis Conversion
11	WO 00/52877	2000 09 08	Method and Apparatus for Finite Field Basis Conversion
12	WO 00/01109	2000 01 06	A Method for Preventing Key Share Attacks
13	WO 00/35223	2000 06 15	Enhanced Subscriber Authentication Protocol
14	WO 00/42511	2000 07 20	Method and Apparatus for Minimizing Differential Power Attacks on Processors
15	WO 99/49612	1999 09 30	Implicit Certificate Scheme
16	WO 01/95068 A2	2001 12 13	A Method for the Application of Implicit Signature Schemes
17	WO 00/05837	2000 02 03	Timing Attack Resistant Cryptographic System
18	WO 98/34202	1998 08 06	Data Card Verification System
19	WO 01/06997 A2 and A3	2001 01 25	Split-Key Key-Agreement Protocol
20	WO 98/51037	1998 11 12	A Log-On Verification Protocol
21	WO 99/21320	1999 04 29	Accelerated Signature Verification on an Elliptic Curve
22	WO 99/59286	1999 11 18	Private Key Validity and Validation
23	WO 98/18234	1998 04 30	Key Agreement and Transport Protocol with Implicit Signatures
24	WO 98/51032	1998 11 12	Two Way Authentication Protocol
25	WO 98/48345	1998 10 29	Arithmetic Processor
26	WO 99/39476	1999 08 09	Secure One-Way Authentication Communication System
27	WO 99/49386	1999 09 30	Accelerated Finite Field Operations on an Elliptic Curve
28	WO 00/25204	2000 05 04	Power-Signature Attack Resistant Cryptographic Scheme