FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. **1058**

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

RSA BSAFE® Crypto-C Micro Edition *by* RSA Security, Inc

(When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

RSA BSAFE® Crypto-C Micro Edition *by* RSA Security, Inc.
(*Software Version: 3.0;* Software)

and tested by the Cryptographic Module Testing accredited laboratory: ***Atlan Laboratories, NVLAP Lab Code 200492-0***
CRYPTIK Version 7.0
is as follows:

Cryptographic Module Specification:	Level 3	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: *(Multi-Chip Standalone)*	Level N/A	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 1	*Mitigation of Other Attacks:*	Level 1
Operational Environment:	Level 1	*tested in the following configuration(s):*	AIX 5L v5.3 (PowerPC 32-bit); AIX 5L v5.3 (PowerPC 64-bit); HP-UX 11.11 (PA-RISC 2.0 32-bit); HP-UX 11.23 (PA-RISC 2.0W 64-bit); HP-UX 11.31 (Itanium2 32-bit); HP-UX 11.31 (Itanium2 64-bit); Red Hat Enterprise Linux AS 4.0 (x86 32-bit) with LSB 3.0.3; Red Hat Enterprise Linux AS 5.0 (x86_64 64-bit) with LSB 3.0.3; Solaris 10 (SPARC v8 32-bit); Solaris 10 (SPARC v8+ 32-bit); Solaris 10 (SPARC v9 64-bit); Solaris 10 (x86_64 64-bit); VxWorks 5.5 (PowerPC 603 32-bit); VxWorks 5.5 (PowerPC 604 32-bit); VxWorks General Purpose Platform 6.0 (PowerPC 604); Windows Mobile 2003/Pocket PC (ARM 32-bit); Windows Mobile 5.0 (ARM 32-bit);Windows Mobile 6.0 Professional (ARM 32-bit); Windows 2003 Server SP2 (x86_64 64-bit) - Visual Studio 2005 SP1 build /MT option; Windows 2003 Server SP2 (Itanium 2 64-bit) - Visual Studio 2005 SP1 build /MT option; Windows 2003 Server SP2 (Itanium 2 64-bit) - Visual Studio 2005 SP1 build /MD option; Windows Vista Ultimate (x86 32-bit) - Visual Studio 2005 SP1 /MD option; Windows Vista Ultimate (x86_64 64-bit) - Visual Studio 2005 SP1 /MD option; Windows XP Professional SP2 (x86 32-bit) - Visual Studio 2005 SP1 /MT option (single user mode)

The following FIPS approved Cryptographic Algorithms are used: **AES (Cert. #810); AES GCM (Cert. #810, vendor affirmed: SP 800-38D); DRBG (Cert. #2); DSA (Cert. #300); ECDSA (Certs. #92 and #93); HMAC (Cert. #449); RNG (Cert. #466); RSA (Cert. #390); SHS (Cert. #807); Triple-DES (Cert. #690)**

The cryptographic module also contains the following non-FIPS approved algorithms: **DES; DES40; Diffie-Hellman; EC Diffie-Hellman; ECAES (non-compliant); ECIES; HMAC MD5; MD2; MD5; PBKDF1 SHA-1; PBKDF2 HMAC SHA-1/SHA-224/SHA-256/SHA-384/SHA-512 (non-compliant); RC2; RC4; RC5; RSA (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength; non-compliant less than 80 bits of encryption strength); RSA PKCS #1 v2.0 (OAEP; non-compliant)**

Overall Level Achieved: 1

Signed on behalf of the Government of the United States

Signature: William Barker

Dated: December 1, 2008

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: November 24, 2008

Director, Industry Program Group
Communications Security Establishment Canada