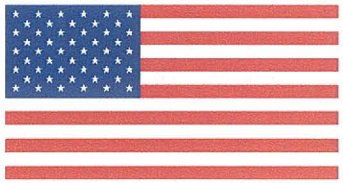
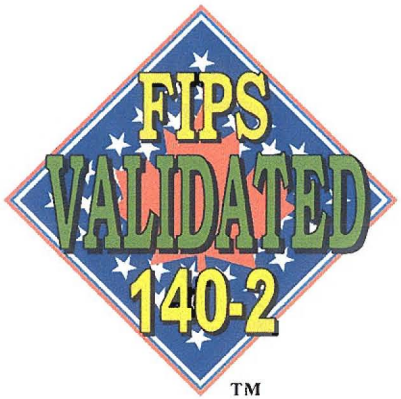
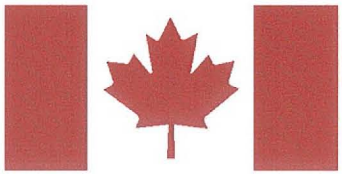
FIPS 140-2 Validation Certificate



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





The Communications Security Establishment of the Government of Canada

Certificate No. **1048**

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-J JCE Provider Module *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-J JCE Provider Module *by* RSA Security, Inc.
(*Software Version: 4.0;* 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 1	*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):* 32-bit x86 Intel Pentium M w/ Windows XP SP2 Professional with Sun JRE 1.4.2; 32-bit x86 Intel Pentium M w/ Windows XP SP2 Professional with Sun JRE 1.5; 32-bit x86 Intel Pentium M w/ Windows XP SP2 Professional with Sun JRE 1.6 (single-user mode)	

The following FIPS approved Cryptographic Algorithms are used: **AES (Cert. #669); DSA (Cert. #251); ECDSA (Cert. #72); HMAC (Cert #353); RNG (Cert. #389 and vendor affirmed: SP 800-90); RSA (Cert.#311); SHS (Cert. #702); Triple-DES (Cert. #614)**

The cryptographic module also contains the following non-FIPS approved algorithms: **AES-GCM (non-compliant); DES; Diffie-Hellman; DESX; ECAES; EC Diffie-Hellman; ECDHC; ECIES; MD2; MD5; PBE (SHA1 and Triple-DES); RIPEMD 160; RNG (X9.31 non-compliant, MD5 and SHA1); RC2; RC4; RC5; RSA OAEP (for key transport); Raw RSA; RSA Keypair Generation MultiPrime; RSA (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength; non-compliant less than 80 bits of encryption strength); HMAC-MD5**

Overall Level Achieved: 1

Signed on behalf of the Government of the United States

Signature: William C Barker

Dated: October 27, 2008

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: October 20, 2008

Director, Industry Program Group
Communications Security Establishment Canada