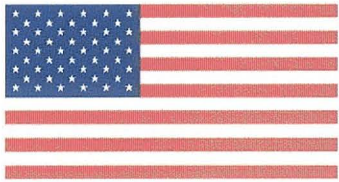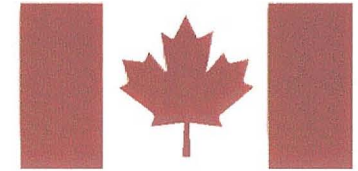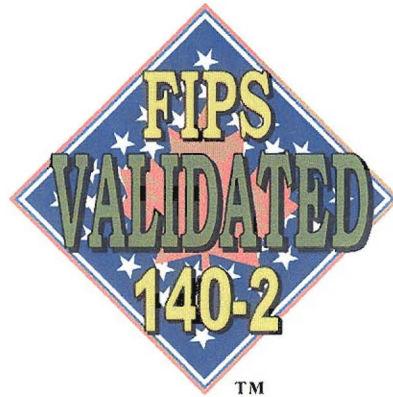# FIPS 140-2 Validation Certificate

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

The Communications Security Establishment of the Government of Canada

TM

Certificate No. 1051

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:

OpenSSL FIPS Object Module by Open Source Software Institute

(When built, installed, protected and initialized as specified in the provided Security Policy. Appendix B of the provided Security Policy specifies the actual distribution tar file containing the source code of this module. There shall be no additions, deletions or alterations to the tar file contents as used during module build. The distribution tar file shall be verified as specified in Appendix B of the provided Security Policy. Installation and protection shall be completed as specified in Appendix A of the provided Security Policy. Initialization shall be invoked as per Section 2.3 of the provided Security Policy. Any deviation from specified verification, protection, installation and initialization procedures will result in a non FIPS 140-2 compliant module.)

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:

OpenSSL FIPS Object Module *by* **Open Source Software Institute**
(Software Version: 1.2; Software)

and tested by the Cryptographic Module Testing accredited laboratory:
is as follows:

DOMUS IT Security Laboratory, NVLAP Lab Code 200017-0
CRYPTIK Version 7.0

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 N/A

Operational Environment: Level 1   *tested in the following configuration(s):* OpenSuSE Linux 32-bit Version 10.2 (gcc Compiler Version 4.1.2 20061115 prerelease); OpenSuSE Linux 64-bit Version 10.2 (gcc Compiler Version 4.1.2 20061115 prerelease); Windows XP Pro SP2 32 bit (Microsoft Visual C++ version 8); Windows XP Pro SP2 64 bit (Microsoft Visual C++ version 8) (single-user mode)

The following FIPS approved Cryptographic Algorithms are used: **Triple-DES (Cert. #627); AES (Cert. #695); DSA (Cert. #264); SHS (Cert. #723); HMAC (Cert. #373); RSA (Cert. #323); RNG (Cert. #407)**

The cryptographic module also contains the following non-FIPS approved algorithms: **Diffie-Hellman; RSA (key wrapping; key establishment methodology provides between 80 and 256 bits of encryption strength)**

Overall Level Achieved: 1

Signed on behalf of the Government of the United States
Signature: *William N Barker*
Dated: November 17, 2008

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada
Signature: *Cam F*
Dated: November 13, 2008

Director, Industry Program Group
Communications Security Establishment Canada