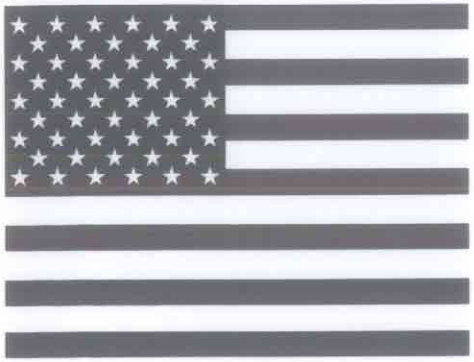
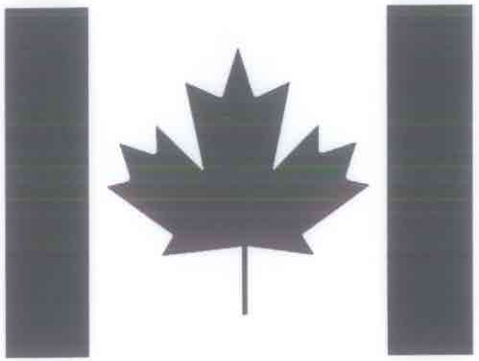


FIPS 140-1
Validation Certificate

Certificate No. 7



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

The Communications Security Establishment of the Government of Canada

The National Institute of Standards and Technology, as the United States FIPS 140-1 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-1 Cryptographic Module Validation Authority; hereby validate the FIPS 140-1 testing results of the Cryptographic Module identified as:

Netscape Security Module 1, by Netscape Communications Corporation

(when operated in the FIPS *mode for secure e-mail, certificate management, & password management)*

In accordance with the Derived Test Requirements for FIPS PUB 140-1, *Security Requirements for Cryptographic Modules.* FIPS-140-1 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive But Unclassified Information* (United States) or *Designated Information* (Canada) within computer and communications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS-140-1 so long as the product, throughout it's 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 140-1 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:

Netscape Security Module 1 ("fipscm_v1";software)

and tested by the Cryptographic Module Testing accredited laboratory: **InfoGard Laboratories, NVLAP LAB CODE 100432-0**
is as follows:

Cryptographic Module Design:	Level 2	*Module Interfaces:*	Level 2
Roles and Services:	Level 2	*Finite State Machine Model:*	Level 2
Physical Security: * *(multi-chip standalone)*	Level 2	*Software Security:*	Level 2
EMI / EMC:	Level 2	*Self Tests:*	Level 2
Key Management:	Level 2		

Operating System Security Level 2 is met when used in the following configuration: **Sun Sparc 5w/ Sun Solaris version 2.4SE (ITSEC-rated); meets Level 1 for WindowsNT 4.0 workstation (operated in single user mode)**

The following FIPS approved *Cryptographic Algorithms* are used: **DES (cert.#6, #10); DSA and SHA-1 (cert.#3)**

The Cryptographic module also contains the following non-FIPS approved algorithms: **RSA, MD5, MD2, RC4, RC5**

End user queries concerning the non-FIPS approved algorithms may be directed to their respective Cryptographic Module Validation Authority.

* (when correctly implementing the tamper evident mechanism specified in the security policy)

Overall Level Achieved: 2

Signed on behalf of the Government of the United States

Signature: Miles E. Smid

Dated: 29, August 97

Manager, Security Technology Group
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: [signature]

Dated: 27 August 97

Director ITS Services
The Communications Security Establishment