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. **1199**

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:

nShield F3 4000, nShield F3 2000, nShield F3 2000 for NetHSM, nShield F3 500 *and* nShield F3 500 for NetHSM *by* Thales - nCipher

(When operated in FIPS mode and initialized to Overall Level 2 per Security Policy)

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:

nShield F3 4000, nShield F3 2000, nShield F3 2000 for NetHSM, nShield F3 500
***and* nShield F3 500 for NetHSM *by* Thales - nCipher**
(Hardware Versions: nC4033P-4K0, nC4033P-2K0, nC4033P-2K0N, nC4133P-500 and nC4133P-500N, Build Standard N;
***Firmware Version: 2.38.4-2;* Hardware)**

---

and tested by the Cryptographic Module Testing accredited laboratory: ***DOMUS IT Security Laboratory, NVLAP Lab Code 200017-0***
CRYPTIK Version 7.0
is as follows:

Cryptographic Module Specification:	Level 2	*Cryptographic Module Ports and Interfaces:*	Level 2
Roles, Services, and Authentication:	Level 3	*Finite State Model:*	Level 2
Physical Security: (Multi-Chip Embedded)	Level 3 + EFP/EFT	*Cryptographic Key Management:*	Level 3
EMI/EMC:	Level 3	*Self-Tests:*	Level 2
Design Assurance:	Level 3	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level N/A	*tested in the following configuration(s):*	N/A

The following FIPS approved Cryptographic Algorithms are used: **AES (Cert. #994); AES GCM (Cert. #994, vendor affirmed); Triple-DES (Certs. #775 and #132); Triple-DES MAC (Cert. #775, vendor affirmed); DSA (Cert. #341); ECDSA (Cert. #121); SHS (Cert. #960); HMAC (Cert. #560); RSA (Cert. #478); RNG (Cert. #564)**

The cryptographic module also contains the following non-FIPS approved algorithms: **ARC FOUR; Aria; Camelia; CAST 6; DES; MD5; SEED; HMAC-MD5, HMAC-Tiger, HMAC-RIPEMD160; RIPEMD 160; Tiger; El-Gamal; KCDSA; HAS 160; AES (Cert. #994, key wrapping; key establishment methodology provides between 128 and 256 bits of encryption strength); Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength); EC Diffie-Hellman (key agreement; key establishment methodology provides 192 bits of encryption strength); RSA (key wrapping; key establishment methodology provides between 80 and 256 bits of encryption strength), ECMQV (key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength); NDRNG; DSA (FIPS 186-3, non-compliant); ECDSA (FIPS 186-3, non-compliant)**

Overall Level Achieved: 2

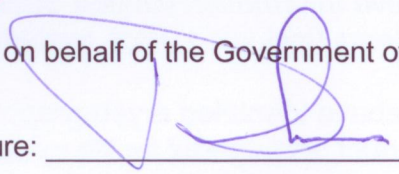
Signed on behalf of the Government of the United States

Signature: Dawn F. Dodson

Dated: 06 October 2009

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: 

Dated: 01 October 2009.

Director, Industry Program Group
Communications Security Establishment Canada