FIPS 140-2 Consolidated Validation Certificate

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

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0040

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below 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 a cryptographic module identified below 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 consolidated 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.

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 are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: Michael D Cooper

Dated: 12/5/2014

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 12/05/2014

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2118	04/03/2014	NonStop Volume Level Encryption (NSVLE)	Hewlett-Packard Development Company, L.P.	Software Version: 2.0
2121	04/03/2014	nShield F2 500+ [1], nShield F2 1500+ [2] and nShield F2 6000+ [3]	Thales-eSecurity Inc.	Hardware Versions: nC3423E-500 [1], nC3423E-1K5 [2] and nC3423E-6K0 [3], Build Standard N; Firmware Version: 2.51.10-2
2122	04/04/2014	VMware Cryptographic Module	VMware, Inc.	Software Version: 1.0
2123	04/09/2014	McAfee Firewall Enterprise Virtual Appliance for VMware	McAfee, Inc.	Software Version: 8.3.1
2124	04/09/2014	Cryptographic Security Kernel	Vidyo, Inc.	Software Version: 2
2125	04/09/2014	ACT2Lite Module	Cisco Systems, Inc.	Hardware Version: 15-14497-02(NX315) or 15-14497-02(AT90S072); Firmware Version: 1.5
2126	04/09/2014	Integral AES 256 Bit Crypto SSD Underlying PCB	Integral Memory PLC.	Hardware Versions: INSSD32GS25MCR140-2(R); INSSD64GS25MCR140-2(R); INSSD128GS25MCR140-2(R); INSSD256GS25MCR140-2(R); INSSD512GS25MCR140-2(R); INSSD1TS25MCR140-2(R); INSSD32GS18MCR140-2(R); INSSD64GS18MCR140-2(R); INSSD128GS18MCR140-2(R); INSSD256GS18MCR140-2(R); INSSD512GS18MCR140-2(R); INSSD1TGS18MCR140-2(R); Firmware Version: S5FDM018
2127	04/09/2014	IDProtect Duo with LASER PKI	Athena Smartcard, Inc.	Hardware Version: STMicroelectronics ST23YR80 Rev. G; Firmware Version: Athena IDProtect 0204.0355.0702 with LASER PKI Applet 3.0
2129	04/25/2014	RFS7000 SERIES Wireless Controller	Motorola Solutions, Inc.	Hardware Versions: RFS-7010 and RFS-7010 GR; Firmware Version: 5.4.10.0-050GR

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2133	04/25/2014	SecureAgent® Software Cryptographic Module	SecureAgent® Software Inc.	Software Version: 2.2.006
2134	04/24/2014	RF-7800W Broadband Ethernet Radio	Harris Corporation	Hardware Versions: RF-7800W-OU50x, OU47x and OU49x; Firmware Version: 2.00
2135	04/24/2014	CloudLink Crypto Module	AFORE Solutions Inc.	Software Version: 1.0
2137	04/29/2014	McAfee Vulnerability Manager Cryptographic Module	McAfee, Inc.	Software Version: 1.0
2138	04/29/2014	Symantec Java Cryptographic Module	Symantec Corporation	Software Version: 1.2
2139	04/30/2014	IBM® z/VM® Version 6 Release 3 System SSL Cryptographic Module	IBM® Corporation	Hardware Version: z10 CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863; Software Version: 5735FAL00: z/VM Version 6 Release 3 plus APAR PM95516
2140	04/30/2014	Uplogix 430 [1], 3200 [2], 500 [3] and 5000 [4]	Uplogix, Inc.	Hardware Version: 43-1102-50 [1], 37-0326-04 [2], 61-5050-33 [3] and 61-5500-33 [4] with Tamper Evident Labels Part No. (61-0001-00); Firmware Version: 4.6.4.22900g