FIPS 140-2 Consolidated Validation Certificate

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

FIPS VALIDATED 140-2 TM

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0041

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 J Cooper
Dated: 3 June 2014

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:
Dated: 3 June 2014

A/ Director, Architecture and Technology Assurance
Communications Security Establishment Canada

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2128	05/20/2014	Gigamon Linux-Based Cryptographic Module	Gigamon Inc.	Software Version: 1.0
2130	05/06/2014	SCS Linux Kernel Cryptographic Services module	Northrop Grumman M5 Network Security	Software Version: kernel-PAE-2.6.32.14-127.scs.fips.fc12.i686
2131	05/30/2014	Network Security Platform Sensor M-8000 P	McAfee, Inc.	Hardware Version: P/N M-8000 P, Version 1.40; FIPS Kit P/N IAC-FIPS-KT8; Firmware Version: 7.1.15.4
2132	05/30/2014	Network Security Platform Sensor M-8000 S	McAfee, Inc.	Hardware Version: P/N M-8000 S, Version 1.40; FIPS Kit P/N IAC-FIPS-KT8; Firmware Version: 7.1.15.4
2141	05/06/2014	Brocade® FCX L2/L3 Switch and Brocade FastIron® SX Series L2/L3 Switch	Brocade Communications Systems, Inc.	Hardware Versions: FI-SX800-S, FI-SX1600-AC, FI-SX1600-DC, FCX624S, FCX624S-HPOE-ADV, FCX624S-F-ADV, FCX648S, FCX648S-HPOE and FCX648S-HPOE-ADV with FIPS Kit (P/N Brocade XBR-000195); Firmware Version: IronWare Release R07.3.00c
2142	05/06/2014	RSA BSAFE® Crypto-C Micro Edition	RSA, The Security Division of EMC	Software Version: 3.0.0.17
2143	05/06/2014	Dell AppAssure Crypto Library	Dell, Inc.	Software Version: 1.0
2144	05/06/2014	FortiGate-3950B/3951B	Fortinet, Inc.	Hardware Versions: FortiGate-3950B and FortiGate-3951B with SKU-FIPS-SEAL-RED; Firmware Version: FortiOS v4.0, build3767, 130920

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2145	05/13/2014	Cisco 1941, 2901, 2911, 2921, 2951, 3925, 3945 Integrated Services Routers (ISRs) and ISM	Cisco Systems, Inc.	Hardware Versions: 1941 [12], 2901 [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, A], 2911 [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11,13, B], 2921 [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, C], 2951 [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, D], [3925, 3945] [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 14, E], PVDM2-8 [1], PVDM2-16 [2], PVDM2-32 [3], PVDM2-48 [4], PVDM2-64 [5], PVDM3-16 [6], PVDM3-32 [7], PVDM3-64 [8], PVDM3-128 [9], PVDM3-192 [10], PVDM3-256 [11], ISM-VPN-19 [12], ISM-VPN-29 [13], ISM-VPN-39 [14], FIPS-SHIELD-2901= [A], FIPS-SHIELD-2911= [B], FIPS-SHIELD-2921= [C], FIPS-SHIELD-2951= [D] and FIPS-SHIELD-3900= [E] with [FIPS Kit (CISCO-FIPS-KIT=), Revision -B0]; Firmware Version: IOS 15.2(4)M5
2146	05/13/2014	Cisco 881W, 881GW, 1941W, 891W, C819HGW+7-A-A-K9, C819HGW-V-A-K9, C819HGW-S-A-K9, and C819HWD-A-K9 Integrated Services Routers (ISRs)	Cisco Systems, Inc.	Hardware Versions: Cisco 881W, 881GW, 891W, C819HGW+7-A-A-K9, C819HGW-V-A-K9, C819HGW-S-A-K9, C819HWD-A-K9 and 1941W with [FIPS Kit (CISCO-FIPS-KIT=), Revision -B0]; Firmware Version: Router Firmware Version: IOS 15.2(4)M5 and AP Firmware Version: 15.2.2-JB
2147	05/13/2014	SafeNet LUNA® EFT	SafeNet, Inc.	Hardware Version: GRK-15, Version Code 0100; Firmware Version: MAL1.1
2148	05/13/2014	nShield F3 10+ [1], nShield F3 500+ [2], nShield F3 6000+ [3], nShield F3 500+ for nShield Connect+ [4], nShield F3 1500+ for nShield Connect+ [5] and nShield F3 6000+ for nShield Connect+ [6]	Thales e-Security Inc.	Hardware Versions: nC4033E-010 [1], nC4433E-500 [2], nC4433E-6K0 [3], nC4433E-500N [4], nC4433E-1K5N [5] and nC4433E-6K0N [6], Build Standard N; Firmware Version: 2.51.10-3

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2149	05/13/2014	nShield F3 10+ [1], nShield F3 500+ [2], nShield F3 6000+ [3], nShield F3 500+ for nShield Connect+ [4], nShield F3 1500+ for nShield Connect+ [5] and nShield F3 6000+ for nShield Connect+ [6]	Thales e-Security Inc.	Hardware Versions: nC4033E-010 [1], nC4433E-500 [2], nC4433E-6K0 [3], nC4433E-500N [4], nC4433E-1K5N [5] and nC4433E-6K0N [6], Build Standard N; Firmware Version: 2.51.10-2
2150	05/13/2014	Dell-CREDANT Cryptographic Kernel (Mac Kernel Mode) [1], Dell-CREDANT Cryptographic Kernel (Mac User Mode) [2] and Dell-CREDANT Cryptographic Kernel (Linux User Mode) [3]	Dell, Inc.	Software Version: 1.8 [1,2,3]
2151	05/13/2014	ProtectV StartGuard	SafeNet, Inc.	Software Version: 1.0
2152	05/13/2014	Cisco 2901, 2911, 2921, 2951, 3925, 3925E, 3945, 3945E and VG350 Integrated Services Routers (ISRs)	Cisco Systems, Inc.	Hardware Versions: 2901 [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, A], 2911 [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, B], 2921 [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, C], 2951 [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, D], [3925, 3925E, 3945, 3945E and VG350] [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, E], PVDM2-8 [1], PVDM2-16 [2], PVDM2-32 [3], PVDM2-48 [4], PVDM2-64 [5], PVDM3-16 [6], PVDM3-32 [7], PVDM3-64 [8], PVDM3-128 [9], PVDM3-192 [10], PVDM3-256 [11], FIPS-SHIELD-2901= [A], FIPS-SHIELD-2911= [B], FIPS-SHIELD-2921= [C], FIPS-SHIELD-2951= [D] and FIPS-SHIELD-3900= [E] with [FIPS Kit (CISCO-FIPS-KIT=), Revision -B0]; Firmware Version: IOS 15.2(4)M5
2153	05/13/2014	McAfee Firewall Enterprise Virtual Appliance for Crossbeam	McAfee, Inc.	Software Version: 8.3.1
2154	05/14/2014	McAfee Firewall Enterprise 1100E, 2150E and 4150E	McAfee, Inc.	Hardware Versions: NSA-1100-FWEX-E, NSA-2150-FWEX-E, NSA-4150-FWEX-E with FRU-686-0089-00; Firmware Version: 8.3.1

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2155	05/14/2014	VMware NSS Cryptographic Module	VMware, Inc.	Software Version: 1.0
2156	05/15/2014	Dell-CREDANT Cryptographic Kernel (Windows Kernel Mode) [1] and Dell-CREDANT Cryptographic Kernel (Windows User Mode) [2]	Dell, Inc.	Software Version: 1.8 [1,2]
2157	05/20/2014	Mocana Cryptographic Suite B Hybrid Module	Mocana Corporation	Hardware Version: Freescale P2020 SEC 3.1; Software Version: 5.5fi
2158	05/20/2014	VaultIC405™, VaultIC421™, VaultIC441™	INSIDE Secure	Hardware Versions: P/Ns: ATVaultIC405, ATVaultIC421 and ATVaultIC441; Platforms: ATVaultIC405M Silicon Rev C, ATVaultIC421M Silicon Rev C and ATVaultIC441M Silicon Rev C; Firmware Version: 1.0.1
2159	05/27/2014	Unified Crypto Module	Comtech EF Data Corporation	Hardware Version: PL-0000235-2; Firmware Version: 2.1.1
2160	05/27/2014	Cisco 819G-4G-A-K9, 819G-4G-V-K9, 819H-K9, 819G-S-K9, 819HG-4G-G-K9, 891, 881, 1905, 1921 and 1941 Integrated Services Routers (ISRs)	Cisco Systems, Inc.	Hardware Versions: 819G-4G-A-K9 , 819G-4G-V-K9 , 819H-K9 , 819G-S-K9, 819HG-4G-G-K9, 881, 891, 1905 [1], 1921 [1], 1941 and FIPS-SHIELD-1900= [1] with [FIPS Kit (CISCO-FIPS-KIT=), Revision -B0]; Firmware Version: IOS 15.2(4)M5
2161	05/27/2014	McAfee Firewall Enterprise 1100F, 2150F and 4150F	McAfee, Inc.	Hardware Versions: (NSA-1100-FWEX-F, NSA-2150-FWEX-F, and NSA-4150-FWEX-F) with FRU-686-0089-00; Firmware Version: 8.3.1
2162	05/28/2014	Encryptics® Cryptographic Library	Encryptics	Software Version: 1.0.3.0