

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. 0047

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: 1 Dec 2014

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: DJ Mc [Signature]
Dated: 1 Dec 2014

ADirector, 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
2235	11/04/2014	McAfee Email Gateway for Virtual Environments	McAfee, Inc.	Software Version: 7.0.1
2273	11/04/2014	QTI Cryptographic Module on Crypto 5 Core	Qualcomm Technologies, Inc.	Hardware Version: Snapdragon 805; Software Version: 5.f1
2274	11/10/2014	VDX 6710, VDX 6720, VDX 6730, VDX 6740, VDX 6740T and VDX 8770 Switches	Brocade Communications Systems, Inc.	Hardware Version: Temporarily unavailable. Please see Security Policy for tested hardware versions and configurations; Firmware Version: Network OS (NOS) v4.1.1
2275	11/04/2014	Xirrus XR Series Wi-Fi Products	Xirrus, Inc.	Hardware Versions: XR-520 [1], XR-520H-FIPS [2], XR-620-FIPS [1], XR-630-FIPS [1], XR-2425H-FIPS [3], XR-2225 [1], XR-2235 [1], XR-2425 [1], XR-2435 [1], XR-2226 [1], XR-2236 [1], XR-2426 [1], XR-2436 [1], XR-4420 [1], XR-4430 [1], XR-4820 [1], XR-4830 [1], XR-4426 [1], XR-4436 [1], XR-4826 [1], XR-4836 [1], XR-6820 [1], XR-6830 [1], XR-6836 [1], XR-7220 [1], XR-7230 [1], XR-7620 [1], XR-7630 [1] and XR-7636 [1]; Enclosure (Form Factor): XE-6000-TBAR [1], XR-520H-FIPS [2] and XR-2425H-FIPS [3]; Firmware Version: AOS-7.1
2276	11/07/2014	McAfee NGFW Cryptographic Kernel Module	McAfee, Inc.	Software Version: 2.0
2277	11/07/2014	SKYWAN Cryptographic Module	ND SatCom Products GmbH	Hardware Version: F-11B13860 TQM8349L-CA Rev. 300; Firmware Version: Boot Loader FW version 2.002.4 and Application FW version 7.250.10
2278	11/14/2014	Cisco 4451-X Integrated Services Router (ISR) (with PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256)	Cisco Systems, Inc.	Hardware Version: ISR 4451-X with FIPS kit ISR4451-FIPS-Kit; Firmware Version: IOS-XE 3.10.2

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2279	11/14/2014	Brocade® FCX 624/648, ICX™ 6610, ICX 6450, ICX 6650 and SX 800/1600 Series	Brocade Communications Systems, Inc.	Hardware Versions: [FCX624S (P/N 80-1002388-08), FCX624S-HPOE-ADV (P/N 80-1002715-08), FCX624S-F-ADV (P/N 80-1002727-07), FCX648S (P/N 80-1002392-08), FCX648S-HPOE (P/N 80-1002391-10), FCX648S-HPOE-ADV (P/N 80-1002716-10), FCX-2XG (P/N 80-1002399-01), ICX 6610-24F-I (P/N 80-1005350-04), ICX 6610-24F-E (P/N 80-1005345-04), ICX 6610-24-I (P/N 80-1005348-05), ICX 6610-24-E (P/N 80-1005343-05), ICX 6610-24P-I (P/N 80-1005349-06), ICX 6610-24P-E (P/N 80-1005344-06), ICX 6610-48-I (P/N 80-1005351-05), ICX 6610-48-E (P/N 80-1005346-05), ICX 6610-48P-I (P/N 80-1005352-06), ICX 6610-48P-E (P/N 80-1005347-06), ICX 6450-24 (P/N 80-1005997-03), ICX 6450-24P (P/N 80-1005996-04), ICX 6450-48 (P/N 80-1005999-04), ICX 6450-48P (P/N 80-1005998-04), ICX 6450-C12-PD (P/N 80-1007578-01), ICX6650-32-E-ADV (P/N: 80-1007115-02), ICX6650-32-I-ADV (P/N: 80-1007116-02), ICX6650-40-E-ADV (P/N: 80-1007179-03), ICX6650-40-I-ADV (P/N: 80-1007181-03), ICX6650-48-E-ADV (P/N: 80-1007180-03), ICX6650-48-I-ADV (P/N: 80-1007182-03), ICX6650-56-E-ADV (P/N: 80-1007117-03), ICX6650-56-I-ADV (P/N: 80-1007118-03), ICX6650-80-E-ADV (P/N: 80-1007119-03), ICX6650-80-I-ADV (P/N: 80-1007120-03), FI-SX800-S (P/N 80-1003050-03 and 80-1007143-03), FI-SX1600-AC (P/N 80-1002764-02

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
				and 80-1007137-02), FI-SX1600-DC (P/N 80-1003005-02 and 80-1007138-02), SX-FISF (P/N 80-1002957-03), SX-FI-ZMR-XL (P/N 80-1006486-02), SX-FI-ZMR-XL-PREM6 (P/N 80-1007350-02), SX-ACPWR-SYS (P/N 80-1003883-02) and SX-DCPWR-SYS (P/N 80-1003886-02)] with FIPS Kit XBR-000195; Firmware Version: IronWare R08.0.01
2280	11/14/2014	KDH3000-CM	Kanguru Solutions(TM)	Hardware Version: 1.0; Firmware Version: V01.04.0000.0000
2281	11/14/2014	Brocade(R) MLXe(R) and Brocade NetIron(R) CER 2000 Series Ethernet Routers, Brocade NetIron CES 2000 Series Ethernet Switches	Brocade Communications Systems, Inc.	Hardware Version: Temporarily unavailable. Please see Security Policy for tested hardware versions and configurations; Firmware Version: Multi-Service IronWare R05.5.00ca
2282	11/14/2014	VIPNet Common Crypto Core	Infotecs	Software Version: 1.0