

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. 0048

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: 1/6/2015

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: [Signature]

Dated: 06/01/2015

[Signature] 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
2283	12/08/2014	VDX 6710, VDX 6720, VDX 6730, VDX 6740, VDX 6740T and VDX 8770 Switches	Brocade Communications Systems, Inc.	Hardware Versions: [BR-VDX6710-54-F and BR-VDX6710-54-R, BR-A-16-F (80-1004566-07 and 80-1006701-02), BR-VDX6720-16-R (80-1004567-07 and 80-1006702-02), BR-VDX6720-24-F (80-1004564-07 and 80-1006699-02), BR-VDX6720-24-R (80-1004565-07 and 80-1006700-02), BR-VDX6720-40-F (80-1004570-07 and 80-1006305-02), BR-VDX6720-40-R (80-1004571-07 and 80-1006306-02), BR-VDX6720-60-F (80-1004568-07 and 80-1006303-02) and BR-VDX6720-60-R (80-1004569-07 and 80-1006304-02), BR-VDX6730-16-F (80-1005649-03 and 80-1006709-02), BR-VDX6730-16-R (80-1005651-03 and 80-1006711-02), BR-VDX6730-24-F (80-1005648-03 and 80-1006708-02), BR-VDX6730-24-R (80-1005650-03 and 80-1006710-02), BR-VDX6730-32-FCOE-F (BR-VDX6730-24-F with BR-VDX6730-24VCS-01 and BR-VDX6730-24FCOE-01 Lic.), BR-VDX6730-32-FCOE-R (BR-VDX6730-24-R with BR-VDX6730-24VCS-01 and BR-VDX6730-24FCOE-01 Lic.), BR-VDX6730-40-F (80-1005680-03 and 80-1006719-02), BR-VDX6730-40-R (80-1005681-03 and 80-1006720-02), BR-VDX6730-60-F (80-1005679-03 and 80-1006718-02), BR-VDX6730-60-R (80-1005678-03 and 80-1006717-02), BR-VDX6730-76-FCOE-F (BR-VDX6730-60-F with BR-VDX6730-60VCS-01 and BR-VDX6730-60FCOE-01 Lic.) and BR-VDX6730-76-FCOE-R (BR-VDX6730-60-R with BR-VDX6730-

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
				60VCS-01 and BR-VDX6730-60FCOE-01 Lic.), BR-VDX6740-24-F, BR-VDX6740-24-R, BR-VDX6740-48-F, BR-VDX6740-48-R, BR-VDX6740-64-ALLSW-F and BR-VDX6740-64-ALLSW-R, BR-VDX6740T-24-F, BR-VDX6740T-24-R, BR-VDX6740T-48-F, BR-VDX6740T-48-R, BR-VDX6740T-64-ALLSW-F and BR-VDX6740T-64-ALLSW-R, BR-VDX8770-4-BND-AC, BR-VDX8770-4-BND-DC, BR-VDX8770-8-BND-AC and BR-VDX8770-8-BND-DC with FRUs (80-1006540-01, 80-1006539-02, 80-1006430-01, 80-1006080-01, 80-1006295-01, 80-1006294-02, 80-1006049-02, 80-1006293-02, 80-1006048-02, 80-1006431-01 and 80-1006429-01)]; Firmware Version: Network OS (NOS) v4.0.1
2284	12/03/2014	whiteCrypton Secure Key Box 4.6.0 Crypto Module	whiteCrypton Corporation	Software Version: 4.6.0
2285	12/03/2014	PacketAssure iQ1000	Ultra Electronics DNE Technologies	Hardware Version: Chassis v.003, PSM v.101; Firmware Version: 3.2.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2286	12/03/2014	Brocade® MLXe®, Brocade® NetIron® CER 2000 Ethernet Routers and Brocade CES 2000 Routers and Switches	Brocade Communications Systems, Inc.	Hardware Versions: {[BR-MLXE-4-MR-M-AC (P/N: 80-1006853-01), BR-MLXE-4-MR-M-DC (P/N: 80-1006854-01), BR-MLXE-8-MR-M-AC (P/N: 80-1004809-04), BR-MLXE-8-MR-M-DC (P/N: 80-1004811-04), BR-MLXE-16-MR-M-AC (P/N: 80-1006820-02), BR-MLXE-16-MR-M-DC (P/N: 80-1006822-02), BR-MLXE-4-MR2-M-AC (P/N: 80-1006870-01), BR-MLXE-4-MR2-M-DC (P/N: 80-1006872-01), BR-MLXE-8-MR2-M-AC (P/N: 80-1007225-01), BR-MLXE-8-MR2-M-DC (P/N: 80-1007226-01), BR-MLXE-16-MR2-M-AC (P/N: 80-1006827-02), BR-MLXE-16-MR2-M-DC (P/N: 80-1006828-02)] with Component P/Ns 80-1006778-01, 80-1005643-01, 80-1003891-02, 80-1002983-01, 80-1003971-01, 80-1003972-01, 80-1003811-02, 80-1002756-03, 80-1004114-01, 80-1004113-01, 80-1004112-01, 80-1004760-02, 80-1006511-02, 80-1004757-02, 80-1003009-01, 80-1003052-01, 80-1003053-01, NI-CER-2048F-ADVPREM-AC (P/N: 80-1003769-07), NI-CER-2048F-ADVPREM-DC (P/N: 80-1003770-08), NI-CER-2048FX-ADVPREM-AC (P/N: 80-1003771-07), NI-CER-2048FX-ADVPREM-DC (P/N: 80-1003772-08), NI-CER-2024F-ADVPREM-AC (P/N: 80-1006902-02), NI-CER-2024F-ADVPREM-DC (P/N: 80-1006904-02), NI-CER-2024C-ADVPREM-AC (P/N: 80-1007032-02), NI-CER-2024C-ADVPREM-DC (P/N: 80-1007034-02), NI-CER-2048C-ADVPREM-AC (P/N: 80-

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
				1007039-02), NI-CER-2048C-ADVPREM-DC (P/N: 80-1007040-02), NI-CER-2048CX-ADVPREM-AC (P/N: 80-1007041-02), NI-CER-2048CX-ADVPREM-DC (P/N: 80-1007042-02), BR-CER-2024F-4X-RT-DC (P/N: 80-1007212-01), BR-CER-2024C-4X-RT-DC (P/N: 80-1007213-01), BR-CER-2024F-4X-RT-AC (P/N: 80-1006529-01), BR-CER-2024C-4X-RT-AC (P/N: 80-1006530-01), NI-CER-2024-2X10G (P/N: 80-1003719-03), BR-CES-2024C-4X-AC (P/N: 80-1000077-01), BR-CES-2024C-4X-DC (P/N: 80-1007215-01), BR-CES-2024F-4X-AC (P/N: 80-1000037-01), BR-CES-2024F-4X-DC (P/N: 80-1007214-01), RPS9 (P/N: 80-1003868-01) and RPS9DC (P/N: 80-1003869-02) } with FIPS Kit XBR-000195; Firmware Version: Multi-Service IronWare R05.6.00aa
2287	12/03/2014	Network Security Platform Sensor M-1250, M-1450, M-2750, M-2850, M-2950, M-3050, M-4050 and M-6050	McAfee, Inc.	Hardware Versions: P/Ns M-1250 Version 1.10 [1], M-1450 Version 1.10 [1], M-2750 Version 1.50 [1], M-2850 Version 1.00 [1], M-2950 Version 1.00 [1], M-3050 Version 1.20 [1], M-4050 Version 1.20 [2] and M-6050 Version 1.40 [2]; FIPS Kit P/Ns IAC-FIPS-KT2 [1] and IAC-FIPS-KT7 [2]; Firmware Version: 7.1.15.4
2288	12/03/2014	IBM Security QRadar FIPS Appliance	IBM Corporation	Hardware Version: QR24 with FIPS Replacement Labels (Part Number: 00AN000); Firmware Version: v7.1 MR1
2289	12/08/2014	Wireless Access Point AP-7131N-GR	Motorola Solutions, Inc.	Hardware Version: AP7131N-GR; Firmware Version: 4.0.4.0-046GRN

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2290	12/08/2014	INTEGRITY Security Services High Assurance Embedded Cryptographic Toolkit	Green Hills Software	Software Version: 2.0
2291	12/10/2014	Seagate Secure® TCG Opal SSC Self-Encrypting Drive FIPS 140-2 Module	Seagate Technology LLC	Hardware Versions: P/Ns 1HN162 and 1M2162; Firmware Version: 0002SDM7, 0002LIM7 and 0002SED7
2292	12/10/2014	RFS7000 Series Wireless Controller	Motorola Solutions, Inc.	Hardware Version: RFS-7010; Firmware Version: 4.1.4.0-0030GR
2294	12/12/2014	RSA BSAFE® Crypto-C Micro Edition	RSA, The Security Division of EMC	Software Version: 4.1

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2295	12/12/2014	Brocade(R) DCX, DCX 8510-8, DCX-4S and DCX 8510-4 Backbones, 6510 FC Switch, 6520 FC Switch and 7800 Extension Switch	Brocade Communications Systems, Inc.	Hardware Versions: {[DCX Backbone (P/Ns 80-1001064-10, 80-1006751-01, 80-1004920-04 and 80-1006752-01), DCX-4S Backbone (P/Ns 80-1002071-10, 80-1006773-01, 80-1002066-10 and 80-1006772-01), DCX 8510-4 Backbone (P/Ns 80-1004697-04, 80-1006963-01, 80-1005158-04 and 80-1006964-01), DCX 8510-8 Backbone (P/Ns 80-1004917-04 and 80-1007025-01)] with Blades (P/Ns 80-1001070-07, 80-1006794-01, 80-1004897-01, 80-1004898-01, 80-1002000-02, 80-1006771-01, 80-1001071-02, 80-1006750-01, 80-1005166-02, 80-1005187-02, 80-1001066-01, 80-1006936-01, 80-1001067-01, 80-1006779-01, 80-1001453-01, 80-1006823-01, 80-1003887-01, 80-1007000-01, 80-1002762-04, 80-1006991-01, 80-1002839-03, 80-1007017-01, 49-1000016-04, 49-1000064-02 and 49-1000294-05), 6510 FC Switch (P/Ns 80-1005232-03, 80-1005267-03, 80-1005268-03, 80-1005269-03, 80-1005271-03 and 80-1005272-03), 6520 FC Switch (P/Ns 80-1007245-03, 80-1007246-03, 80-1007242-03, 80-1007244-03, 80-1007257-03), 7800 Extension Switch (P/Ns 80-1002607-07, 80-1006977-02, 80-1002608-07, 80-1006980-02, 80-1002609-07 and 80-1006979-02)} with FIPS Kit P/N Brocade XBR-000195; Firmware Version: Fabric OS v7.2.0 (P/N 63-1001405-01)

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2296	12/12/2014	SRA EX6000 and SRA EX7000	Dell SonicWALL, Inc.	Hardware Versions: P/Ns 101-500210-68 Rev. A (SRA EX6000) and 101-500188-70 Rev. A (SRA EX7000); Firmware Version: SRA 10.7.1
2297	12/12/2014	SRA EX9000	Dell SonicWALL, Inc.	Hardware Version: P/N 101-500352-59 Rev A; Firmware Version: SRA 10.7.1
2300	12/16/2014	RSA BSAFE® Crypto-C Micro Edition	RSA, The Security Division of EMC	Software Version: 4.1
2301	12/18/2014	IOS Common Cryptographic Module (IC2M)	Cisco Systems, Inc.	Firmware Version: Rel 3(1.5.2)
2303	12/24/2014	ID-One PIV-C on Cosmo V8	Oberthur Technologies	Hardware Version: '0F'; Firmware Version: '5601'; Firmware Extension: '082371' with ID-One PIV Applet Suite 2.3.5
2304	12/24/2014	Accellion kiteworks Cryptographic Module	Accellion, Inc.	Software Version: KWLIB_1_0_1
2305	12/24/2014	Barco ICMP	Barco n.v.	Hardware Version: R7681133-08 [A] or R7681133-12 [B]; Firmware Version: 1.1 build 9202 [A] or 1.2 build 10163B [B]