

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. 0036

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: 11/9/14

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: [Signature]

Dated: 8/01/14

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
2050	12/03/2013	Brocade ICX 6430 and ICX 6450 Series Stackable Switch with FastIron 7.4.00a Firmware	Brocade Communications Systems, Inc	Hardware Versions: ICX-6430-24 P/N 80-1006002-02, ICX-6430-24P P/N 80-1006000-02, ICX-6430-48 P/N 80-1006003-02, ICX-6430-48P P/N 80-1006001-02, ICX-6450-24 P/N 80-1005997-02, ICX-6450-24P P/N 80-1005996-02, ICX-6450-48 P/N 80-1005999-03 and ICX-6450-48P P/N 80-1005998-02 with FIPS Kit (P/N Brocade XBR-000195); Firmware Version: FastIron v7.4.00a
2051	12/03/2013	μMACE	Motorola Solutions, Inc.	Hardware Version: P/N AT58Z04; Firmware Versions: R01.03.11, R01.03.12, or R01.03.13
2052	12/05/2013	MX Series 3D Universal Edge Routers with the Multiservices DPC	Juniper Networks, Inc	Hardware Version: [(MX240 with one to two 750-024064), (MX480 and MX960 with one to four 750-024064)] with (750-021524 and RE-S-2000-4096-S) and JNPR-FIPS-TAMPER-LBL; Firmware Version: JUNOS-FIPS 10.4R11
2053	12/05/2013	Datacryptor® 100M Ethernet	Thales e-Security	Hardware Version: 1600x439, Rev. 01 and 1600x439, Rev. 02; Firmware Version: 5.0
2054	12/05/2013	Datacryptor® 100M Ethernet	Thales e-Security	Hardware Version: 1600x439, Rev. 01 and 1600x439, Rev. 02; Firmware Version: 5.0
2055	12/05/2013	ActivIdentity Digital Identity Applet v2 on Gemalto IDCore 3020 (v2)	ActivIdentity	Hardware Version: A1023378; Firmware Version: Build#11 - M1005011+ Softmask V03, Applet Version: Digital Identity Applet Suite 2.7
2056	12/05/2013	RSA BSAFE® Crypto-C Micro Edition	RSA, The Security Division of EMC	Software Version: 4.0.1
2057	12/13/2013	RSA BSAFE® Crypto-J JSAFE and JCE Software Module	RSA, The Security Division of EMC	Software Version: 6.1

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2058	12/13/2013	RSA BSAFE® Crypto-J JSAFE and JCE Software Module	RSA, The Security Division of EMC	Software Version: 6.1
2059	12/13/2013	Gemini	Sony Corporation	Hardware Version: 1.0.0; Firmware Version: 2.0.0
2060	12/13/2013	Oracle Solaris Kernel Cryptographic Framework with SPARC T4 and SPARC T5	Oracle Corporation	Hardware Versions: 527-1437-01 and 7043165; Software Versions: 1.0 and 1.1
2061	12/13/2013	Oracle Solaris Kernel Cryptographic Framework	Oracle Corporation	Software Versions: 1.0 and 1.1
2062	12/17/2013	Cubic Managed Asset Tag (MAT) Cryptographic Module and Cubic SINK Cryptographic Module	Cubic Global Tracking Solutions	Hardware Version: 380270-1 Rev. -; Firmware Version: mat_v2_1_0 or sink_v2_1_0
2063	12/18/2013	PSD MODEL 145, 146, 147, 148	Neopost Technologies, S. A.	Hardware Version: 4150859LB; Firmware Version: P/N A0015972B, Version 28.02
2065	12/24/2013	Cisco 5508 Wireless LAN Controller	Cisco Systems, Inc.	Hardware Version: CT5508 Revision Number B0; FIPS Kit AIR-CT5508FIPSKIT=; Opacity Baffle Version A0; Firmware Version: 7.0.240.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2066	12/24/2013	Kanguru Defender 1000™	Kanguru Solutions	Hardware Versions: 1.0 (P/Ns KDF1000-4G, KDF1000-4G-Red, KDF1000-4G-Green, KDF1000-4G-Blue, KDF1000-4G-Yellow, KDF1000-4G-Brown, KDF1000-4G-Gray, KDF1000-4G-Silver, KDF1000-8G, KDF1000-8G-Red, KDF1000-8G-Green, KDF1000-8G-Blue, KDF1000-8G-Yellow, KDF1000-8G-Brown, KDF1000-8G-Gray, KDF1000-8G-Silver, KDF1000-16G, KDF1000-16G-Red, KDF1000-16G-Green, KDF1000-16G-Blue, KDF1000-16G-Yellow, KDF1000-16G-Brown, KDF1000-16G-Gray, KDF1000-16G-Silver, KDF1000-32G, KDF1000-32G-Red, KDF1000-32G-Green, KDF1000-32G-Blue, KDF1000-32G-Yellow, KDF1000-32G-Brown, KDF1000-32G-Gray, KDF1000-32G-Silver, KDF1000-64G, KDF1000-64G-Red, KDF1000-64G-Green, KDF1000-64G-Blue, KDF1000-64G-Yellow, KDF1000-64G-Brown, KDF1000-64G-Gray, KDF1000-64G-Silver, KDF1000-128G, KDF1000-128G-Red, KDF1000-128G-Green, KDF1000-128G-Blue, KDF1000-128G-Yellow, KDF1000-128G-Brown, KDF1000-128G-Gray and KDF1000-128G-Silver); Firmware Version: 2.03.10 and 2.05.10
2067	12/24/2013	McAfee Virtual SIEM Cryptographic Module	McAfee, Inc.	Software Version: 1.0
2068	12/24/2013	McAfee SIEM Cryptographic Module	McAfee, Inc.	Software Version: 1.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2069	12/24/2013	HP Networking 3800 Switch Series	Hewlett-Packard Company	Hardware Versions: Switches: (3800-24G-PoE+-2SFP+ Switch (J9573A) [1]; 3800-48G-PoE+-4SPF+ Switch (J9574A) [2]; 3800-24G-2SFP+ Switch (J9575A) [3]; 3800-48G-4SFP+ Switch (J9576A) [4]; 3800-24G-2XG Switch (J9585A) [5]; 3800-48G-4XG Switch (J9586A) [6]; 3800-24G-PoE+-2XG Switch (J9587A) [7]; 3800-48G-PoE+-4XG Switch (J9588A) [8] and 3800-24SFP-2SFP+ Switch (J9584A) [9]); Power Supplies: (J9580A [1,2,7,8] and J9581A [3,4,5,6,9]) with Tamper Evident Seal Kit: J9740A; Firmware Version: KA.15.10.0015