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. 0020

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: ______________________

Dated: 9/20/2012

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: ______________________

Dated: 6 September, 2012

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
1764	08/23/2012	IDProtect Duo with PIV	Athena Smartcard, Inc.	Hardware Version: Inside Secure AT90SC28880RCFV Rev. G; Firmware Version: Athena IDProtect 010E.1245.0002 with PIV Applet 3.0
1773	08/01/2012	565 Advanced Services Platform [1], 5100 Advanced Services Platform [2] and 5200 Advanced Services Platform [3]	Ciena® Corporation	Hardware Version: [NT0H50DAE5 REV 004 [1], NTPM50AAE5 Rev 11 [2], NT0H50AA Rev 014 [3], SP Card NT0H5066E5 Rev 04 [1] and NT0H41ABE5 Rev 8 [2,3], QOTR/E Card NT0H25BAE5 Rev 2 [1,2,3], OCM Card NT0H40BCE5 Rev 18 [3], Filler Card NT0H52ABE6 Rev 02 [1,2,3]] with FIPS security kit NT0H25BZ Rev 3; Firmware Version: 11.2
1774	08/01/2012	Luna® PCM	SafeNet Inc.	Hardware Version: LTK-02-0501; Firmware Version: 4.8.7
1775	08/01/2012	Luna® PCM Key Export (KE) Cryptographic Module	SafeNet, Inc.	Hardware Version: LTK-02-0501; Firmware Version: 4.8.7
1776	08/01/2012	Luna® CA4	SafeNet Inc.	Hardware Version: LTK-02-0501; Firmware Version: 4.8.7
1777	08/07/2012	Thales e-Security keyAuthority®	Thales e-Security, Inc.	Hardware Version: 1.0; Firmware Version: 3.0.3
1781	08/07/2012	IDflex V	Valid S/A	Hardware Version: Inside Secure AT90SC28872RCU Rev. G; Firmware Version: Valid IDflex V 010B.0352.0005 with LASER PKI Applet 3.0
1782	08/07/2012	ProtectServer Internal Express (PSI-e)	SafeNet, Inc.	Hardware Versions: VBD-04-0302 and VBD-04-0303; Firmware Version: 3.20.00

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1784	08/15/2012	HP Networking 5400 zl [1,2] and 8200 zl [3,4] Switch Series	Hewlett-Packard Company	Hardware Versions: 5406 zl [1] 5412 zl [2], 8206 zl [3], 8212 zl [4] [A]; Switches: (J8697A [1], J8698A [2], J9447A [3] and J9091A [4] [A]); Management Modules: (J8726A [1,2] and two J9092A [3,4] [A]); Power Supply: (J9306A: one [1,3] or two [2,4]); Support Module: (J9095A [3,4] [A]); Fabric Module: (two J9093A [3,4] [A]); Blank Plate: (5069-8563: five [1,3] or eleven [2,4]); PSU Blank Plate (5003-0753: one [1,3] or two [2,4]); Opacity Shield Kits: (J9710A [1], J9711A [2], J9712A [3] and J9713A [4]); High Performance Fan Trays: (J9721A [1], J9722A [2], J9723A [3] and J9724A [4]); with ([HP Gig-T/SFP+ V2 zl Mod: J9536A] and [Tamper Evident Seal Kit: J9709A]) [1,2,3,4]; Firmware Version: K.15.07.0003 [A]
1785	08/24/2012	RSA BSAFE® Crypto-J JSAFE and JCE Software Module	RSA Security, Inc.	Software Version: 6.0
1786	08/24/2012	RSA BSAFE® Crypto-J JSAFE and JCE Software Module	RSA Security, Inc.	Software Version: 6.0
1787	08/22/2012	IMB	GDC Technology (USA), LLC	Hardware Version: GDC-IMB-v1; Firmware Version: 1.1 with Security Manager Firmware Version 1.2.11
1788	08/22/2012	Cryptographic Security Kernel	Q1 Labs	Software Version: 1.0
1789	08/22/2012	McAfee Firewall Enterprise S1104, S2008, S3008, S4016, S5032 and S6032	McAfee, Inc.	Hardware Versions: FWE-S1104, FWE-S2008, FWE-S3008, FWE-S4016, FWE-S5032 and FWE-S6032; Firmware Version: 7.0.1.03 and 8.2.0
1791	08/24/2012	Red Hat Enterprise Linux 6.2 OpenSSH Client Cryptographic Module	Red Hat®, Inc.	Software Version: 2.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1792	08/24/2012	Red Hat Enterprise Linux 6.2 OpenSSH Server Cryptographic Module	Red Hat®, Inc.	Software Version: 2.0
1793	08/28/2012	HID Global Digital Identity Applet v2 on NXP JCOP 2.4.2	HID Global	Hardware Version: P/N P5CD145; Firmware Version: JCOP 2.4.2 R0 MaskID 53 and patchID 98, Digital Identity Applet Suite 2.7.1
1794	08/28/2012	Secure Generic Sub-System (SGSS), Version 3.5	Thales e-Security	Hardware Versions: 1213H130 Issue 6E, 1213R130 Issue 1, 1213P130 Issue 2 and 1213P130 Issue 2A; Software Version: 3.0.0
1795	08/31/2012	Sm@rtCafé Expert 6.0 FIPS	Giesecke & Devrient	Hardware Versions: P5CC081, P5CD081 and P5CD145; Firmware Version: Sm@rtCafTExpert 6.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1796	08/31/2012	Brocade DCX, DCX 8510-8, DCX-4S and DCX 8510-4 Backbones; 6510 FC Switch; and 7800 Extension Switch	Brocade Communications Systems, Inc.	Hardware Version: [6510 FC Switch (P/Ns 80-1005232-02, 80-1005267-02, 80-1005268-02, 80-1005269-02, 80-1005271-02 and 80-1005272-02) [A,B], 7800 Extension Switch (P/Ns 80-1002607-06, 80-1002608-06 and 80-1002609-06) [A,B], [DCX Backbone (P/Ns 80-1001064-08, 80-1001064-09, 80-1004920-02 and 80-1004920-03), DCX-4S Backbone (P/Ns 80-1002071-08, 80-1002071-09, 80-1002066-08 and 80-1002066-09), DCX 8510-4 Backbone (P/Ns 80-1004697-02, 80-1004697-03, 80-1005158-02 and 80-1005158-03) and DCX 8510-8 Backbone (P/Ns 80-1004917-02 and 80-1004917-03] with Blades (P/Ns 80-1001070-06 [A,B], 80-1004897-01, 80-1004898-01, 80-1002000-02, 80-1001071-02, 80-1000696-01, 80-1005166-01, 80-1005187-01, 80-1001066-01, 80-1001067-01, 80-1001453-01, 80-1003887-01, 80-1002762-04, 80-1000233-10, 80-1002839-02, 49-1000016-04, 49-1000064-02 and 49-1000294-05)] with FIPS Kit P/N Brocade XBR-000195; Firmware Version: Fabric OS v7.0.0b (P/N 63-1000968-01) [A] or Fabric OS v7.0.0b1 (P/N 63-1001098-01) [B]