FIPS 140-2 Consolidated Validation Certificate
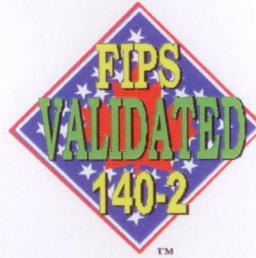
The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0017

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: _Dorai F Dodson_

Dated: _18 June 2012_

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: _11 June 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

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1695	05/18/2012	iPASOLINK MODEM AES Card	NEC Corporation	Hardware Version: 5.00; Firmware Version: NWA-055300-004
1712	05/03/2012	Kanguru Defender 2000	Kanguru Solutions	Hardware Versions: P/Ns KDF2000-2G, KDF2000-4G and KDF2000-8G, Version 1.0; Firmware Version: 2.02.10
1713	05/03/2012	BlackBerry Cryptographic Library	Research In Motion Ltd.	Software Version: 2.0.0.10
1715	05/03/2012	HP MSM430 Dual Radio 802.11N TAA AP [1], HP MSM430 Dual Radio 802.11N AP (WW) [2], HP MSM430 Dual Radio 802.11N AP (JP) [3], HP MSM460 Dual Radio 802.11N TAA AP [4], HP MSM460 Dual Radio 802.11N AP (WW) [5], HP MSM460 Dual Radio 802.11N AP (JP) [6], HP MSM466 Dual Radio 802.11N TAA AP [7], HP MSM466 Dual Radio 802.11N AP (WW) [8] and HP MSM466 Dual Radio 802.11N AP (JP) [9]	Hewlett-Packard Development Company, L.P.	Hardware Versions: J9654A [1], J9651A [2], J9652A [3], J9655A [4], J9591A [5], J9589A [6], J9656A [7], J9622A [8] and J9620A [9] with FIPS kit J9740A; Firmware Version: 5.6.0
1717	05/03/2012	Cisco Catalyst 6506-E [1], Catalyst 6509-E [2] and Catalyst 6513-E [3] Switches with Supervisor Cards (VS-S2T-10G or VS-S2T-10G-XL) and Line Cards (WS-X6908-10G or WS-X6908-10G-2TXL)	Cisco Systems, Inc.	Hardware Version: 6506-E -M0 [1], 6509-E -N0 [2], 6513-E -S0 [3], Supervisor Card VS-S2T-10G -B0, Supervisor Card VS-S2T-10G-XL -C0, Line Card WS-X6908-10G -A0, Line Card WS-X6908-10G-2TXL version -B0 and FIPS kit packaging (CVPN6500FIPS/KIT=); Firmware Version: 15.0(1)SY1
1718	5/7/2012	Juniper Networks LN1000 Mobile Secure Router	Juniper Networks, Inc.	Hardware Version: LN1000-V with JNPR-FIPS-TAMPER-LBLS; Firmware Version: 11.2S4
1719	05/22/2012	INTEGRITY Security Services High Assurance Embedded Cryptographic Toolkit	Green Hills Software	Software Version: 1.0.5

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1720	05/23/2012	mRevenector 2011	Francotyp-Postalia GmbH	Hardware Version: 580036020300/01; Firmware Version: Bootloader: 90.0036.0201.00/2011485001; Software-Loader: 90.0036.0206.00/2011485001
1721	05/23/2012	Vormetric Encryption Expert Cryptographic Module	Vormetric Inc.	Software Version: 4.4.1
1722	05/23/2012	Postal mRevenector US 2011	Francotyp-Postalia GmbH	Hardware Version: 580036020300/01; Firmware Version: Bootloader: 90.0036.0201.00/2011485001; Software-Loader: 90.0036.0206.00/2011485001; IBIP Application: 90.0036.0203.00/2011485001
1723	05/23/2012	SSG 140	Juniper Networks, Inc.	Hardware Versions: (SSG-140-SB and SSG-140-SH) with JNPR-FIPS-TAMPER-LBLS; Firmware Version: ScreenOS 6.3r6
1724	05/23/2012	Hughes SPACEWAY Crypto Kernel	Hughes Network Systems, LLC.	Firmware Version: 1.0
1725	05/29/2012	Postal mRevenector DE 2011	Francotyp-Postalia GmbH	Hardware Version: 580036020300/01; Firmware Versions: Bootloader: 90.0036.0201.00/2011485001; Software-Loader: 90.0036.0206.00/2011485001; FRANKIT-Application: 90.0036.0204.00/2011515001
1726	05/31/2012	Voltage IBE Cryptographic Module for z/OS	Voltage Security, Inc.	Hardware Version: Crypto Express2 card (CEX2C) [a separately configured version of 4764-001 (P/N 12R6536)]; Software Version: 4.0; Firmware Version: 4764-001(2096a16d)