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

November 2016

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 A Cooper

Dated: 12/2/2016

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 2 Dec. 2016

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

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
2785	11/07/2016	Protiva PIV Applet v1.55 on Protiva TOP DM Card	Gemalto	Hardware Version: GCX4-M2569420 [1, 2], GXP4-M2569430 [3, 4], GCX4-M2569422 [1, 2], GCX4-A1004155 [1, 2] and GCX4-A1026517 [1, 2]; Firmware Version: GCX4-FIPS EI07 (MPH051) [1], GCX4-FIPS EI08 [2], GXP4-FIPS EI07 (MPH052) [3] and GXP4-FIPS EI08 [4]; Applet Version: Protiva PIV Applet v1.55
2786	11/07/2016	SR-OS Cryptographic Module	Nokia Corporation	Firmware Version: 14.0R4
2787	11/07/2016	Panorama M-100 and M-500	Palo Alto Networks	Hardware Version: P/Ns 910-000030 Version 00D [1], 910-000092 Version 00D [1] and 910-000073 Version 00D [2]; FIPS Kit P/N 920-000140 Version 00A [1] and FIPS Kit P/N 920-000145 Version 00A [2]; Firmware Version: 7.1.3
2788	11/07/2016	Check Point CryptoCore	Check Point Software Technologies Ltd.	Software Version: 4.0
2789	11/08/2016	CN6000 Series Encryptors	Senetas Corporation Ltd, distributed by Gemalto NV (SafeNet)	Hardware Version: Senetas Corp. Ltd. CN6040 Series: A6040B (AC), A6041B (DC) and A6042B (AC/DC); Senetas Corp. Ltd. CN6100 Series: A6100B (AC), A6101B (DC) and A6102B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN6040 Series: A6040B (AC), A6041B (DC) and A6042B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN6100 Series: A6100B (AC), A6101B (DC) and A6102B (AC/DC); Firmware Version: 2.7.1
2790	11/08/2016	FortiGate-5140B Chassis with FortiGate-5001D Blade	Fortinet, Inc.	Hardware Version: Chassis: P09297-01; Blade: P1AB76; Air Filter: PN P10938-01; Front Filler Panel: PN P10945-01: ten; Rear Filler Panel: PN P10946-01: fourteen; Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: 5.2.7, build8892, 160328
2791	11/14/2016	CN8000 Multi-slot Encryptor	Senetas Corporation Ltd, distributed by Gemalto NV (SafeNet) and ID Quantique SA	Hardware Version: A8003-01, A8003-02, A8003-03, A8003-04, A8003-05, A8003-06, A8003-07, A8003-08, A8003-09 and A8003-10; Firmware Version: 2.7.1
2792	11/14/2016	BC-FNA (Bouncy Castle FIPS .NET API)	Legion of the Bouncy Castle Inc.	Software Version: 1.0.1
2793	11/15/2016	Advanced Configurable Cryptographic Environment (ACCE) v3 HSM Crypto Module	Ultra Electronics AEP	Hardware Version: 2870-G1; Firmware Version: 2r3, 2r4, and 3r2
2794	11/15/2016	CN Series Ethernet Encryptors	Senetas Corporation Ltd, distributed by Gemalto NV (SafeNet)	Hardware Version: Senetas Corp. Ltd. CN4000 Series: A4010B (DC), A4020B (DC); Senetas Corp. Ltd. CN6010 Series: A6010B (AC), A6011B (DC) and A6012B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN4000 Series: A4010B (DC), A4020B (DC); Senetas Corp. Ltd. & SafeNet Inc. CN6010 Series: A6010B (AC), A6011B (DC) and A6012B (AC/DC); Firmware Version: 2.7.1
2795	11/15/2016	Trusted Platform Module ST33TPHF2ESPI	STMicroelectronics	Hardware Version: ST33HTPH2E28AHA5, ST33HTPH2E32AHA5, ST33HTPH2E28AAE5 and ST33HTPH2E32AAE5; Firmware Version: 47.08

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
2796	11/22/2016	Seagate Secure(R) TCG Enterprise SSC Self-Encrypting Drive	Seagate Technology, LLC	Hardware Version: ST4000NM0121[1] and ST4000NM0131[2]; Firmware Version: BE52[1] and BE53[2]
2797	11/22/2016	PA-3060 and PA-7080 Firewalls	Palo Alto Networks	Hardware Version: PA-3060 P/N 910-000104-00C Rev. C and PA-7080 P/N 910-000122-00A with 910-000028-00B, 910-000117-00A, 910-000136-00A, or 910-000137-00A; FIPS Kit P/Ns: 920-000138-00A Rev. A and 920-000119-00A Rev. A; Firmware Version: 7.1.3
2798	11/23/2016	Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module v4.0 with CPACF	Red Hat(R), Inc.	Software Version: 4.0; Hardware Version: COP chips integrated within processor unit; Firmware Version: Feature 3863 (aka FC3863) with System Driver Level 22H
2799	11/28/2016	PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series and PA-7050 Firewalls	Palo Alto Networks	Hardware Version: PA-200 P/N 910-000015-00E Rev. E [1], PA-500 P/N 910-000006-00O Rev. O [2], PA-500-2GB P/N 910-000094-00O Rev. O [2], PA-2020 P/N 910-000004-00Z Rev. Z [3], PA-2050 P/N 910-000003-00Z Rev. Z [3], PA-3020 P/N 910-000017-00J Rev. J [4], PA-3050 P/N 910-000016-00J Rev. J [4], PA-4020 P/N 910-000002-00AB Rev. AB [5], PA-4050 P/N 910-000001-00AB Rev. AB [5], PA-4060 P/N 910-000005-00S Rev. S [5], PA-5020 P/N 910-000010-00F Rev. F [6], PA-5050 P/N 910-000009-00F Rev. F [6], PA-5060 P/N 910-000008-00F Rev. F [6] and PA-7050 P/N 910-000102-00B Rev. B with 910-000028-00B, 910-000117-00A, 910-000137-00A, 910-000136-00A [7]; FIPS Kit P/Ns: 920-000084-00A Rev. A [1], 920-000005-00A Rev. A [2], 920-000004-00A Rev. A [3], 920-000081-00A Rev. A [4], 920-000003-00A Rev. A [5], 920-000037-00A Rev. A [6] and 920-000112-00A Rev. A [7]; Firmware Version: 7.1.3
2800	11/30/2016	Palo Alto Networks VM-Series	Palo Alto Networks	Software Version: 7.1.3
2801	11/30/2016	Protiva™ PIV v2.0 using TOP DL v2 and TOP IL v2	Gemalto	Hardware Version: A1025258 and A1023393; Firmware Version: Build#11 - M1005011 + Softmask V04, Applet Version: PIV Applet v2.00 + OATH Applet v2.10