FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Canadian Centre for Cyber Security

July 2019

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Canadian Centre for Cyber Security, 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: 8/13/19

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: August 13, 2019

Manager, Product Assurance and Standards
Canadian Centre for Cyber Security

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3481	07/09/2019	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. CN6140 Series: A6140B (AC), A6141B (DC) and A6142B (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); Senetas Corp. Ltd. & SafeNet Inc. CN6140 Series: A6140B (AC), A6141B (DC) and A6142B (AC/DC); Firmware Version: 3.0.3
3482	07/09/2019	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: 3.0.3
3483	07/09/2019	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: 3.0.3
3484	07/09/2019	CN9000 Series Encryptors	Senetas Corporation Ltd, distributed by Gemalto NV (SafeNet)	Hardware Version: Senetas Corp. Ltd. CN9000 Series: A9100B (AC), A9101B (DC), A9102B (AC/DC); Senetas Corp. Ltd. CN9000 Series: A9120B (AC), A9121B (DC), A9122B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN9000 Series: A9100B (AC), A9101B (DC), A9102B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN9000 Series: A9120B (AC), A9121B (DC), A9122B (AC/DC); Firmware Version: 3.0.3
3485	07/09/2019	Aruba AP-214, AP-215, AP-224, AP-225, AP-228, AP-274, AP-275, AP-277, AP-324, and AP-325 Wireless Access Points	Aruba, a Hewlett Packard Enterprise company	Hardware Version: [AP-214-F1 (HPE SKU JW169A), AP-215-F1 (HPE SKU JW171A), AP-224-F1 (HPE SKU JW173A), AP-225-F1 (HPE SKU JW175A), AP-228-F1 (HPE SKU JW183A), AP-274-F1 (HPE SKU JW177A), AP-275-F1 (HPE SKU JW179A), AP-277-F1 (HPE SKU JW181A), AP-324-F1 (HPE SKU JW185A) and AP-325-F1 (HPE SKU JW187A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 8.2-FIPS
3486	07/10/2019	Enterprise Secure Key Manager	Utimaco Inc.	Hardware Version: HW-ESKM-V1 , Version 5.1; Firmware Version: 7.1.0

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3487	07/11/2019	Boot Manager in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016	Microsoft Corporation	Software Version: 10.0.14393.1770
3488	07/15/2019	ColorTokens OpenSSL FIPS Object Module	ColorTokens	Software Version: 2.0.11
3489	07/15/2019	Acme Packet 4600 [1] and Acme Packet 6300 [2] and Acme Packet 6350 [3]	Oracle Communications	Hardware Version: 4600 [1], 6300 [2] and 6350 [3]; Firmware Version: E-CZ8.2.0
3490	07/15/2019	Acme Packet 1100 [1] and Acme Packet 3900 [2]	Oracle Communications	Hardware Version: 1100 [1] and 3900 [2]; Firmware Version: E-CZ8.2.0
3491	07/15/2019	Acme Packet VME	Oracle Communications	Software Version: E-CZ8.2.0
3492	07/16/2019	Trusted Platform Module 2.0 SLB 9670	Infineon Technologies AG	Hardware Version: SLB 9670 (Package PG-UQFN-32-1 or PG-VQFN-32-13); Firmware Version: 7.85
3493	07/17/2019	LogRhythm FIPS Object Module for OpenSSL	LogRhythm	Software Version: 2.0.16
3494	07/17/2019	RUGGEDCOM Ethernet Switches and RUGGEDCOM Serial Device Server	Siemens Canada Ltd.	Hardware Version: M969F, M2100F, M2200F, RSG2100F, RSG2200F, RSG2488F, RS416F, RS900F, RS900GF, and RS940GF; Firmware Version: 4.2.2.F
3495	07/19/2019	Panzura CloudFS™ FIPS Cryptographic Module	Panzura, Inc.	Software Version: 1.0
3496	07/19/2019	Embedded Module and Embedded Module Lite	Persistent Systems, LLC	Hardware Version: P/Ns WR-5200, Versions 4.0, 6.0, 7.0 and WR-5250, Versions 1.0 and 3.0; Firmware Version: 19.3.2, 19.3.3 and 19.4.0
3498	07/24/2019	Ciena Waveserver Ai Encryption Module	Ciena® Corporation	Hardware Version: 186-1606-820-EB, Revision 001 with PCB P/N: 174-0534-220 Revision 2; Firmware Version: 1.3.5
3499	07/30/2019	Juniper Networks EX4600, QFX5100 and QFX5200 Ethernet Switches	Juniper Networks, Inc.	Hardware Version: EX4600-40F, QFX5100-24Q, QFX5100-48S, QFX5100-48SH, QFX5100-48T, QFX5100-48TH, QFX5100-96S, QFX5200-32C, QFX5200-48Y; Firmware Version: JUNOS 18.1R1
3500	07/31/2019	totemo Cryptographic Module (TCM)	Totemo AG	Software Version: 3.0