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

March 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: 4/4/2019

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 2019-04-02

Manager, Product Assurance and Standards
Canadian Centre for Cyber Security

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3382	03/22/2019	Titan Chip	Google, Inc.	Hardware Version: H1B2P; Firmware Version: gqfips-1.2
3383	03/22/2019	River Cryptographic Module	Google, Inc.	Hardware Version: RiverHD and RiverQD; Firmware Version: River-gqfips-1.2
3384	03/27/2019	Delta Cryptographic Module	Google, Inc.	Hardware Version: Delta [Configuration 0]; [Configuration 1]; [Configuration 2] with components ARM Cortex-M7 CPU, RR16FFGL_111UHD32768X39M16B8W0R1E1L1P0D0L16, RR16FFGL_111HS16384X8M16B8W1R1E1L0P0D0A0U20 and RR16FFGL_111HS32768X8M16B8W1R1E1L0P0D0A0U20; Firmware Version: Delta-gqfips-1.2
3387	03/01/2019	NetApp CryptoMod	NetApp, Inc.	Software Version: 2.1
3388	03/04/2019	Octopus Authentication Server Cryptographic Module	Secret Double Octopus Ltd.	Software Version: 2.0.5
3389	03/04/2019	wolfCrypt	wolfSSL Inc.	Software Version: 4.0
3390	03/05/2019	Bomgar FIPS Remote Support Appliance	Bomgar Corporation	Hardware Version: R630; Tamper-Evident Label Kit: BMG-720-1214-00; Front Bezel: 720-1199-01; Firmware Version: 4.4.2FIPS with 16.2.1FIPS
3391	03/06/2019	Security Builder FIPS Java Module	Certicom Corp.	Software Version: 2.9[1], 2.9.2[2]
3392	03/06/2019	Samsung SAS 12G TCG Enterprise SSC SEDs PM1643 Series	Samsung Electronics Co., Ltd.	Hardware Version: MZILT15THMLA-000H9, MZILT7T6HMLA-000H9, MZILT3T8HALS-000H9, MZILT1T9HAJQ-000H9 and MZILT920HAHQ-000H9; Firmware Version: P102
3393	03/08/2019	Ruckus Wireless, Inc. R710, R610, R720, T610 and T710 Wireless Access Points	Ruckus Wireless, Inc.	Hardware Version: R710, R610, R720, T610 and T710; Firmware Version: 3.6.0.3
3394	03/08/2019	NetX Crypto	Express Logic, Inc.	Software Version: 5.11SP1-FIPS
3395	03/11/2019	Secure Execution Environment (SEE) Loader	PrimeKey Labs GmbH	Hardware Version: 1.0.0; Firmware Version: V1.0.2-FIPS
3396	03/12/2019	Ultrastar® DC HC530 TCG Enterprise HDD	Western Digital Corporation	Hardware Version: P/Ns WUH721414AL5205 and WUH721414AL4205; Firmware Version: R075 or R07G
3397	03/12/2019	HPE Smart Array Gen10 P-Class RAID Controllers	Hewlett Packard Enterprise Development LP	Hardware Version: P408i-p SR Gen10, P408e-p SR Gen10, P408i-a SR Gen10, P816i-a SR Gen10, P204i-b SR Gen10, P408e-m SR Gen10, P204i-c SR Gen10, P416ie-m SR Gen10; Firmware Version: 1.34
3398	03/13/2019	Cisco Systems 3504, 5520, and 8540 Wireless LAN Controllers	Cisco Systems, Inc.	Hardware Version: 3504, 5520 and 8540; Firmware Version: 8.5
3399	03/13/2019	Honeywell Crypto Engine Core	Honeywell International Inc.	Hardware Version: 5.3.4
3400	03/13/2019	Honeywell Inline Crypto Engine (SDCC)	Honeywell International Inc.	Hardware Version: 3.0.0
3401	03/13/2019	Honeywell Pseudo Random Number Generator	Honeywell International Inc.	Hardware Version: 2.3.1

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3402	03/13/2019	Apple CoreCrypto Module v9.0 for Intel	Apple Inc.	Software Version: 9.0
3409	03/20/2019	RSA BSAFE(R) Crypto Module	RSA Security LLC	Software Version: 1.0.1
3410	03/20/2019	IBM 4768 Cryptographic Coprocessor Security Module	IBM Corporation	Hardware Version: P/Ns 4768-001, P/N: 01PP165-N36741 POST0 v0651 MB0 v0660 and 4768-001, P/N: 01KV353-N37513 POST0 v0651 MB0 v0650; Firmware Version: 6.0.12z P0662 M0663 P0652 F08A8 (d608bcad)
3411	03/21/2019	CryptoFlow Net Creator Java Crypto Module	Certes Networks, Inc.	Software Version: 1.0
3412	03/21/2019	Ultrastar® DC SS530 TCG Enterprise SSD	Western Digital Corporation	Hardware Version: P/Ns WUSTM3240ASS205, WUSTM3280ASS205, WUSTM3216ASS205, WUSTM3232ASS205, WUSTR6440ASS205, WUSTR6480ASS205, WUSTR6416ASS205, WUSTR6432ASS205, WUSTR6464ASS205, WUSTR1548ASS205, WUSTR1596ASS205, WUSTR1519ASS205, WUSTR1538ASS205, WUSTR1576ASS205, WUSTR1515ASS205; Firmware Version: R900, R901, R920 and R925
3413	03/22/2019	RF-7800W Broadband Ethernet Radio	Harris Corporation	Hardware Version: RF-7800W-OU50x, RF-7800W-OU47x and RF-7800W-OU49x; Firmware Version: 6.00
3414	03/22/2019	Trend Micro Cryptographic Module with CCJ 3.0.0	Trend Micro Inc.	Software Version: 3.0.0
3415	03/25/2019	Boot Manager in Windows 10 Enterprise LTSB	Microsoft Corporation	Software Version: 10.0.10240.17643
3416	03/25/2019	Juniper Networks MX240, MX480, MX960, MX2010, MX2020 3D Universal Edge Routers and EX9204, EX9208, EX9214 Ethernet Switches with RE1800 Routing Engine	Juniper Networks, Inc.	Hardware Version: MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with components identified in Security Policy Table 1; Firmware Version: Junos OS 17.3R2
3417	03/27/2019	IDPrime PIV v3.0 Applet on IDCore 3130 Platform	Gemalto	Hardware Version: P/N SLE78CFX400VPH with packaging A1977038 and P/N SLE78CLFX400VPH with packaging A1714221; Firmware Version: IDCore 3130 (Build09C) with Applets [PIV v3.0 (Build08), PIV Admin v3.0 (Build 08), MoC Server (version 1.1)]
3418	03/27/2019	Thycotic HSM Module	Thycotic Software LLC	Software Version: 1.2.5
3419	03/27/2019	Mojo Access Point	Mojo Networks, Inc.	Hardware Version: C-120 and C-130 with Tamper Evident Seal Kit: C-TPL-A; Firmware Version: 8.2.1

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3420	03/27/2019	EOS MACsec Bravo Hybrid Module	Arista Networks Inc.	Hardware Version: P/Ns Credo MACsec chip CMX42550 and Renesas Security chip R5H30211 or N313X; Chassis: DCS-7508N, Version 06.00; DCS-7512N, Version 00.06; DCS-7516N, Version 10.00; Supervisor: DCS-7500E-SUP, Version 01.02; DCS-7500-SUP2-D, Version 03.03; DCS-7516-SUP2, Version 10.00; Linecard: DCS-7500R2M-36CQ-LC, Version 21.01; Fixed Hardware: DCS-7280SRAM-48C6, Version 21.00; DCS-7280SRM-40CX2, Version 21.00; DCS-7280CR2M-30, Version 20.01; Firmware Version: 1.0
3421	03/28/2019	Oracle Linux 6 Kernel Crypto API Cryptographic Module	Oracle Corporation	Software Version: R6-1.0.0
3422	03/28/2019	Granada	Sony Imaging Products & Solutions Inc.	Hardware Version: 1.0.0; Firmware Version: 1.0.0
3423	03/31/2019	Juniper Networks MX104 3D Universal Edge Router with the Multiservices MIC	Juniper Networks, Inc.	Hardware Version: MX104 with RE-MX104 and MS-MIC-16G; Firmware Version: Junos OS 18.2R1