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

July 2017

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, 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: 8/1/2017

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: PV Cantano A/DIR ATA

Dated: 1 Aug 2017

Director, Architecture and Technology Assurance
Communications Security Establishment

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
2947	07/05/2017	NCoded Cryptographic Mobile Module	NCoded Communications LLC	Software Version: 2.1
2948	07/06/2017	Juniper Networks SRX5400, SRX5600, and SRX5800 Services Gateways with Junos 15.1X49-D75	Juniper Networks, Inc.	Hardware Version: SRX5400, SRX5600, SRX5800 with components identified in Security Policy Table 1 and JNPR-FIPS-TAMPER-LBLS; Firmware Version: JUNOS-FIPS-MODE 15.1X49-D75
2949	07/06/2017	Aruba 5400R zl2 Switch Series	Hewlett Packard Enterprise	Hardware Version: 5406R zl2 J9821A [1] and 5412R zl2 J9822A [2]; Interface Modules: (J9537A [2], J9546A [2], J9986A [1,2], 9987A [1,2], J9988A [1,2], J9989A [2], J9990A [1,2], J9991A [2], J9992A [2], J9993A [1,2], J9995A [1,2], J9996A [2]); Management Module: J9827A [1,2]; Firmware Version: KB.16.02.0015
2950	07/06/2017	HyperPKI™ HYP2003	Hypersecu Information Systems Inc.	Hardware Version: 1.0.0
2951	07/07/2017	InformaCast C Crypto Library	Singlewire Software	Software Version: 2.1
2952	07/07/2017	InformaCast Java Crypto Library	Singlewire Software	Software Version: 3.0
2953	07/07/2017	Attivo Cryptographic Module	Attivo Networks Inc.	Software Version: 1.0
2954	07/11/2017	HPE FlexNetwork MSR1000, MSR2000, MSR3000 and MSR4000 Router Series	Hewlett Packard Enterprise	Hardware Version: {HPE FlexNetwork MSR1002-4 Router (JG875A) with (JD574B, JD573B, and JD559A) or with (JD573B and JD559A) and opacity shield JG598A, HPE FlexNetwork MSR1003-8S AC Router (JH060A) with (JD560A, JD559A, and JD576A) and opacity shield JG598A, HPE FlexNetwork MSR2003 AC Router (JG411A) with (JD558A and JD574B) or with (JD559A, JD576A, and JF821A) and opacity shield JG598A, HPE FlexNetwork MSR2003 TAA-compliant AC Router (JG866A) with (JD558A and JD574B) or with (JD559A, JD576A, and JF821A) and opacity shield JG598A, HPE FlexNetwork MSR2004-24 AC Router (JG734A) with (JD560A, JD559A, JF821A, and JD576A) and opacity shield JG598A, HPE FlexNetwork MSR2004-48 Router (JG735A) with (JD560A, JD559A, JF821A, and JD576A) and opacity shield JG598A, HPE FlexNetwork MSR3012 AC Router (JG409A) with (JG604A, JF281A, and JG430A) and opacity shield JG599A, HPE FlexNetwork MSR3044 Router (JG405A) with (JD559A, JD560A, JD561A, JG438A, JG442A, JG443A, and JG447A) and opacity shield JG600A, HPE FlexNetwork MSR3064 Router (JG404A) with (JG604A, JF281A, JG211A, JG737A, JG430A, JG447A, JD624A, JG415A, JD613A, JG457A, and JG435A) and opacity shield JG601A, HPE FlexNetwork MSR4060 Router Chassis (JG403A) with JG869A and (JG415A, JF254B, JG435A, and JG447A) and opacity shield JG602A, HPE FlexNetwork MSR4080 Router Chassis (JG402A) with JG869A and (JF841A, JG416A, JF841A, JG415A, JF254B, JC160A, JC159A, and JF837A) and opacity shield JG603A} with tamper evidence labels: JG585A or JG586A; Firmware Version: HPE Comware 7.1.045 Release R0305P08

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
2955	07/11/2017	HPE FlexNetwork 7500 and HPE FlexFabric 7900 and 12904 Switch Series	Hewlett Packard Enterprise	Hardware Version: HPE FlexNetwork 7502 Switch Chassis (JD242C) with (JH208A) [1], HPE FlexNetwork 7503 Switch Chassis (JD240C) with (JH207A) [1], HPE FlexNetwork 7503 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle (JH331A) with (JH209A) [1], HPE FlexNetwork 7506 Switch Chassis (JD239C) with (JH207A) [1], HPE FlexNetwork 7506 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle (JH332A) with (JH209A) [1], HPE FlexNetwork 7510 Switch Chassis (JD238C) with (JH207A) [1], HPE FlexNetwork 7510 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle (JH333A) with (JH209A) [1], HPE FlexFabric 7904 Switch Chassis (JG682A) with (JG683B) [2], HPE FlexFabric 7910 Switch Chassis (JG841A) with (JH001A or JG842A) and (JG683B) [2], HPE FlexFabric 12904E Switch AC Chassis (JH262A) with (JH263A) [3];; Firmware Version: HPE Comware 7.1.045, Release R7179 [1], HPE Comware 7.1.045, Release R2150 [2], HPE Comware 7.1.045, Release R1150 [3]
2956	07/11/2017	Windows Embedded Compact Cryptographic Primitives Library (bcrypt.dll)	Microsoft Corporation	Software Version: 7.00.2872 [1] and 8.00.6246 [2]
2957	07/12/2017	Microsoft Corporation Windows Embedded Compact Enhanced Cryptographic Provider 7.00.2872 and Microsoft Corporation Windows Embedded Compact Enhanced Cryptographic Provider 8.00.6246	Microsoft Corporation	Software Version: 7.00.2872 [1] and 8.00.6246 [2]
2958	07/13/2017	Lenel OnGuard Access Control Cryptographic Module	UTC Fire & Security Americas Corporation, Inc.	Software Version: 7.3.345.54
2959	07/17/2017	Trusted Platform Module 2.0 SLB 9660/SLB 9665/SLB 9670	Infineon Technologies AG	Hardware Version: P/Ns SLB 9660 (Package PG-TSSOP-28-2 or PG-VQFN-32-13) [1], SLB 9665 (Package PG-TSSOP-28-2 or PG-VQFN-32-13) [1] and SLB 9670 (Package PG-VQFN-32-13) [2]; Firmware Version: 5.80 [1] or 7.80 [2]
2960	07/17/2017	Cisco Firepower Cryptographic Module	Cisco Systems, Inc.	Firmware Version: 6.1
2961	07/18/2017	128 Technology Cryptographic Module	128 Technology	Software Version: 2.1
2962	07/18/2017	Ubuntu Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 1.0
2963	07/18/2017	HGST Ultrastar® He¹² TCG Enterprise HDD	HGST, a Western Digital company	Hardware Version: P/Ns HUH721212AL5205 (0001) and HUH721212AL4205 (0001); Firmware Version: R39C

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
2964	07/19/2017	BoringCrypto	Google, Inc.	Software Version: 24e5886c0edfc409c8083d10f9f1120111efd6f5
2965	07/19/2017	IMS3-SM	Dolby Laboratories, Inc.	Hardware Version: IMS3-41 [A], IMS3-42 [A] and IMS3-43 [A]; Firmware Version: (1.2.9-0, 1.2.9-3 and 1.2.4-0) [A]
2966	07/20/2017	Allegro Cryptographic Engine	Allegro Software Development Corporation	Software Version: 6.2
2968	07/25/2017	Huawei AR2240, AR3260 and AR169FGVW-L Series Routers	Huawei Technologies Co., Ltd.	Hardware Version: AR2240 P/N 03022UFU Version C.2, AR3260 P/N 03022NPN Version I.3 and AR169FGVW-L P/N 50010168 Version L.2; Tamper Evident Seals P/N 4057-113016 and External Baffle P/N 99089JEB; Firmware Version: V200R008C10SPC120
2969	07/25/2017	McAfee OpenSSL FIPS Object Module	McAfee LLC	Software Version: 1.0.1
2970	07/26/2017	Prime PIV v2.1 Applet on TOP DL V2.1 platform	Gemalto	Hardware Version: NXP P60D144P VA (MPH149); Firmware Version: TOPDLV2.1 (Filter04), PIV Applet version 2.1
2971	07/27/2017	Huawei S5720-EI Series Switches	Huawei Technologies Co., Ltd.	Hardware Version: S5720-36C-EI-28S-AC P/N 02359503 Version M.2, S5720-36C-EI-AC P/N 02359562 Version M.2, S5720-56C-EI-AC P/N 02359504 Version K.2, S5720-36C-PWR-EI-AC P/N 02359573 Version L.3 and S5720-56C-PWR-EI-AC P/N 02359576 Version L.2 all with Tamper Seals P/N 4057-113016 and External Baffle P/N 99089JEB; Firmware Version: V200R010C00SPC900B900
2972	07/27/2017	Huawei S5720-SI & S5720-LI Series Switches	Huawei Technologies Co., Ltd.	Hardware Version: S5720-12TP-LI-AC P/N 98010567 Version E.3 with [1 and 2], S5720-12TP-PWR-LI-AC P/N 98010570 Version D.2 with [1 and 2], S5720-28X-LI-24S-AC P/N 98010629 Version D.2 with [1 and 2], S5720-28X-LI-AC P/N 98010581 Version C.2 with [1 and 2], S5720-28X-PWR-LI-AC P/N 98010593 Version C.2 with [1 and 2], S5720-28X-PWR-SI-AC P/N 02350DLW Version E.3 with [1 and 2], S5720-28X-SI-24S-AC P/N 98010625 Version C.22 with [1 and 2], S5720-28X-SI-AC P/N 02350DLT Version E.3 with [1 and 2], S5720-52P-LI-AC P/N 98010600 Version C.2 with [1 and 2], S5720-52P-PWR-LI-AC P/N 98010612 Version C.2 with [1], S5720-52P-SI-AC P/N 02350DLU Version E.3 with [1 and 2], S5720-52X-LI-AC P/N 98010606 Version D.2 with [1 and 2], S5720-52X-PWR-LI-AC P/N 98010619 Version C.2 with [1], S5720-52X-PWR-SI-AC P/N 02350DLX Version E.3 with [1 and 2], S5720-52X-SI-AC P/N 02350DLV Version E.3 with [1 and 2]; Tamper Seals P/N 4057-113016 [1] and External Baffle P/N 99089JEB [2]; Firmware Version: V200R010C00SPC900B900
2973	07/27/2017	MicroCloud X4	Bluechip Systems LLC	Hardware Version: P/Ns MCX4-004, MCX4-008; Firmware Version: X4 Linux 3.4.110.1, MicroCloud Manager 1.9
2974	07/27/2017	Samsung Kernel Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 1.6.1 [1] and 1.8 [2]

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
2975	07/28/2017	HGST Ultrastar® SS300 TCG Enterprise SSD	Western Digital Technologies, Inc. HGST, a Western Digital brand	Hardware Version: P/Ns HUSMM3216ASS205 (001) [1, 2, 3, 4, 5], HUSMM3232ASS205 (001) [1, 2, 3, 4, 5], HUSMM3240ASS205 (001) [1, 2, 3, 4, 5], HUSMM3280ASS205 (001) [1, 2, 3, 4, 5], HUSMR3216ASS205 (001) [1, 2, 3, 4, 5], HUSMR3232ASS205 (001) [1, 2, 3, 4, 5], HUSMR3240ASS205 (001) [1, 2, 3, 4, 5] and HUSMR3280ASS205 (001) [1, 2, 3, 4, 5]; Firmware Version: R098 [1], R100 [2], R110 [3], R116 [4] or R118 [5]
2976	07/31/2017	d'Cryptor® SC	D'Crypt Private Limited	Hardware Version: P/N: DC-SPC-1, HW Version: 1.0; Firmware Version: 1.2
2977	07/31/2017	Huawei S7700 Series Switches	Huawei Technologies Co., Ltd.	Hardware Version: S7703 P/N 02113959 Version P.3 with [1, 2 and 7], S7706 P/N 02113960 Version N.2 with [1, 3, 5 and 7] and S7712 P/N 02113961 Version P.2 with [1, 4, 6 and 7]; LPU P/N 03030MQP [1], MPU P/N 03030MPV [2], MPU P/N 03030MQS [3], MPU P/N 03031FSL [4], CSS P/N 03030QHL [5], CSS P/N 03030XYD [6] and Tamper Seals P/N 4057-113016 [7]; Firmware Version: V200R010C00SPC900B900
2978	07/31/2017	Ubuntu Strongswan Cryptographic Module	Canonical Ltd.	Software Version: 1.0