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

May 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: 6/6/2019

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: June 4, 2019

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
3449	05/02/2019	SAP CommonCryptoLib Crypto Kernel	SAP SE	Software Version: 8.4.47.0 32-bit [1] and 64-bit [2]
3450	05/02/2019	F5(R) Device Cryptographic Module	F5 Networks	Hardware Version: BIG-IP i4000, BIG-IP i5000, BIG-IP i5820-DF, BIG-IP i7000, BIG-IP i7820-DF, BIG-IP i10800, BIG-IP i11800-DS, BIG-IP i15800, BIG-IP 4000, BIG-IP 5250v-F, BIG-IP 7000, BIG-IP 7200v-F, BIG-IP 10200v-F, BIG-IP 10350v-F, VIPRION B2250, VIPRION B4450; Firmware Version: 13.1.1 EHF
3451	05/06/2019	BitLocker(R) Windows OS Loader (winload) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Mobile, Windows 10 for Surface Hub	Microsoft Corporation	Software Version: 10.0.10586.1176
3452	05/07/2019	Radiant Logic Cryptographic Module for Java	Radiant Logic Inc.	Software Version: 2.1
3453	05/07/2019	Unbound Tech EKM Cryptographic Module	Unbound Tech	Software Version: 2.0
3454	05/07/2019	Juniper CryptoCore Cryptographic Module	Juniper Networks, Inc.	Software Version: 1.0
3455	05/07/2019	Extreme VDX 6740, VDX 6740T, VDX 6940 and VDX 8770 Switches	Extreme Networks, Inc.	Hardware Version: P/Ns: 80-1007483-05, 80-1007486-01, 80-1007864-03, 80-1008009-02, 80-1008531-01, 80-1005850-01 and 80-1006294-03; Firmware Version: 7.3.0aa
3456	05/09/2019	PTP 700 Point to Point Wireless Ethernet Bridge	Cambium Networks, Ltd.	Hardware Version: P/Ns C045070B003A, C045070B003B, C045070B009A, C045070B009B, C045070B034A, C045070B039A, C045070B004A, C045070B010A, C045070B038A, C045070B040A, C045070B002A, C045070B008A, C045070B006A, C045070B012A, C045070B026A and C045070B028A; Firmware Version: 700-02-65-FIPS
3457	05/09/2019	NETSCOUT FIPS Object Module	NETSCOUT Systems, Inc.	Software Version: 1.0
3458	05/10/2019	Cisco Aironet 1562 e/i/d/ps, 2802 e/i and 3802 e/i/p Wireless LAN Access Points	Cisco Systems, Inc.	Hardware Version: 1562e, 1562i, 1562d, 1562ps, 2802e, 2802i, 3802e, 3802i, 3802p with FIPS Kit: AIRLAP-FIPSKIT=, VERSION B0; Firmware Version: 8.5
3459	05/21/2019	Ezio PKI Card	Thales	Hardware Version: NXP P60D144P VA (MPH149); Firmware Version: TOPDLV2.1 (Filter04), IDPrime MD Applet version V4.3.6.A and MSPNP Applet V1.2
3460	05/21/2019	Nutanix Cryptographic Module for OpenSSL	Nutanix, Inc.	Software Version: 5.0

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3461	05/28/2019	Ruckus Wireless, Inc. SmartZone 104 (SZ-104), SmartZone 124 (SZ-124) and SmartZone 300 (SZ-300) WLAN Controllers	Ruckus Wireless, Inc.	Hardware Version: SZ-104, SZ-124 and SZ-300; Firmware Version: 3.6.0.3
3462	05/28/2019	NPCT7xx TPM 2.0 rev 1.38	Nuvoton Technology Corporation	Hardware Version: LAG019 in TSSOP28 Package, LAG019 in QFN32 Package, and LAG019 in UQFN16 Package; Firmware Version: 7.2.1.0
3464	05/28/2019	BitLocker(R) Windows Resume (winresume) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise	Microsoft Corporation	Software Version: 10.0.10586.1176
3465	05/29/2019	HiCOS PKI Applet v2.0 on IDEMIA ID-One Cosmo v8.1-R2	Chunghwa Telecom Co., Ltd.	Hardware Version: P/N '30'; Firmware Version: '5F02'-'090191' and HiCOS PKI Applet V2.0 '03020206'