# 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 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 A Cooper

Dated: 12/14/2017

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 12/13/2017

Director, Architecture and Technology Assurance
Communications Security Establishment

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

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 |
|---|---|---|---|---|
| 3056 | 11/02/2017 | TRANSEC Module | VT iDirect, Inc. | Hardware Version: E0002268; Firmware Version: Cloak 1.0.2.0 |
| 3057 | 11/07/2017 | IBM(R) z/OS(R) Version 2 Release 2 System SSL Cryptographic Module | IBM Corporation | Software Version: HCPT420/JCPT421 with APAR OA52653; Hardware Version: COP chips integrated within processor unit; Firmware Version: Feature 3863 (aka FC3863) with System Driver Level 27I |
| 3058 | 11/07/2017 | Huawei USG 9520/9560/9580 Firewall | Huawei Technologies Co., Ltd. | Hardware Version: Base Models: USG9520 (P/N 02350FRU Rev D.2) [1], USG9560 (P/N 02350FRW Rev D.2) [2] and USG9580 (P/N 02350FRX Rev D.2) [3]; SPU/SPC cards: SPU-X3-B (P/N 03056640) [1, 2, 3], SPU-X3-B2 (P/N 03056989) [1, 2, 3], SPU-X8X16-B (P/N 03056638) [1, 2, 3], SPC-20-O-E8KE (P/N 03056636) [1, 2, 3], SPU-X3-20-O-E8KE (P/N 03056634) [1, 2, 3], SPU-X8X16-20-O-E8KE (P/N 03056635) [1, 2, 3], SPC-APPSEC-FW (P/N 03056688) [1, 2, 3], SPUA-20-O-H (P/N 03057426) [1, 2, 3], SPUA-20-O-M (P/N 03057427) [1, 2, 3], SPCA-20-O-H&M (P/N 03057429) [1, 2, 3], SPUB-20-O-H (P/N 03057520) [1, 2, 3], SPUB-20-O-M (P/N 03057518) [1, 2, 3], SPCB-20-O-H&M (P/N 03057522) [1, 2, 3]; External Baffle: 99089JEB, Version A.2 [1, 3]; Tamper Seal 4057-113016, Version A.3 [1, 2, 3]; Firmware Version: V500R001C50 |
| 3059 | 11/09/2017 | Atalla Cryptographic Subsystem (ACS) | Micro Focus | Hardware Version: C9B60-2101A; Firmware Version: Loader Version 1.20, PSMCU Versions 0.95 or 0.96, CMS-OCT Version 0.95, CMS-NTX Version 0.95 |
| 3060 | 11/09/2017 | CommVault Crypto Library | CommVault Systems, Inc. | Software Version: 2.0 |
| 3061 | 11/10/2017 | HGST Ultrastar SS200 TCG Enterprise SSD | HGST, a Western Digital brand | Hardware Version: P/Ns SDLL1HLR-076T Version 1, SDLL1MLR-038T Version 1, SDLL1CLR-020T Version 1 and SDLL1DLR-920G Version 1; Firmware Version: XC00 |
| 3062 | 11/14/2017 | MVC201 | MikroM GmbH | Hardware Version: MVC201-IS1 rev.1.1, MVC201-IF1 rev.1.1, MVC201-MS1 rev.1.1, MVC201-MF1 rev.1.1, MVC201-RS1 rev.1.1 and MVC201-RS2 rev.1.1; Firmware Version: 1.23.157.20779; Bootloader Version 1.3.7.18217 |
| 3063 | 11/14/2017 | Red Hat Enterprise Linux OpenSSH Server Cryptographic Module | Red Hat(R), Inc. | Software Version: 5.0 |
| 3064 | 11/14/2017 | IBM(R) Crypto for C | IBM(R) Corporation | Software Version: 8.6.0.0 |
| 3065 | 11/15/2017 | Trusted Platform Module ST33TPHF20SPI & ST33TPHF20I2C | STMicroelectronics | Hardware Version: ST33HTPH2E28AAF0 [1,3], ST33HTPH2E32AAF0 [1,3], ST33HTPH2E28AAF1 [1,3], ST33HTPH2E32AAF1 [1,3], ST33HTPH2028AAF3 [2,4], ST33HTPH2032AAF3 [2,4], ST33HTPH2E28AHB3 [3], ST33HTPH2E32AHB3 [3], ST33HTPH2E28AHB4 [3], ST33HTPH2E32AHB4 [3], ST33HTPH2E28AHB7 [5], ST33HTPH2E32AHB7 [5], ST33HTPH2E28AHB8 [5], ST33HTPH2E32AHB8 [5], ST33HTPH2028AHB9 [6] and ST33HTPH2032AHB9 [6]; Firmware Version: 49.00 [1], 4A.00 [2], 49.04 [3], 4A.04 [4], 49.05 [5] and 4A.05 [6] |

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 |
|---|---|---|---|---|
| 3066 | 11/15/2017 | Trusted Platform Module ST33TPHF2ESPI & ST33TPHF2EI2C | STMicroelectronics | Hardware Version: ST33HTPH2E28AAF0 [1,2], ST33HTPH2E32AAF0 [1,2], ST33HTPH2E28AAF1 [1,2], ST33HTPH2E32AAF1 [1,2], ST33HTPH2E28AHB3 [2], ST33HTPH2E32AHB3 [2], ST33HTPH2E28AHB4 [2], ST33HTPH2E32AHB4 [2], ST33HTPH2E28AHB7 [3], ST33HTPH2E32AHB7 [3], ST33HTPH2E28AHB8 [3] and ST33HTPH2E32AHB8 [3]; Firmware Version: 49.00 [1], 49.04 [2] and 49.05 [3] |
| 3067 | 11/27/2017 | Red Hat Enterprise Linux OpenSSH Client Cryptographic Module | Red Hat(R), Inc. | Software Version: 5.0 |
| 3068 | 11/27/2017 | NetBrain OpenSSL Cryptographic Module | NetBrain Technologies, Inc. | Software Version: 1.0 |
| 3069 | 11/27/2017 | Aruba IAP-214, IAP-215, IAP-224, IAP-225, IAP-274, IAP-275, IAP-277, RAP-108 and RAP-109 Wireless Access Points with Aruba Instant Firmware | Aruba, a Hewlett Packard Enterprise company | Firmware Version: ArubaInstant 6.5.1.0-4.3.1 |