# 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

**June 2023**

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: TIMOTHY HALL

Digitally signed by TIMOTHY HALL
Date: 2023.07.07 13:21:24 -04'00'

Dated:

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: King, Lyall

Digitally signed by King, Lyall
DN: C=CA, O=GC, OU=CSE-CST, CN="King, Lyall"
Reason: I am approving this document
Location:
Date: 2023.07.07 07:42:52-04'00'
Foxit PDF Editor Version: 12.1.2

Dated:

Director, Risk Mitigation Programs
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 |
|---|---|---|---|---|
| 4528 | 06/05/2023 | Apricorn FIPS 140-2 Encryption System Gen 2 | Apricorn | Hardware Version: P/Ns AFESG2-1 Rev A2, AFESG2-2 Rev A2 and AFESG2-3 Rev A2; Firmware Version: 2.2 |
| 4529 | 06/05/2023 | Aegis Fortress L3 Cryptographic Module | Apricorn | Hardware Version: P/Ns AFL3-500, AFL3-1TB, AFL3-2TB, AFL3-3TB, AFL3-4TB, AFL3-5TB, AFL3-S500, AFL3-S1TB, AFL3-S2TB, AFL3-S4TB, AFL3-S8TB, AFL3-S16TB and AFL3-S20TB; Hardware Version: Rev B1; Firmware Version: 3.3 |
| 4530 | 06/05/2023 | IBM(R) z/VM(R) Version 7 Release 2 System SSL Cryptographic Module | IBM Corporation | Software Version: 5735FAL00: z/VM Version 7 Release 2 with 7201RSU (GA-level release) and the PTF for APAR PH24751; Hardware Version: z14 CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 |
| 4531 | 06/09/2023 | Infoblox Trinzic HW Appliances | Infoblox | Hardware Version: Trinzic 805 (TE-815, TE-825, TR-805, ND-805), Trinzic 1405 (TE-1415, TE-1425, TR-1405, ND-1405), Trinzic 2205 (TE-2215, TE-2225, TR-2205, ND-2205), Trinzic 4005 (TE-4015, TE-4025, TR-4005, ND-4005) with Label Kit IB-FIPS; Firmware Version: NIOS 8.5.2 with Hotfix-NIOS_8.5.2_409296_J81082-506fbabaabd86fbe9c99de0b49c9a7f8-Mon-Oct-25-08-19-32-2021 |
| 4532 | 06/12/2023 | Acme Packet 1100, Acme Packet 3900, Acme Packet 3950 and Acme Packet 4900 | Oracle Communications | Hardware Version: 1100, 3900, 3950 and 4900; Firmware Version: S-Cz9.0 |
| 4533 | 06/12/2023 | FortiGate-1101E/2000E/2201E/2500E/3301E | Fortinet, Inc. | Hardware Version: FortiGate-1101E (C1AJ13), FortiGate-2201E (C1AH54), FortiGate-3301E (C1AJ38), FortiGate-2000E (C1AF49) and FortiGate-2500E (C1AF51) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.2 build 5203 |
| 4534 | 06/13/2023 | Kasten BoringCrypto | Kasten, Inc. | Software Version: 853ca1ea1168dff08011e5d42d94609cc0ca2e27 |
| 4535 | 06/15/2023 | Infoblox Trinzic Virtual Appliances | Infoblox | Software Version: NIOS 8.5.2 with Hotfix-NIOS_8.5.2_409296_J81082-506fbabaabd86fbe9c99de0b49c9a7f8-Mon-Oct-25-08-19-32-2021 |
| 4536 | 06/15/2023 | Cryptographic Primitives Library | Microsoft Corporation | Software Version: 10.0.18362[1], 10.0.18363[2] and 10.0.19041[3] |
| 4537 | 06/20/2023 | Virtual TPM | Microsoft Corporation | Software Version: 10.0.18362[1], 10.0.18363[2] and 10.0.19041[3] |
| 4538 | 06/20/2023 | BitLocker Dump Filter | Microsoft Corporation | Software Version: 10.0.18362[1], 10.0.18363[2] and 10.0.19041[3] |
| 4539 | 06/22/2023 | FastIron ICX™ 7850 Series Switch/Router | CommScope Technologies LLC | Hardware Version: P/Ns ICX 7850-32Q / 84-1003423-01, Version 0300; ICX7850-48F / 84-1003425-01, Version 0300; ICX7850-48FS / 84-1003424-01, Version 0200; Firmware Version: IronWare R08.0.95g |
| 4540 | 06/22/2023 | Ubuntu 18.04 OpenSSL Cryptographic Module | Canonical Ltd. | Software Version: 2.0 |
| 4541 | 06/22/2023 | Silver Peak ECOS Cryptographic Library | Silver Peak Systems Inc. | Software Version: Crypto Library 2020 Version 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 |
|---|---|---|---|---|
| 4543 | 06/29/2023 | Aruba IAP-315, IAP-345, IAP-377, IAP-503H, IAP-505H, IAP-504, IAP-505, IAP-514, IAP-515, IAP-534, IAP-535, and IAP-555 Wireless Access Points | Aruba, a Hewlett Packard Enterprise company | Hardware Version: [IAP-315-US TAA (HPE SKU JW814A), IAP-345-USF1 (HPE SKU JZ034A), IAP-345-RWF1 (HPE SKU JZ032A), IAP-377-USF1 (HPE SKU JZ188A), IAP-377-RWF1 (HPE SKU JZ187A), IAP-503H-US TAA (HPE SKU R3V39A), IAP-505H-US TAA (HPE SKU R3V49A), IAP-504-US TAA (HPE SKU R2H34A), IAP-505-US TAA (HPE SKU R2H39A), IAP-514-US TAA (HPE SKU Q9H68A), IAP-515-US TAA (HPE SKU Q9H73A), IAP-534-US TAA (HPE SKU JZ342A), IAP-535-US TAA (HPE SKU JZ347A), IAP-555-US TAA (HPE SKU JZ367A)]; Firmware Version: Aruba Instant 8.8 |
| 4544 | 06/29/2023 | eToken 5300 Mini and Micro MD 4.3.5 | Thales | Hardware Version: 214-010381-001, [1] [2], 214-010382-001, [1] [2]: STM32F042K6U6TR [1] and SLE78CFX3000PH [2]; Firmware Version: 5300 FIPS FW ver-14.0.15 [1] and {IDCore30-revB - Build 06, IDPrime MD Applet version V4.3.5.D and MSPNP Applet V1.2} [2] |
| 4545 | 06/30/2023 | Windows OS Loader | Microsoft Corporation | Software Version: 10.0.17763.10021 and 10.0.17763.10127; Hardware Version: Intel Xeon Silver 4114, Intel Xeon Gold 6230, Intel Xeon Platinum 8260 and Intel Xeon D-1559 |
| 4546 | 06/30/2023 | Boot Manager | Microsoft Corporation | Software Version: 10.0.22000; Hardware Version: Intel i5-1145G7 |