

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

August 2022

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: _____

Dated: _____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: _____

Director, Risk Mitigation Programs
Canadian Centre for Cyber Security

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4275	08/08/2022	LogRhythm 7.8.0 Data Processor	LogRhythm	Software Version: 7.8.0
4276	08/08/2022	Ascom Smartphone BoringCrypto	Ascom Sweden AB	Software Version: 7f02881e96e51f1873afcf384d02f782b48967ca
4277	08/15/2022	CBL-Mariner 1.0 Kernel Crypto API	Microsoft Corporation	Software Version: 1.0
4278	08/15/2022	Cisco Catalyst 9115AXI/AXE, 9120AXI/AXE/AXP, 9130AXI/AXE and 9105AXI/AXW Wireless LAN Access Points	Cisco Systems, Inc.	Hardware Version: 9115AXI, 9115AXE, 9120AXI, 9120AXE, 9120AXP, 9130AXI, 9130AXE, 9105AXI and 9105AXW with FIPS Kit: AIR-AP-FIPSKIT=; Firmware Version: AireOS 8.10MR3 and IOS-XE 17.3
4279	08/17/2022	Infraguard Processor Module	Advantor Systems, A Vectrus Company	Hardware Version: [5.16 with components NAND MX30LF1G08AA-TI and SDRAM MT48H16M32LFB5-6 IT:C], [5.16 with components NAND S34ML01G100TFI000 and SDRAM MT48H16M32LFB5-6 IT:C], [5.16 with components NAND MT29F2G08ABAEAWP-AITX:E and SDRAM MT48H16M32LFB5-6 IT:C], [5.16 with components NAND K9F1G08U0D-SIB0 and SDRAM MT48H16M32LFB5-6 IT:C], [5.16 with components NAND MX30LF1G08AA-TI and SDRAM MT48H16M32LFB5-6 AAT:C], [5.16 with components NAND S34ML01G100TFI000 and SDRAM MT48H16M32LFB5-6 AAT:C], [5.16 with components NAND MT29F2G08ABAEAWP-AITX:E and SDRAM MT48H16M32LFB5-6 AAT:C] and [5.16 with components NAND K9F1G08U0D-SIB0 and SDRAM MT48H16M32LFB5-6 AAT:C]; Firmware Version: 2.3.0
4281	08/23/2022	Secure Drive + KP	Glyph Production Technologies	Hardware Version: SDPL1000KP; SDPL2000KP; SDPL4000KP; SDPL5000KP; SDPLSSD1000KP; SDPLSSD2000KP; SDPLSSD4000KP; SDPLSSD8000KP; Firmware Version: CLEVX_SATA-KP_v2.2, CLEVX_3637E_USB_V0313 or CLEVX_3637E_USB_V0314
4282	08/23/2022	OpenSSL FIPS Provider	The OpenSSL Project	Software Version: 3.0.0
4283	08/24/2022	Summit Linux FIPS Core Crypto Module	Laird Connectivity	Software Version: 7.1; Hardware Version: ATSAMA5D31 and ATSAMA5D36
4284	08/28/2022	Qumulo Secure	Qumulo, Inc.	Software Version: 1.0
4285	08/29/2022	Secure Drive + BT	Glyph Production Technologies	Hardware Version: SDPL1000BT; SDPL2000BT; SDPL4000BT; SDPL5000BT; SDPLSSD1000BT; SDPLSSD2000BT; SDPLSSD4000BT; SDPLSSD8000BT; Firmware Version: CLEVX_SATA-BT_v2.3 and (CLEVX_3637E_USB_V0313 or CLEVX_3637E_USB_V0314)
4286	08/30/2022	VMware's VPN Crypto Module	VMware, Inc.	Software Version: 2.0
4287	08/30/2022	NextFlex AirGuardian	NextFlex	Hardware Version: A25 Rev. A; Firmware Version: 1.4
4288	08/31/2022	LogRhythm 7.8.0 Console	LogRhythm	Software Version: 7.8.0
4289	08/31/2022	LogRhythm 7.8.0 Platform Manager	LogRhythm	Software Version: 7.8.0
4290	08/31/2022	LogRhythm 7.8.0 System Monitor Agent	LogRhythm	Software Version: 7.8.0

