FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of
the United States of America

October 2021

The Canadian Centre for Cyber Security

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: _____November 12 2021_____

Director, Risk Mitigation Programs
Canadian Centre for Cyber Security

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4040	10/05/2021	Avaya BoringCrypto Android	Avaya, Inc.	Software Version: 1.0
4041	10/06/2021	Samsung SAS 12G TCG Enterprise SSC SEDs PM1643a Series	Samsung Electronics Co., Ltd.	Hardware Version: MZILT920HBHQ-000H9, MZILT920HBHQ-00AH9, MZILT1T9HBJR-000H9, MZILT1T9HBJR-00AH9, MZILT3T8HBLS-000H9, MZILT3T8HBLS-00AH9, MZILT7T6HALA-000H9, MZILT7T6HALA-00AH9, MZILT15THALA-000H9 and MZILT15THALA-00AH9; Firmware Version: 3P00
4042	10/06/2021	Motorola BoringCrypto Android	Motorola Mobility LLC	Software Version: 7f02881e96e51f1873afcf384d02f782b48967ca
4043	10/16/2021	Citrix ADC MPX	Citrix Systems, Inc.	Hardware Version: 8905 FIPS, 8910 FIPS, 8920 FIPS, 15020-50G FIPS, 15030-50G FIPS, 15040-50G FIPS, 15060-50G FIPS, 15080-50G FIPS, 15100-50G FIPS, 15120-50G FIPS; Firmware Version: 12.1.55.180
4044	10/18/2021	NV-2108 Flashtec(TM) PCIe NVRAM Drive	Microchip Technology, Inc.	Hardware Version: NV-2108; Firmware Version: 3.2.13.0
4045	10/18/2021	MS1201 Security Sub-system	eWBM	Hardware Version: 2.2.0; Firmware Version: 2.5.3
4046	10/18/2021	Ubuntu 20.04 Strongswan Cryptographic Module	Canonical Ltd.	Software Version: 3.0
4047	10/20/2021	Vocera Cryptographic Module v3.1	Vocera Communications, Inc.	Software Version: 3.1; Hardware Version: 88W8787; Firmware Version: 3.0
4048	10/21/2021	Crestron Mobile Crypto Module	Crestron Electronics, Inc.	Software Version: 1.0
4049	10/25/2021	Ubuntu 18.04 IBM-GT Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 2.0
4050	10/26/2021	BotSink 3200 and 5100	Attivo Networks Inc.	Hardware Version: 3200 and 5100; Firmware Version: 3.3
4051	10/26/2021	ACM 200	Attivo Networks Inc.	Hardware Version: 200; Firmware Version: 3.3
4053	10/27/2021	Ruckus Networks Virtual SmartZone (vSZ)	CommScope Technologies LLC	Software Version: 5.2.1.3
4055	10/27/2021	SUSE Linux Enterprise Server Libica Cryptographic Module	SUSE, LLC	Software Version: 1.0; Hardware Version: IBM z15; Firmware Version: Feature Code 3863 (FC3863)
4056	10/28/2021	FireEye EX Series: EX3500, EX5500, EX8400, EX8500	FireEye, Inc.	Hardware Version: EX3500, EX5500, EX8400, EX8500; Firmware Version: 9.0.3
4057	10/28/2021	FireEye CM Series: CM4500, CM7500, CM9400, CM9500	FireEye, Inc.	Hardware Version: CM4500, CM7500, CM9400, CM9500; Firmware Version: 9.0.3
4058	10/28/2021	FireEye EX Series: EX5500V	FireEye, Inc.	Software Version: 9.0.3
4059	10/28/2021	FireEye HX Series: HX4502V	FireEye, Inc.	Software Version: 5.0.4
4060	10/28/2021	FireEye NX Series: NX1500, NX2500, NX2550, NX3500, NX4500, NX5500, NX6500	FireEye, Inc.	Hardware Version: NX1500, NX2500, NX2550, NX3500, NX4500, NX5500, NX6500; Firmware Version: 9.0.3
4061	10/28/2021	FireEye VX Series: VX5500, VX12500, VX12550	FireEye, Inc.	Hardware Version: VX5500, VX12500, VX12550; Firmware Version: 9.0.3

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4062	10/28/2021	FireEye CM Series: CM1500V, CM2500V, CM7500V	FireEye, Inc.	Software Version: 9.0.3
4063	10/28/2021	FireEye VX Series: VX7690Vfips	FireEye, Inc.	Software Version: 9.0.3