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

July 2020

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 COOPER Digitally signed by MICHAEL COOPER Date: 2020.08.05 11:34:07 -04'00'

Dated: ______________________

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: ______________________

Dated: August 5 2020

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3675	07/02/2020	X-Wall MX+	Enova Technology Corporation	Hardware Version: xF; Firmware Version: mr.20.06.02.2203.CIF
3676	07/02/2020	X-Wall MX+	Enova Technology Corporation	Hardware Version: xN; Firmware Version: mr.20.06.02.2203.CIF
3677	07/07/2020	Juniper Networks vSRX 3.0 Virtual Firewall	Juniper Networks, Inc.	Software Version: Junos OS 19.2R1
3678	07/13/2020	BoringCrypto	Google, LLC	Software Version: ae223d6138807a13006342edfeef32e813246b39
3679	07/13/2020	Ruckus Networks SmartZone 104 (SZ-104), SmartZone 124 (SZ-124) and SmartZone 300 (SZ-300) WLAN Controllers	Ruckus Wireless, Inc.	Hardware Version: PF1-S104-US00, RevA; PF1-S124-US00, RevA; PF1-S300-WW00, RevA; PF1-S300-WW10, RevA; Firmware Version: 5.1.1.3
3680	07/14/2020	Trusted Platform Module ST33TPHF2ESPI & ST33TPHF2EI2C	STMicroelectronics	Hardware Version: ST33HTPH2E28AAF0 [1], ST33HTPH2E32AAF0 [1], ST33HTPH2E28AAF1 [1], ST33HTPH2E32AAF1 [1], ST33HTPH2E28AHB3 [1], ST33HTPH2E32AHB3 [1], ST33HTPH2E28AHB4 [1], ST33HTPH2E32AHB4 [1], ST33HTPH2E28AHB7 [2], ST33HTPH2E32AHB7 [2], ST33HTPH2E28AHB8 [2], ST33HTPH2E32AHB8 [2], ST33HTPH2E28AHC0 [1], ST33HTPH2E32AHC0 [1], ST33HTPH2E28AHC2 [2], ST33HTPH2E32AHC2 [2], ST33HTPH2E28AHD0 [1] and ST33HTPH2E32AHD0 [1]; Firmware Version: 49.40 [1] and 49.41 [2]
3681	07/14/2020	Trusted Platform Module ST33TPHF2ESPI & ST33TPHF2EI2C	STMicroelectronics	Hardware Version: ST33HTPH2E28AAF0 [1], ST33HTPH2E32AAF0 [1], ST33HTPH2E28AAF1 [1], ST33HTPH2E32AAF1 [1], ST33HTPH2E28AHB3 [1], ST33HTPH2E32AHB3 [1], ST33HTPH2E28AHB4 [1], ST33HTPH2E32AHB4 [1], ST33HTPH2E28AHB7 [2], ST33HTPH2E32AHB7 [2], ST33HTPH2E28AHB8 [2], ST33HTPH2E32AHB8 [2], ST33HTPH2E28AHD6 [1] and ST33HTPH2E32AHD6 [1]; Firmware Version: 49.14 [1] and 49.15 [2]
3682	07/15/2020	Trusted Platform Module ST33TPHF20SPI & ST33TPHF20I2C	STMicroelectronics	Hardware Version: ST33HTPH2E28AAF0 [1], ST33HTPH2E32AAF0 [1], ST33HTPH2E28AAF1 [1], ST33HTPH2E32AAF1 [1], ST33HTPH2028AAF3 [3], ST33HTPH2032AAF3 [3], ST33HTPH2E28AHB3 [1], ST33HTPH2E32AHB3 [1], ST33HTPH2E28AHB4 [1], ST33HTPH2E32AHB4 [1], ST33HTPH2E28AHB7 [2], ST33HTPH2E32AHB7 [2], ST33HTPH2E28AHB8 [2], ST33HTPH2E32AHB8 [2], ST33HTPH2028AHB9 [4], ST33HTPH2032AHB9 [4], ST33HTPH2E28AHC0 [1], ST33HTPH2E32AHC0 [1], ST33HTPH2028AHC1 [3 and 5], ST33HTPH2032AHC1 [3 and 5], ST33HTPH2E28AHC2 [2], ST33HTPH2E32AHC2 [2], ST33HTPH2028AHC3 [4], ST33HTPH2032AHC3 [4], ST33HTPH2028AHC9 [3 and 5], ST33HTPH2032AHC9 [3 and 5], ST33HTPH2E28AHD0 [1], ST33HTPH2E32AHD0 [1], ST33HTPH2028AHD1 [3] and ST33HTPH2032AHD1 [3]; Firmware Version: 49.40 [1], 49.41 [2], 4A.40 [3], 4A.41 [4] and 4A.10 [5]
3683	07/15/2020	Ubuntu 18.04 Azure Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 2.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3684	07/15/2020	Trusted Platform Module ST33TPHF20SPI & ST33TPHF20I2C	STMicroelectronics	Hardware Version: ST33HTPH2E28AAF0 [1], ST33HTPH2E32AAF0 [1], ST33HTPH2E28AAF1 [1], ST33HTPH2E32AAF1 [1], ST33HTPH2028AAF3 [2], ST33HTPH2032AAF3 [2], ST33HTPH2E28AHB3 [1], ST33HTPH2E32AHB3 [1], ST33HTPH2E28AHB4 [1], ST33HTPH2E32AHB4 [1], ST33HTPH2E28AHB7 [3], ST33HTPH2E32AHB7 [3], ST33HTPH2E28AHB8 [3], ST33HTPH2E32AHB8 [3], ST33HTPH2028AHB9 [4], ST33HTPH2032AHB9 [4], ST33HTPH2E28AHD6 [1], ST33HTPH2E32AHD6 [1], ST33HTPH2028AHD7 [2] and ST33HTPH2032AHD7 [2]; Firmware Version: 49.14 [1], 4A.14 [2], 49.15 [3] and 4A.15 [4]
3685	07/15/2020	MiniCrypt	Teledyne Webb Research	Firmware Version: 1.6
3686	07/20/2020	VMware's VPN Crypto Module	VMware, Inc.	Software Version: 1.0
3687	07/20/2020	CGI Momentum™ Java Cryptographic Module	CGI Federal Inc.	Software Version: 3.0.1
3688	07/21/2020	KIOXIA TCG Enterprise SSC Self-Encrypting Solid State Drive (PX04S model) Type C1	KIOXIA Corporation	Hardware Version: A0 with PX04SMQ080B, A0 with PX04SMQ160B; Firmware Version: AR04
3689	07/23/2020	QinetiQ BRACER™ Handset	QinetiQ Limited	Hardware Version: BM1800449, version 1.0; Firmware Version: 1.3.0/DB17011
3690	07/27/2020	Virtual TPM	Microsoft Corporation	Software Version: 10.0.17763
3691	07/28/2020	SXF1800	NXP Semiconductors Netherlands B.V.	Hardware Version: P/N SXF1800HN/V102B; Firmware Version: JCOP 4.4 R1.16.8; V2X applet V2.12.3; GS applet v2.12.1
3692	07/28/2020	Key# crypto	Raonsecure Co., Ltd.	Software Version: 1.3
3693	07/28/2020	FastIron ICX™ 7850 Series Switch/Router	Ruckus Wireless, Inc.	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 R08.0.90a
3694	07/31/2020	CGI Momentum™ C++ Cryptographic Module	CGI Federal Inc.	Software Version: 2.2