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

November 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: TIMOTHY HALL Digitally signed by TIMOTHY HALL Date: 2022.12.06 07:58:02 -05'00'

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: 2022.12.05 15:34:58-05'00' Foxit PDF Editor Version: 12.0.1

Dated:

Director, Risk Mitigation Programs
Canadian Centre for Cyber Security

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4351	11/01/2022	Aruba VIA Cryptographic Module	Aruba, a Hewlett Packard Enterprise Company	Software Version: 1.0
4352	11/02/2022	Core Crypto Engine	SZ DJI Technology Co., Ltd.	Hardware Version: 0xDF; Firmware Version: TEE 1.1.0, REE 1.1.0, TEE Secure Boot ROM 1.0.0
4353	11/03/2022	Kasten BoringCrypto	Kasten, Inc.	Software Version: ae223d6138807a13006342edfeef32e813246b39
4354	11/03/2022	Google Tensor UFS Inline Storage Encryption Cryptographic Module	Google, LLC.	Software Version: 1.0; Hardware Version: de8b6c8621
4355	11/07/2022	Cryptographic Module for Intel® Platforms' Security Engine Chipset	Intel Corporation	Hardware Version: 2.0; Firmware Version: 3.1
4356	11/07/2022	Type 3 Data Encryption Device (V3K-102)	Viasat, Inc.	Hardware Version: P/Ns 1090927, revisions 002, 003, 004, 005; 1163385, revisions 001 and 002; Firmware Version: 1.4.2
4357	11/07/2022	HyperOTP Token	Hypersecu Information Systems Inc.	Hardware Version: P449, V1.0; Firmware Version: V1.0 (build015010, build015210, build021010 or build021210)
4358	11/07/2022	Thunder Series TH3040S, TH5440S, TH5840S and TH7440S-11	A10 Networks, Inc.	Hardware Version: TH3040S, TH5440S, TH5840S and TH7440S-11; Firmware Version: 4.1.4-GR1-P5
4359	11/08/2022	Rubrik Cryptographic Library for Java	Rubrik Inc.	Software Version: 3.0.2.1
4360	11/08/2022	KMF/Wave/Traffic CryptR	Motorola Solutions, Inc.	Hardware Version: P/Ns CLN8566A, Rev. 0x1 and CLN1875A, Rev. 0x1; Firmware Version: R03.07.04 with or without AES128 R01.00.01, AES256 R01.00.03, and/or ADP/DES-CBC/DES-ECB/DES-OFB/DES-XL/DVI-XL/DVP-XL R01.00.00
4361	11/09/2022	FortiAnalyzer 6.2	Fortinet, Inc.	Firmware Version: FortiAnalyzer v6.2, build9599
4362	11/09/2022	FortiManager 6.2	Fortinet, Inc.	Firmware Version: FortiManager v6.2, build9599
4363	11/09/2022	SAAB Encrypted Automatic Identification System Cryptographic Module (EAISCM)	Saab AB (publ) TransponderTech (SAAB)	Firmware Version: 1.0
4364	11/14/2022	Nutanix Cryptographic Module for OpenSSH Client	Nutanix, Inc.	Software Version: 6.0
4365	11/14/2022	Nutanix Cryptographic Module for OpenSSH Server	Nutanix, Inc.	Software Version: 6.0
4366	11/14/2022	Ubuntu 20.04 Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 3.1
4367	11/15/2022	Titan-D Chip	Google, LLC.	Hardware Version: H1D3P; Firmware Version: dnafips-1.0
4368	11/16/2022	Trend Micro Java Crypto Module	Trend Micro Inc.	Software Version: 3.0.2.1
4369	11/16/2022	Zscaler Java Crypto Module	Zscaler Inc.	Software Version: 3.0.2.1

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4370	11/16/2022	Okta Cryptographic Module for Java	Okta, Inc.	Software Version: 3.0.2.1
4371	11/16/2022	Proofpoint Cryptographic Module for Java	Proofpoint Inc.	Software Version: 3.0.2.1
4372	11/16/2022	Forcepoint Java Crypto Module	Forcepoint	Software Version: 3.0.2.1
4373	11/16/2022	OneView Java Crypto Module	Hewlett Packard Enterprise	Software Version: 3.0.2.1
4374	11/16/2022	HID Global Cryptographic Module	HID Global Corporation	Software Version: 3.0.2.1
4375	11/16/2022	Radiant Logic Cryptographic Module for Java	Radiant Logic Inc.	Software Version: 3.0.2.1
4376	11/21/2022	REDCOM Crypto Module	REDCOM Laboratories, Inc.	Software Version: 2.2.1
4377	11/21/2022	CyberArk Cryptographic Module	CyberArk Software Ltd.	Software Version: 2.2.1
4379	11/26/2022	Versa Networks Branch	Versa Networks, Inc.	Software Version: 1.0
4380	11/26/2022	Versa Networks Controller	Versa Networks, Inc.	Software Version: 1.0
4381	11/28/2022	OmniSwitch AOS Cryptographic Module	Alcatel Lucent Enterprise USA Inc.	Software Version: 8.6.R11
4382	11/28/2022	cVu 16100 Network Packet Broker	cPacket Networks, Inc.	Hardware Version: cVu 16100 NG TAA; Firmware Version: 21.3.0