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

April 2024

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: 2024.05.02 17:25:18 -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: 2024.05.02 11:55:50-04'00' Foxit PDF Editor Version: 12.1.2

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
4684	04/02/2024	Thales Luna K7 Cryptographic Module	Thales	Hardware Version: 808-000048-002, 808-000048-003, 808-000066-001, 808-000073-001, 808-000073-002; Firmware Version: 7.8.4 with bootloader version 1.1.1, 1.1.2, 1.1.4 or 1.1.5
4685	04/02/2024	Honeywell Mobility EdgeTM BoringCrypto	Honeywell International, Inc.	Software Version: dcdc7bbc6e59ac0123407a9dc4d1f43dd0d117cd
4686	04/03/2024	Virtual TPM	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
4687	04/03/2024	Cryptographic Primitives Library	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
4688	04/03/2024	BitLocker Dump Filter	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
4689	04/03/2024	Pensando TLS Library	Pensando Systems, Inc	Software Version: 1.0
4690	04/05/2024	Eclypses Cryptographic Library	Eclypses, Inc.	Software Version: 1.0.0; Hardware Version: N/A; Firmware Version: N/A
4691	04/12/2024	SUSE Rancher Kubernetes Cryptographic Library	SUSE LLC	Software Version: 853ca1ea1168dff08011e5d42d94609cc0ca2e27
4692	04/15/2024	BlueCat Catcrypt for Java	BlueCat Networks	Software Version: 1.0.2.4
4693	04/16/2024	CyberArk Cryptographic Module for Java	CyberArk Software Ltd	Software Version: 3.0.2.1
4694	04/24/2024	VMware's BoringCrypto Module	Broadcom Inc.	Software Version: 6.0
4695	04/24/2024	Thunder	A10 Networks, Inc.	Hardware Version: TH1040, TH3350S, TH6655S and TH7655S; Firmware Version: 5.2.1-P5
4696	04/30/2024	BSAFE(TM) Java Crypto Module 6.3	Dell Australia Pty Limited, BSAFE Product Team	Software Version: 6.3
4697	04/30/2024	BSAFE(TM) Java Crypto Module 6.3	Dell Australia Pty Limited, BSAFE Product Team	Software Version: 6.3