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

February 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: 2020.04.23 10:04:41 -04'00'

Dated: _____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: ___March 2 2020_____

Manager, Product Assurance and Standards
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
3614	02/04/2020	ASI-HSM AHX5 KNET Cryptographic Module	Kryptus	Hardware Version: 1.0.1; Firmware Version: 1.0.1
3615	02/06/2020	Windows OS Loader	Microsoft Corporation	Software Version: 10.0.17763
3616	02/19/2020	Oracle Linux 7 NSS Cryptographic Module	Oracle Corporation	Software Version: R7-4.0.0
3617	02/19/2020	AWS Key Management Service HSM	Amazon Web Services, Inc.	Hardware Version: 2.0; Firmware Version: 1.5.132 and 1.5.135
3618	02/19/2020	Amazon Linux 2 Libgcrypt Cryptographic Module	Amazon Web Services, Inc.	Software Version: 1.0
3619	02/20/2020	Cyphre Crypto Core	Cyphre Security Solutions, LLC	Software Version: OpenSSL-FIPS-Cyphre-v1.0; Hardware Version: NXP QorIQ P4080 Rev3
3620	02/21/2020	Hypori Cryptographic Module for BoringSSL	Intelligent Waves	Software Version: 66005f41fbc3529ffe8d007708756720529da20d
3621	02/24/2020	Juniper Networks MX80, MX104, MX240, MX480, MX960 3D Universal Edge Routers with RE-S-X6-64G/RE-S-X6-128G Routing Engine and MIC-MACSEC-20GE MACSec Card	Juniper Networks, Inc.	Hardware Version: MX80, MX104, MX240, MX480, MX960 with components identified in Security Policy Table 1; Firmware Version: Junos OS 18.3R1-S1
3622	02/25/2020	Ubuntu 18.04 OpenSSL Cryptographic Module	Canonical Ltd.	Software Version: 2.0
3623	02/26/2020	F5(R) vCMP Cryptographic Module	F5 Networks	Firmware Version: 14.1.0.3 EHF
3624	02/26/2020	Socionext Secure Module	Socionext Inc.	Hardware Version: 0x00000001; Firmware Version: 0x00010004