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

December 2023

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

Dated:

Digitally signed by TIMOTHY HALL
Date: 2024.01.08 10:37:33 -05'00'

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: King, Lyall

Dated:

Digitally signed by King, Lyall
DN: C=CA, O=GC, OU=CSE-CST, CN="King, Lyall"
Reason: I am approving this document
Location:
Date: 2024.01.08 09:18:08-05'00'
Foxit PDF Editor Version: 12.1.2

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4668	12/05/2023	Prisma SD-WAN Controller's Cryptographic Module	Palo Alto Networks, Inc.	Software Version: 1.0
4669	12/08/2023	RapidIdentity FIPS Cryptographic Module	Identity Automation	Software Version: 2.0
4670	12/12/2023	Kernel Mode 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
4671	12/14/2023	7705 SAR-OS SAR-A/M Cryptographic Module (SARCM)	Nokia Corporation	Software Version: SAR-OS 21.10R5
4672	12/14/2023	7705 SAR-OS SAR-18/8/X/Ax/Wx/W/H/Hc Control Plane Cryptographic Module (SARCM)	Nokia Corporation	Software Version: SAR-OS 21.10R5