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

March 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: 2024.04.05 10:54:39 -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: 2024.04.04 11:10:40-04'00'
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
4679	03/11/2024	JCOP 4.5 on P71D600	NXP Semiconductors, Inc.	Hardware Version: N7122 A1; Firmware Version: [Platform ID J3R6000373181200 and ROM ID B3375FE9B5508BC4 and Patch ID 0000000000000000 and NXP IoT applet v7.2.22 and NXP SEMS Lite applet v2.0.2.11]
4680	03/19/2024	Hypersecu HYP2003 MFA Cryptographic Module	Hypersecu Information Systems Inc.	Hardware Version: SLE78CLUFX5000PH; Firmware Version: 7.04
4681	03/25/2024	Samsung NVMe TCG Opal SSC SEDs BM1733a Series	Samsung Electronics Co., Ltd.	Hardware Version: MZEM515THALC-00AMV; Firmware Version: MPOA3A5Q
4682	03/27/2024	Nokia BC-FJA (Bouncy Castle FIPS Java API)	NOKIA SOLUTIONS AND NETWORKS OY	Software Version: 1.0.2.3
4683	03/27/2024	Zebra DCS Cryptographic Library	Zebra Technologies Corporation	Firmware Version: DAACUS00-002-R00 on Zebra CR6080, and DAACWS00-002-R00 on Zebra CS6080