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

January 2019

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 A Cooper

Dated: 2/6/2019

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 2019 - Feb - 06

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
3347	01/02/2019	Certes Enforcement Points	Certes Networks, Inc.	Hardware Version: CEP220, CEP250, CEP300, CEP420, CEP520; Firmware Version: CEP v5.3
3348	01/02/2019	Oracle Linux Unbreakable Enterprise Kernel (UEK) Cryptographic Module	Oracle Corporation	Software Version: R6-1.0.0[1] and R7-2.0.0[2]
3349	01/02/2019	SecureDrive BT	SECUREDATA, Inc.	Hardware Version: SD-BT-12-BU-1TB, SD-BT-12-BU-2TB, SD-BT-20-BU-1TB, SD-BT-20-BU-2TB, SD-BT-20-BU-4TB, SD-BT-20-BU-5TB, SD-BT-12-BU-250GB-SSD, SD-BT-12-BU-500GB-SSD, SD-BT-12-BU-1TB-SSD, SD-BT-12-BU-2TB-SSD, SD-BT-12-BU-4TB-SSD, SD-BT-12-BU-8TB-SSD; Firmware Version: CLEVX_SATA-BT_v2.3 and (CLEVX_3637E_USB_V0313 or CLEVX_3637E_USB_V0314)
3350	01/03/2019	Sansec HSM	Beijing Sansec Technology Development Co., Ltd	Hardware Version: SecHSM-V2; Firmware Version: 1.0.12
3351	01/28/2019	Enhanced Bandwidth Efficient Modem (EBEM) Cryptographic Module	Viasat, Inc.	Hardware Version: P/Ns 1010162 Version 1, 1010162 with ESEM Version 1, 1091549 Version 1, 1075559 Version 1, 1075559 with ESEM Version 1, 1091551 Version 1, 1010163 Version 1, 1010163 with ESEM Version 1, 1091550 Version 1, 1075560 Version 1, 1075560 with ESEM Version 1 and 1091552 Version 1; P/N 1047117 (tamper evident seal applied over ESEM); Firmware Version: 02.11.06
3352	01/28/2019	SC4000 Series Mesh Radio	Silvus Technologies, Inc.	Hardware Version: P/Ns SC42-SUB-FIPS Rev A1 and SC44-SUB-FIPS Rev A1; Firmware Version: 3.16.0.0
3353	01/29/2019	Okta Cryptographic Module for Java	Okta, Inc.	Software Version: 2.1
3354	01/30/2019	Samsung BoringSSL Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 1.2.1
3355	01/31/2019	Cisco Firepower Management Center Virtual (FMCv) Cryptographic Module	Cisco Systems, Inc.	Software Version: 6.2