

FIPS 140-2 Consolidated Validation Certificate



The National Institute of Standards and Technology of the United States of America



April 2023



The Canadian Centre for Cyber Security

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: _____

Dated: _____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: _____

Director, Risk Mitigation Programs
Canadian Centre for Cyber Security

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4463	04/05/2023	Ascom Smartphone BoringCrypto v2	Ascom Sweden AB	Software Version: dcdc7bbc6e59ac0123407a9dc4d1f43dd0d117cd
4464	04/05/2023	Ubuntu 18.04 Azure Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 2.0
4465	04/06/2023	F5(R) Device Cryptographic Module	F5, Inc	Hardware Version: BIG-IP i7800 and BIG-IP 10350v-F with FIPS Kit P/N: F5-ADD-BIG-FIPS140; Firmware Version: 14.1.2
4466	04/07/2023	AxioCrypto-M235x	Security Platform Inc.	Hardware Version: 1.0; Firmware Version: 2.1.0
4467	04/07/2023	Trusted Platform Module 2.0 SLB 9672 FW 16.10, FW 16.12 and SLB 9673 FW 26.10	Infineon Technologies AG	Hardware Version: P/Ns SLB 9672AU20 (Package PG-UQFN-32-1 or PG-UQFN-32-2) [1], SLB 9672XU20 (Package PG-UQFN-32-1 or PG-UQFN-32-2) [1], SLB 9673AU20 (Package PG-UQFN-32-1 or PG-UQFN-32-2) [2] and SLB 9673XU20 (Package PG-UQFN-32- or PG-UQFN-32-2) [2]; Firmware Version: 16.10.16488 [1], 16.12.16858 [1] and 26.10.16688 [2]
4468	04/07/2023	Trusted Platform Module 2.0 SLB 9672 FW 17.10, FW 17.12 and SLB 9673 FW 27.10	Infineon Technologies AG	Hardware Version: PNs SLB 9672AU20 (Package PG-UQFN-32-3) [1] and SLB 9673AU20 (Package PG-UQFN-32-3) [2]; Firmware Version: 17.10.16488 [1], 17.12.16858 [1] and 27.10.16688 [2]
4469	04/10/2023	Poly Unified Communications Cryptographic Module	Plantronics, Inc.	Hardware Version: Qualcomm Snapdragon 835 and NXP i.MX 8M; Firmware Version: 1.0
4470	04/11/2023	RSA BSAFE(R) Crypto-C Micro Edition	Dell Inc., BSAFE Product Team	Software Version: 4.1.4
4471	04/14/2023	F5(R) Device Cryptographic Module	F5, Inc.	Hardware Version: BIG-IP i4000, BIG-IP i5000, BIG-IP i5820-DF, BIG-IP i7000, BIG-IP i7820-DF, BIG-IP i10800, BIG-IP i11800-DS, BIG-IP i15800, BIG-IP 5250v-F, BIG-IP 7200v-F, BIG-IP 10200v-F, BIG-IP 10350v-F, VIPRION B2250, VIPRION B4450; Firmware Version: 14.1.0.3 EHF
4472	04/14/2023	Amazon Linux 2 GnuTLS Cryptographic Module	Amazon Web Services, Inc.	Software Version: 1.0
4473	04/14/2023	Hewlett Packard Enterprise OpenSSL Cryptographic Module on Red Hat Enterprise Linux	Aruba, a Hewlett Packard Enterprise Company	Software Version: rhel8.20210325
4474	04/14/2023	FastIron ICX™ 7450 Series Switch/Router	CommScope Technologies LLC	Hardware Version: ICX7450-24P, ICX7450-48P, ICX7450-48F, ICX7400-4X1GF, ICX7400-4X10GF, ICX7400-4X10GC, ICX7400-1X40GQ, ICX7400-SERVICE-MOD, RPS16-E, RPS16DC-E, RPS16-I, RPS16DC-I, ICX-FAN10-I, ICX-FAN10-E, Filler Panel; Firmware Version: IronWare R08.0.95g
4475	04/14/2023	Q-Box	Q-Net Security, Inc.	Hardware Version: 100211; Firmware Version: 2.2.2
4476	04/14/2023	FastIron ICX™ 7650 Series Switch/Router	CommScope Technologies LLC	Hardware Version: P/Ns ICX7650-48F, ICX7650-48P and ICX7650-48ZP; Firmware Version: IronWare R08.0.95g
4477	04/17/2023	F5(R) vCMP Cryptographic Module	F5, Inc.	Firmware Version: 14.1.0.3 EHF

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4478	04/17/2023	Samsung SCrypto Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 2.5
4479	04/17/2023	eToken 5110+ FIPS	Thales	Hardware Version: 909-000156-001 - A3016629, 909-000157-001 - A3016639; Firmware Version: 5110+ FIPS - FW ver-22-00-0000, IDCore3130 - Build12G, IDPrime 930 Applet V4.5.0F, MSPNP Applet V1.2
4480	04/17/2023	eToken 5110+ FIPS	Thales	Hardware Version: 909-000154-001 - A3014536; Firmware Version: 5110+ FIPS - FW ver-22-00-0000, IDCore3130 - Build12G, IDPrime 930 Applet V4.5.0F, MSPNP Applet V1.2
4481	04/17/2023	ADYTON Cryptographic Module	Worldline S/ANV	Hardware Version: 9071000001; Firmware Version: 1.3.0
4482	04/17/2023	CLEAR Cryptosystem	Quantum Knight, INC.	Software Version: 3.0.2.1
4483	04/17/2023	Forescout OpenSSL FIPS Module	Forescout Technologies, Inc.	Software Version: 2.2.1
4484	04/17/2023	Boot Manager	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
4486	04/26/2023	Cisco Catalyst 9300 Series Switches	Cisco Systems, Inc.	Hardware Version: Cisco Catalyst 9300-24T, Cisco Catalyst 9300-24P, Cisco Catalyst 9300-24U, Cisco Catalyst 9300-24UX, Cisco Catalyst 9300-48T, Cisco Catalyst 9300-48P, Cisco Catalyst 9300-48U, Cisco Catalyst 9300-48UX and Cisco Catalyst 9300-48UN; Firmware Version: Cisco IOS-XE 16.9.2, Cisco IOS-XE 16.12 and Cisco IOS-XE 17.3
4487	04/26/2023	Cisco Catalyst 9200L Series Switches	Cisco Systems, Inc.	Hardware Version: Cisco Catalyst C9200L-24P-4G, Cisco Catalyst C9200L-24P-4X, Cisco Catalyst C9200L-24T-4G, Cisco Catalyst C9200L-24T-4X, Cisco Catalyst C9200L-48P-4G, Cisco Catalyst C9200L-48P-4X, Cisco Catalyst C9200L-48T-4G, Cisco Catalyst C9200L-48T-4X, Cisco Catalyst C9200L-24P8X-2Y, Cisco Catalyst C9200L-24P8X-4X, Cisco Catalyst C9200L-48P12X-4X and Cisco Catalyst C9200L-48P8X-2Y; Firmware Version: Cisco IOS-XE 16.12 and Cisco IOS-XE 17.3
4488	04/26/2023	ControlUp Cryptographic Library	ControlUp Technologies, Inc.	Software Version: 1.0.2
4489	04/26/2023	Digi DAL OS OpenSSL 3.0	Digi International	Software Version: 3.0.0
4490	04/26/2023	AWS OpenSSL FIPS Provider	Amazon Web Services, Inc.	Software Version: 3.0.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4491	04/27/2023	FastIron ICX™ 7750, ICX™ 7250 and ICX™ 7150 Series Switch/Router	CommScope Technologies LLC	Hardware Version: Base Models: ICX7150-C12P-2X10GR-A [1], ICX7150-24-4X10GR-A [2], ICX7150-24P-4X10GR-A [3], ICX7150-48-4X10GR-A [4], ICX7150-48P-4X10GR-A [5], ICX7150-48PF-4X10GR-A [6], ICX7150-48ZP-8X10GR2-A [7], ICX7250-24G [8], ICX7250-48P [9], ICX7750-48F [10], ICX7750-48C [11], ICX7750-26Q [12]; with Power Supply components: RPS20 [7], EPS4000 [8, 9], RPS17 [7, 8, 9], RPS9I [10, 11, 12], RPS9E [10, 11, 12], RPS9DCI [10, 11, 12], RPS9DCE [10, 11, 12]; with Fan components: ICX-FAN11 [7], ICX7750-FAN-I [10, 11, 12], ICX7750-FAN-E [10, 11, 12], ICX7750-FAN-I- SINGLE [10, 11, 12], ICX7750-FAN-E- SINGLE [10, 11, 12]; and optional component: ICX7750-6Q [10, 11, 12]; Firmware Version: IronWare R08.0.95g
4492	04/27/2023	Trellix FIPS Provider	Trellix	Software Version: 3.0.0a
4493	04/27/2023	Oracle Cloud Infrastructure for BoringCrypto	Oracle Corporation	Software Version: 853ca1ea1168dff08011e5d42d94609cc0ca2e27
4494	04/28/2023	Cisco Catalyst 9300 Series Switches	Cisco Systems, Inc.	Hardware Version: Cisco Catalyst 9300-24S, Cisco Catalyst 9300-48S, Cisco Catalyst 9300L-24T-4G, Cisco Catalyst 9300L-24P-4G, Cisco Catalyst 9300L-48T-4G, Cisco Catalyst 9300L-48P-4G, Cisco Catalyst 9300L-24T-4X, Cisco Catalyst 9300L-24P-4X, Cisco Catalyst 9300L-48T-4X, Cisco Catalyst 9300L-48P-4X, Cisco Catalyst 9300L-24UX-4X, Cisco Catalyst 9300L-48UX-4X, Cisco Catalyst 9300L-24UX-2Q and Cisco Catalyst 9300L-48UX-2Q; Firmware Version: Cisco IOS-XE 16.12 and Cisco IOS-XE 17.3
4495	04/30/2023	FIPS AP43	Mist Systems	Hardware Version: AP43-FIPS-US [REV. AA and AB] and AP43E-FIPS-US [REV. AA and AB]; Firmware Version: fips_apfw-0.9.23115-illyrio-9e5f