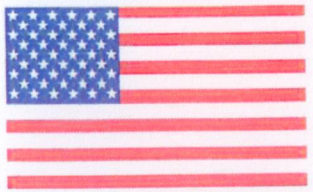
FIPS 140-2 Consolidated Validation Certificate



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

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0043

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, 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 J Cooper

Dated: 1 Aug 2014

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 1 Aug 2014

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2201	07/07/2014	IBM System Storage TS1140 Tape Drive - Machine Type 3592, Model E07	IBM® Corporation	Hardware Version: EC Level: M11776, P/N: 00V6759; Firmware Version: EC Level: M11776, P/N: 35P2401
2202	07/07/2014	IDPrime MD 830 with OATH & MPCOS applets	Gemalto	Hardware Version: SLE78CFX3009P; Firmware Version: IDCore 30 Build 1.17, IDPrime MD Applet version V4.1.2.F with MSPNP Applet V1.0, OATH Applet V2.11 and MPCOS Applet V3.8
2203	07/09/2014	Pitney Bowes iButton Postal Security Device (PSD)	Pitney Bowes, Inc.	Hardware Version: MAXQ1959B-F50#; Firmware Version: 09.02.00; Indicia Type: 0, 1, 2, 5, 7 and 8
2204	07/07/2014	ePass Token	Feitian Technologies Co., Ltd.	Hardware Version: 1.0.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2205	07/09/2014	Brocade® MLXe® and Brocade NetIron® CER 2000 Series Ethernet Routers	Brocade Communications Systems, Inc.	Hardware Versions: BR-MLXE-4-MR-M-AC, BR-MLXE-4-MR-M-DC, BR-MLXE-8-MR-M-AC, BR-MLXE-8-MR-M-DC, BR-MLXE-16-MR-M-AC, BR-MLXE-16-MR-M-DC, BR-MLXE-4-MR2-M-AC, BR-MLXE-4-MR2-M-DC, BR-MLXE-8-MR2-M-AC, BR-MLXE-8-MR2-M-DC, BR-MLXE-16-MR2-M-AC, BR-MLXE-16-MR2-M-DC, NI-CER-2048F-ADVPREM-AC, NI-CER-2048F-ADVPREM-DC, NI-CER-2048FX-ADVPREM-AC, NI-CER-2048FX-ADVPREM-DC, NI-CER-2024F-ADVPREM-AC, NI-CER-2024F-ADVPREM-DC, NI-CER-2024C-ADVPREM-AC, NI-CER-2024C-ADVPREM-DC, NI-CER-2048C-ADVPREM-AC, NI-CER-2048C-ADVPREM-DC, NI-CER-2048CX-ADVPREM-AC and NI-CER-2048CX-ADVPREM-DC with FIPS Kit (P/N Brocade XBR-000195) and NI-MLX-MR and BR-MLX-MR2-M Management Modules; Firmware Version: IronWare Release R05.3.00ea or IronWare Release R05.4.00cb

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2206	07/09/2014	Aviat Networks Eclipse Cryptographic Module	Aviat Networks, Inc.	Hardware Versions: NUe 2RU Chassis (P/N EXE-002), Fan Card (P/N EXF-101), Node Controller Card (P/N EXN-004), FIPS Installation Kit (P/N 179-530153-001), Replacement Labels (P/N 007-600331-001), at least one of: [RAC 6X (P/N EXR-600-001), RAC 6XE (P/N EXR-600-002), RAC 60 (P/N EXR-660-001), or RAC 60E (P/N EXR-660-002)] and all remaining slots filled by one of the following: P/N 131-501768-001, EXA-001, EXD-040-001, EXD-152-001, EXD-153-001, EXD-156-001, EXD-160-001, EXD-161-001, EXD-171-001, EXD-180-002, EXD-180-005, EXD-180-102, EXD-181-001, EXD-181-002, EXD-252-001, EXD-331-001, EXD-400-002, EXP-024, EXR-910-001, EXR-999-003, EXS-001, EXS-002 or EXX-001; Firmware Versions: 07.07.10, 08.00.55 and 08.00.70
2207	07/09/2014	MultiApp V3 Platform	Gemalto	Hardware Versions: M7820 SLE78CLX1600P (Contact-only) and M7820 SLE78CLX1600P (Contactless-only); Firmware Version: MultiApp V3.0, Demonstration Applet V1.2

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2208	07/11/2014	CN Series Ethernet Encryptors	Senetas Corporation Ltd. and SafeNet Inc.	Hardware Versions: Senetas Corp. Ltd. CN4010 Series: A4010B [O] (DC); Senetas Corp. Ltd. CN6010 Series: A6010B [O] (AC), A6011B [O] (DC) and A6012B [O] (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN4010 Series: A4010B [Y] (DC); Senetas Corp. Ltd. & SafeNet Inc. CN6010 Series: A6010B [Y] (AC), A6011B [Y] (DC) and A6012B [Y] (AC/DC); Firmware Version: 2.4.0
2209	07/11/2014	Verdi Self Encrypting Drive (SED)	Western Digital Corporation	Hardware Version: WD4001FYUG-01UVZ; Firmware Version: VR08
2210	07/11/2014	3e-636M CyberFence Cryptographic Module	3e Technologies International, Inc.	Hardware Version: 1.0; Firmware Version: 5.1
2212	07/23/2014	Suite B Cryptographic Module	United States Special Operations Command (USSOCOM)	Software Version: 2.3.1
2213	07/23/2014	Aspen	Sony Corporation	Hardware Version: 2.0.0; Firmware Versions: 1.2.1 and 1.2.2
2214	07/31/2014	Samsung Kernel Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: SKC 1.4.1.3
2215	07/31/2014	Motorola GGM 8000 Gateway	Motorola Solutions, Inc.	Hardware Version: Base Unit P/N CLN1841E Rev A with FIPS Kit P/N CLN8787A Rev B and Power Supply [P/N CLN1850A Rev G (AC) or P/N CLN1849A Rev H (DC)]; Firmware Version: XS-16.6.0.69, GS-16.6.0.69 or KS-16.6.0.69
2216	07/31/2014	Motorola Network Router (MNR) S6000	Motorola Solutions, Inc.	Hardware Version: Base Unit P/N CLN1780L Rev E with Encryption Module P/N CLN8261D Rev N; Firmware Version: GS-16.6.0.69 or PS-16.6.0.69