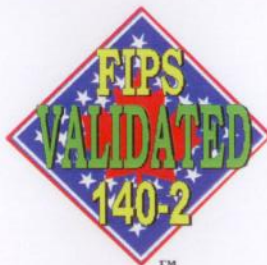


FIPS 140-2 Consolidated Validation Certificate



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. 0011


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: 
Dated: 13 Dec 2011

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: 
Dated: 5 December, 2011

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 |
|---------------------------|----------------------------------|-------------------------------------|--------------------------------|--|
| 1625 | 11/30/2011 | Mocana Cryptographic Suite B Module | Mocana Corporation | Software Version: 5.3.1v |
| 1627 | 11/01/2011 | Port Authority Series | Communication Devices Inc. | Hardware Versions: PA111-SA CDI 01-03-0912B, PA111-RM CDI 01-03-0912B, PA155-RM CDI 01-03-0912B and PA199-RM CDI 01-03-0912B; Firmware Version: 10.00.78 |
| 1628 | 11/07/2011 | XM Crypto Module | NAL Research Corporation | Firmware Version: 1.1.0 |
| 1629 | 11/16/2011 | PMCryptolib | Protected Mobility LLC | Software Version: 1.0 |
| 1630 | 11/10/2011 | Infraguard Processor Module | Advantor Systems, LLC | Hardware Version: 5.1; Firmware Version: 1.01 |
| 1632 | 11/10/2011 | Samsung Key Management Module | Samsung Electronics Co., Ltd. | Software Version: 1.0 |
| 1633 | 11/10/2011 | Dolphin DCI 1.2 | Doremi Cinema LLC | Hardware Versions: DOLPHIN-DCI-1.2-A0, DOLPHIN-DCI-1.2-A1, DOLPHIN-DCI-1.2-C0 and DOLPHIN-DCI-1.2-C1; Firmware Versions: 2.0.8p, 21.03m-1 and 99.03f |
| 1634 | 11/10/2011 | MIIKOO | Pierson Capital Technology LLC | Hardware Version: D4; Firmware Versions: Device Bootstrap v3.1, Device Application 006262 and Cryptographic Algorithm v2.1 |

| Certificate Number | Validation / Posting Date | Module Name(s) | Vendor Name | Version Information |
|--------------------|---------------------------|--|------------------------|--|
| 1635 | 11/10/2011 | Seagate Secure Constellation® ES.2 [10-16], Savvio® 10K.5 [1-6] and Savvio® 15K.3 [7-9] Self-Encrypting Drives FIPS 140 Module | Seagate Technology LLC | Hardware Versions: 9XS066 [1], 9XS066-251 [2], 9XS066-257 [3], 9XS066-047 [4], 9XS066-090 [5], 9XR066 [1], 9XR066-251 [2], 9XR066-257 [3], 9XR066-047 [4], 9XR066-090 [5], 9XR066-038 [6], 9XP066 [1], 9XP066-047 [2], 9XP066-090 [3], 9XN066 [1], 9XN066-251 [2], 9XN066-257 [3], 9XN066-047 [4], 9XN066-090 [5], 9XM066 [7], 9XM066-251 [8], 9XM066-257 [9], 9XL066 [7], 9XL066-251 [8], 9XL066-257 [9], 9XT260 [10], 9XT260-251 [11], 9XT260-257 [12], 9XT260-038 [13], 9XT260-047 [14], 9XT260-090 [15] and 9XT160 [16]; Firmware Versions: A002 [1], CSF2 [2], CNF1 [3], NS03 [4], HF72 [5], NA00 [6], A002 [7], YSF3 [8], YNF2 [9], 0002 [10], RSF3 [11], RNF3 [12], NQE1 [13], NS01 [14], NF72 [15] and F000 [16] |
| 1636 | 11/10/2011 | Seagate Secure Constellation® ES [7-9] and Constellation®.2 [1-6] Self-Encrypting Drives FIPS 140 Module | Seagate Technology LLC | Hardware Versions: 9XU268 [1], 9XU268-251 [2], 9XU268-257 [3], 9XU268-047 [4], 9XU268-090 [5], 9XU264 [1], 9XU264-251 [2], 9XU264-257 [3], 9XU264-047 [4], 9XU264-090 [5], 9XU168 [6], 9XU164 [6], 9XU162 [6], 1AV268 [7], 1AV264 [7], 1AV264-257 [8], 1AV262 [7], 1AV168 [9], 1AV164 [9] and 1AV162 [9]; Firmware Versions: A002 [1], ASF2 [2], ANF1 [3], NS01 [4], QF70 [5], 0002 [6], A001 [7], PNF0 [8] and A001 [9] |
| 1637 | 11/16/2011 | Security Builder FIPS Java Module | Certicom Corp. | Software Version: 2.8 |

| Certificate Number | Validation / Posting Date | Module Name(s) | Vendor Name | Version Information |
|--------------------|---------------------------|--|--|---|
| 1638 | 11/16/2011 | HiKey - Flash and HiKey PKI Token | Chunghwa Telecom Co., Ltd. Telecommunication Laboratories | Hardware Versions: 2.0 and 2.1; Software Version: Card OS version 3.2 with PKI Applet: 2.1; Firmware Version: 2.0 |
| 1639 | 11/16/2011 | Cisco 5940 Embedded Services Routers | Cisco Systems, Inc. | Hardware Versions: Cisco 5940 ESR air-cooled card and Cisco 5940 ESR conduction-cooled card; Firmware Version: 15.1(2)GC1 |
| 1640 | 11/17/2011 | WatchKey USB Token | Watchdata Technologies Pte Ltd | Hardware Version: K6 with Z32L256D32U and K003010A; Firmware Version: 360C6702 |
| 1641 | 11/17/2011 | Mocana Cryptographic Suite B Module | Mocana Corporation | Software Version: 5.4fm |
| 1642 | 11/21/2011 | PKI BLADE Cosmo | U.S. Department of State | Hardware Version: P/N B0; Firmware Version: FC10 (with op- code 071964) with ID-One PIV Applet Suite V2.3.2-a and PKI BLADE Applet V1.2 |
| 1643 | 11/29/2011 | Cisco Common Cryptographic Module (C3M) | Cisco Systems, Inc. | Software Version: 0.9.8r.1.1 |