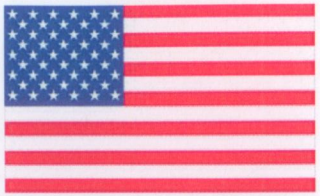
FIPS 140-2 Consolidated Validation Certificate



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. 0003

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: Dawn F Dodson

Dated: March 7, 2011

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: February 25, 2011

Director, Industry Program Group
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1491	01/28/2011	HX280 Broadband Satellite Router	Hughes Network Systems, LLC	Hardware Version: Rev C.; Firmware Version: 6.6.0.3
1492	02/04/2011	IBM® z/OS® Version 1 Release 11 System SSL Cryptographic Module	IBM® Corporation	Hardware Version: FC3863 w/System Driver Level 77, CEX3A and CEX3C [CEX3A and CEX3C are separately configured versions of 4765-001 (P/N 45D6048)]; Software Version: System SSL level HCPT3B0/JCPT3B1 with APAR OA31595, RACF level HRF7760 with APAR OA30951 and ICSF level HCR7770 with APAR OA32012; Firmware Version: 4765-001 (e1ced7a0)
1496	02/10/2011	Cisco Secure Access Control Server (ACS) FIPS module (cryptolib)	Cisco Systems, Inc.	Software Version: 1.1
1497	02/10/2011	Cisco Secure Access Control Server (ACS) FIPS module (NSS)	Cisco Systems, Inc.	Software Version: 3.12.5
1499	02/10/2011	PA-500, PA-2000 Series and PA-4000 Series Firewalls	Palo Alto Networks	Hardware Version: HW P/N 910-000006-00D Rev. D with FIPS Kit P/N 920-000005-001 Rev. 1 (PA-500), HW P/N 910-000004-00K Rev. K with FIPS Kit P/N 920-000004-001 Rev. 1 (PA-2020), HW P/N 910-000003-00K Rev. K with FIPS Kit P/N 920-000004-001 Rev. 1 (PA-2050), HW P/N 910-000002-00Q Rev. Q with FIPS Kit P/N 920-000003-001 Rev. 1 (PA-4020), HW P/N 910-000001-00P Rev. P with FIPS Kit P/N 920-000003-001 Rev. 1 (PA-4050) and HW P/N 910-000005-00G Rev. G with FIPS Kit P/N 920-000003-001 Rev. 1 (PA-4060); Firmware Version: 3.1.2
1500	02/10/2011	Pragma Systems Cryptographic Module	Pragma Systems, Inc.	Software Version: 1.0.0.12

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1501	02/24/2011	Cryptographic Module for F5 and C5	ActivIdentity, Inc.	Software Version: 1.7.0.4
1502	02/24/2011	RSA BSAFE® Crypto-J JSAFE and JCE Software Module	RSA, The Security Division of EMC	Software Version: 5.0
1503	02/24/2011	RSA BSAFE® Crypto-J JSAFE and JCE Software Module	RSA, The Security Division of EMC	Software Version: 5.0
1504	02/24/2011	Data Locker Enterprise, V2.0	Data Locker Inc.	Hardware Versions: P/Ns DL500E2 and DL1000E2; Firmware Version: 2.30
1505	02/24/2011	IBM 4765 Cryptographic Coprocessor Security Module	IBM® Corporation	Hardware Version: P/N 45D6048 Version 1.0; Firmware Version: e1ced7a0