

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. 0033

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: 10/17/13

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 1 October, 2013

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

12. 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
1891	09/06/2013	Microsoft Windows 8, Microsoft Windows Server 2012, Microsoft Windows RT, Microsoft Surface Windows RT, Microsoft Surface Windows 8 Pro, and Microsoft Windows Phone 8 Kernel Mode Cryptographic Primitives Library (CNG.SYS)	Microsoft Corporation	Software Version: 6.2.9200
1892	09/06/2013	Microsoft Windows 8, Microsoft Windows Server 2012, Microsoft Windows RT, Microsoft Surface Windows RT, Microsoft Surface Windows 8 Pro, and Microsoft Windows Phone 8 Cryptographic Primitives Library (BCRYPTPRIMITIVES.DLL)	Microsoft Corporation	Software Version: 6.2.9200
1893	09/13/2013	Microsoft Windows 8, Microsoft Windows Server 2012, Microsoft Windows RT, Microsoft Surface Windows RT, Microsoft Surface Windows 8 Pro, and Microsoft Windows Phone 8 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH.DLL)	Microsoft Corporation	Software Version: 6.2.9200
1895	09/13/2013	Microsoft Windows 8, Microsoft Windows Server 2012, Microsoft Windows RT, Microsoft Surface Windows RT, Microsoft Surface Windows 8 Pro, and Microsoft Windows Phone 8 Boot Manager	Microsoft Corporation	Software Version: 6.2.9200
1896	09/06/2013	Microsoft Windows 8, Microsoft Windows Server 2012, Microsoft Windows RT, Microsoft Surface Windows RT, Microsoft Surface Windows 8 Pro, and Microsoft Windows Phone 8 BitLocker® Windows OS Loader (WINLOAD)	Microsoft Corporation	Software Version: 6.2.9200

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1897	09/06/2013	Microsoft Windows 8, Microsoft Windows Server 2012, Microsoft Windows RT, Microsoft Surface Windows RT, Microsoft Surface Windows 8 Pro, and Microsoft Windows Phone 8 Code Integrity (CI.DLL)	Microsoft Corporation	Software Version: 6.2.9200
1898	09/06/2013	Microsoft Windows 8, Microsoft Windows Server 2012, and Microsoft Surface Windows 8 Pro BitLocker® Windows Resume (WINRESUME)	Microsoft Corporation	Software Version: 6.2.9200
1899	09/13/2013	Microsoft Windows 8, Microsoft Windows Server 2012, Microsoft Windows RT, Microsoft Surface Windows RT, Microsoft Surface Windows 8 Pro, and Microsoft Windows Phone 8 BitLocker® Dump Filter (DUMPFVE.SYS)	Microsoft Corporation	Software Version: 6.2.9200
1995	09/11/2013	Sun Crypto Accelerator 6000	Oracle Corporation	Hardware Versions: 375-3424, Revisions -02, -03, -04, -05 and -06; Firmware Versions: Bootstrap version 1.0.1 or 1.0.10, Operational firmware versions 1.1.7, 1.1.8, or 1.1.9
1996	09/06/2013	Fixmo Client Crypto Module	Fixmo, Inc.	Software Version: 1.0
1997	09/13/2013	Check Point CryptoCore	Check Point Software Technologies Ltd	Software Version: 2.0
1998	09/17/2013	Motorola Mobility Linux Kernel Software Cryptographic Module	Motorola Mobility LLC	Software Version: 1.0
1999	09/17/2013	Liberty™ Cryptographic Module	Thales Communications, Inc.	Firmware Version: 01.00.05.0018
2000	09/17/2013	SafeNet ProtectDrive Cryptographic Engine	SafeNet, Inc.	Software Version: 1.0.1
2001	09/17/2013	SafeNet ProtectDrive Cryptographic Engine	SafeNet, Inc.	Software Version: 1.0.1

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2002	09/19/2013	Cisco Catalyst 6503-E, Catalyst C6504-E, Catalyst 6506-E, Catalyst 6509-E and Catalyst 6513-E Switches with Supervisor Cards (VS-S2T-10G and VS-S2T-10G-XL) and Line Cards (WS-X6908-10G, WS-X6908-10G-2TXL, WS-X6904-40G-2T and WS-X6904-40G-2TXL)	Cisco Systems, Inc.	Hardware Versions: (6503-E -H0, 6504-E -G0, 6506-E -M0, 6509-E -N0 and 6513-E -S0; Supervisor Cards VS-S2T-10G -B0 and VS-S2T-10G-XL -C0; Line Cards WS-X6904-40G-2T -A0, WS-X6904-40G-2TXL -A0, WS-X6908-10G -A0 and WS-X6908-10G-2TXL-B0; Slot Cover SPA-BLANK -G0) with FIPS kit packaging (CVPN6500FIPS/KIT=); Firmware Version: 15.1(1)SY
2003	09/30/2013	IMS-SM	Doremi Labs	Hardware Versions: (IMS-SM-C1 and IMS-SM-C2) [1] and (IMS-SM-E1 and IMS-SM-E2) [2]; Firmware Versions: (4.0.3-0, 4.0.0-3 and 6.0.3-0) [1] and (4.2.0-4, 4.2.0-3 and 6.0.12-0) [2]
2004	09/30/2013	Covia Connector Cryptographic Module	Covia Labs, Inc.	Software Version: 2.0