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. 0032

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: 30 Sep 13

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 23 Sep 2013

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
1894	08/27/2013	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 Cryptographic Provider (RSAENH.DLL)	Microsoft Corporation	Software Version: 6.2.9200
1986	08/09/2013	TecSec Armored Card - Contactless Cryptographic Module	TecSec Incorporated	Hardware Version: P/N Inside Secure AT90SC28880RCFV Revision G; Firmware Versions: P/Ns Athena IDProtect Duo Version 010E.0264.0001, TecSec SSD Applet Version 1.001, TecSec PIV Applet Version 1.007, TecSec BOCC Applet Version 1.001, TecSec CKM Attribute Container Applet Version 1.002, TecSec CKM Info Applet Version 1.000
1987	08/13/2013	Wi-Q Portal Gateway	Stanley Security Solutions, Inc.	Hardware Version: 12562C; Firmware Version: 3.017.156
1988	08/13/2013	CN6000 Series Encryptors	Senetas Corporation Ltd.	Hardware Versions: CN6040 Series: A6040B (AC), A6041B (DC) and A6042B (AC/DC); CN6100 Series: A6100B (AC), A6101B (DC) and A6102B (AC/DC); Firmware Version: 2.2.0
1989	08/13/2013	Windows Embedded Compact Cryptographic Primitives Library (bcrypt.dll)	Microsoft Corporation	Software Version: 7.00.1687
1990	08/13/2013	IMB-1000 HFR and IMB-1200 HFR Secure Media Blocks	Ultra Stereo Labs, Inc.	Hardware Version: Rev. 14; Firmware Version: 02272013
1991	08/13/2013	Stonesoft Cryptographic Kernel Module	Stonesoft Corporation	Software Version: 1.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1992	08/19/2013	TecSec Armored Card - Contact Cryptographic Module	TecSec Incorporated	Hardware Version: P/N Inside Secure AT90SC320288RCT Revision E; Firmware Versions: P/Ns Athena IDProtect Version 0108.0264.0001, TecSec SSD Applet Version 1.001, TecSec PIV Applet Version 1.007, TecSec BOCC Applet Version 1.001, TecSec CKM Attribute Container Applet Version 1.002, TecSec CKM Info Applet Version 1.000
1993	08/27/2013	IBM® Java JCE FIPS 140-2 Cryptographic Module	IBM® Corporation	Software Version: 1.7
1994	08/27/2013	IBM® Crypto for C	IBM® Corporation	Software Version: 8.2.2.0