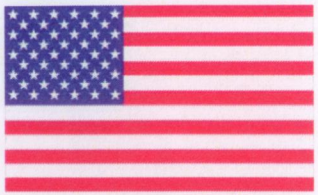
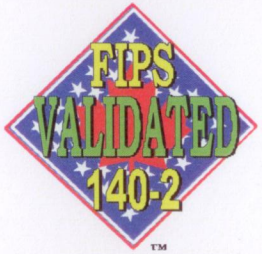
FIPS 140-2 Consolidated Validation Certificate



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. 0008

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: Sept 19, 2011

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: Sep 2, 2011

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1570	08/12/2011	Cruzer Enterprise FIPS Edition	SanDisk Corporation	Hardware Versions: P/Ns 54-89-15381-004G, 54-89-15381-008G, 54-89-15381-016G and 54-89-153-032G, Version Revision 1; Firmware Version: 9.5.21.01.F3
1577	08/05/2011	EXP9000 Hardware Security Module	Futurex	Hardware Version: P/N 9750-2075, Revision B; Firmware Version: 4.0.0
1580	08/10/2011	HP TippingPoint Security Management System	Hewlett-Packard TippingPoint	Firmware Version: 3.2.0.8312.3
1586	08/09/2011	Unified Platform Cryptographic Library	ZTE Corporation	Software Version: 1.1
1587	08/05/2011	ePO Cryptographic Module	McAfee Inc.	Software Version: 1.0
1588	08/05/2011	Agent Cryptographic Module	McAfee, Inc.	Software Version: 1.0
1589	08/10/2011	UEP Cryptographic Module	ZTE Corporation	Software Version: 4.11.10
1590	08/10/2011	STOP OS 7 Kernel Cryptographic Module	BAE Systems	Software Version: 1.1
1591	08/12/2011	Symantec Cryptographic Module	Symantec Corporation	Software Version: 1.0
1592	08/22/2011	Harris Unified Audio Card	Harris Corporation	Hardware Version: EA-103168-002; Firmware Versions: MPC 860: SK-007765-007 v R03A08, DSP: SK-007765-013 v R03A05, Boot Loader / Factory Test: R03A02, Low Level Boot: R01D01 and DSP Factory Test: R01D02
1593	08/22/2011	Mxtran Payeeton Solution	Mxtran Inc.	Hardware Version: MX11E25644E; Firmware Version: Simker v2.30
1595	08/31/2011	Symantec Enterprise Vault Cryptographic Module	Symantec Corporation	Software Version: 1.0
1596	08/31/2011	B400™ Remote Support Appliance	Bomgar Corporation	Hardware Version: B400; Software Version: 10.6.2 FIPS; Firmware Version: 3.2.2 FIPS

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1597	08/31/2011	B200™ and B300™ Remote Support Appliances	Bomgar Corporation	Hardware Version: B200 and B300; Software Version: 10.6.2 FIPS; Firmware Version: 3.2.2 FIPS