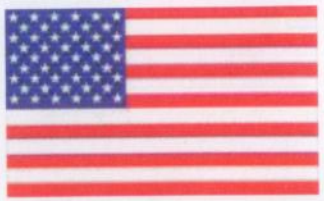
FIPS 140-2 Consolidated Validation Certificate



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. 0034

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: Michael J Cooper

Dated: 11/18/2013

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 7 NOV 2013

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2005	10/25/2013	Communication Server	Lenel Systems International, Inc.	Software Versions: 6.5.624 or 6.6.287
2006	10/25/2013	CHR Cryptographic Module	Bull SAS	Hardware Version: 005/A; Firmware Version: V1.04-00L
2007	10/25/2013	Standalone IMB	GDC Technology (USA), LLC	Hardware Versions: GDC-IMB-v2, R8 and R9; Firmware Version: 2.0 with Security Manager Firmware Version 1.3.0
2008	10/25/2013	HP TippingPoint Intrusion Prevention System	Hewlett-Packard TippingPoint	Hardware Versions: 5200NX and 7100NX; Firmware Version: 3.5