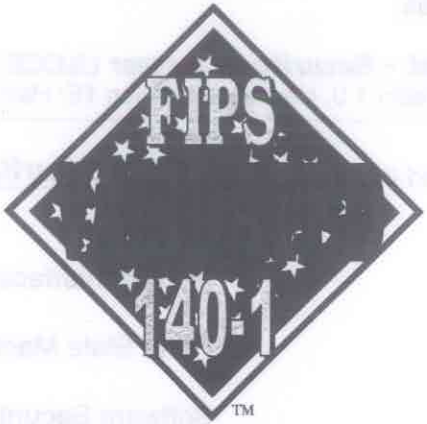
FIPS 140-1 Validation Certificate

The National Institute of Standards and Technology of the United States of America



The Communications Security Establishment of the Government of Canada

Certificate No. 123

The National Institute of Standards and Technology, as the United States FIPS 140-1 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-1 Cryptographic Module Validation Authority; hereby validate the FIPS 140-1 testing results of the Cryptographic Module identified as:

Advanced Configurable Crypto Environment - Security Processor (ACCE SP), *by Baltimore Technologies, Inc.*

(When operated in FIPS mode)

In accordance with the Derived Test Requirements for FIPS 140-1, *Security Requirements for Cryptographic Modules.* FIPS 140-1 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive But Unclassified Information* (United States) or *Designated Information* (Canada) within computer and communications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-1 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this 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.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-1 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 in the product identified as:

Advanced Configurable Crypto Environment – Security Processor* (ACCE SP), *by Baltimore Technologies, Inc.
(Firmware Version 1.0, Hardware Version 1E; Hardware)

and tested by the Cryptographic Module Testing accredited laboratory: ***Domus IT Security Laboratory*, NVLAP LAB CODE 200017-0** is as follows:

Cryptographic Module Design:	Level 4	Module Interfaces:	Level 4
Roles and Services:	Level 4	Finite State Machine Model:	Level 4
Physical Security: (Multi-chip embedded)	Level 4	Software Security:	Level 4
EMI / EMC:	Level 4	Self Tests:	Level 4
Key Management:	Level 4		

Operating System Security Level **N/A** is met when used in the following configuration(s): **N/A**

The following FIPS approved Cryptographic Algorithms are used: ***DES (Certs.#81 and #82); DES MAC; Triple DES (Certs.#23 and #24); Triple DES MAC; DSA/SHA-1 (Cert.#36); RSA (Vendor-affirmed)***

The Cryptographic module also contains the following non-FIPS approved algorithms: ***Diffie-Hellman Key Exchange*; MD5**

End user queries concerning the non-FIPS approved algorithms may be directed to their respective Cryptographic Module Validation Authority.

Overall Level Achieved: 4

Signed on behalf of the Government of the United States

Signature: _____

Dated: 7 December 2000

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 30 NOV 2000

Director, Information Protection Group
The Communications Security Establishment

Validated Cryptographic Module
ACCE SP v1.0 – Hardware 1E
November 20, 2000

The ACCE SP v1.0 has been validated to an overall FIPS 140-1 Security Level 4.

Description of the Cryptographic Module and the Product of Which it is a Part:
The ACCE SP v1.0 provides highly-secure cryptographic services and key storage. It is used in a range of Baltimore and OEM products along with an application (the *single user* of the ACCE SP) to provide custom functionality. An example use is the *Europay NSP* which was developed for Europay, a major European financial institution.

Implemented Cryptographic Algorithms:

- FIPS - approved: DES (ECB and CBC Mode), 3-DES (ECB and CBC),SHA-1 and
- Other: RSA, MD5, and Diffie-Hellman

The cryptographic module has been found to meet the indicated FIPS 140-1 security levels for the following sections:

SECTION	LEVEL ACHIEVED	EVALUATOR
Cryptographic Modules	Level 4	Megan Annette
Module Interfaces	Level 4	Megan Annette
Roles and Services	Level 4	Pamela Grannum, Megan Annette
Finite State Machine Model	Level 4	Pamela Grannum, Tim Boreham
Physical Security	Level 4	Vince Tam
Software Security	Level 4	Pamela Grannum, Tim Boreham
Operating System Security	Not Applicable	Pamela Grannum
Cryptographic Key Management	Level 4	Pamela Grannum
Cryptographic Algorithms	Level 4	Pamela Grannum, Dawn Adams
EMI/EMC	Level 4	Pamela Grannum
Self-Tests	Level 4	Pamela Grannum

NOTE: The Security Policy document, the Formal Security Policy Model and the Finite State Machine document were all written and prepared by Baltimore Technologies (UK) Ltd.

Vendor Address: BaltimoreTechnologies (UK) Ltd
61/62 Fitzwilliam Lane
Dublin 2, Ireland
http://www.baltimore.com

Vendor Point of Contact: Ralph Shaw
+353-1-647 7300