FIPS 140-2 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. **444**

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

Model 330G2 Smart Card *by* Datakey, Inc.

(When operated in FIPS mode)

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 *Designated Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module 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 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.

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments.

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 in the product identified as:

Model 330G2 Smart Card by Datakey, Inc.
(Hardware Version: 1.0, Firmware Version: 2.0, EXFs: GSC-IS application executable (G2 EXF) Version 22; Hardware)

and tested by the Cryptographic Module Testing accredited laboratory: ***Atlan Laboratories, NVLAP LAB CODE 200492-0,*** **CRYPTIK Version 5.8**

is as follows:

Cryptographic Module Specification:	Level 2	Cryptographic Module Ports and Interfaces:	Level 2
Roles, Services, and Authentication:	Level 2	Finite State Model:	Level 2
Physical Security: *(Single Chip)*	Level 3	Cryptographic Key Management:	Level 2
EMI/EMC:	Level 3	Self Tests:	Level 2
Design Assurance:	Level 2	Mitigation of Other Attacks:	Level N/A
Operational Environment:	Level N/A	tested in the following configuration(s):	N/A

The following FIPS approved Cryptographic Algorithms are used: **DES (Cert. #88); Triple-DES (Cert. #236); DSA/SHA-1 (Cert. #35); RSA (PKCS #1, vendor affirmed)**

The Cryptographic module also contains the following non-FIPS approved algorithms: **Diffie-Hellman (key agreement)**

Overall Level Achieved: 2

Signed on behalf of the Government of the United States

Signature: ______________________________

Dated: 27 July 2004

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: ______________________________

Dated: 29 June 04

Director, Information Protection Group
The Communications Security Establishment