Cryptographic Module Validation Certificate

Certificate No. F0011

Cryptographic Module Name :	PGP Software Developer's Kit (SDK) Cryptographic Module
Version :	3.12.0
Hardware Version :	N/A
Firmware Version :	N/A
Software Version :	3.12.0
Physical Embodiment :	Multi-chip standalone
Security Requirements :	JCMVP Cryptographic Module Security Requirements (MSR-01-EN), 11 / 02 / 2009
Testing Requirements :	JCMVP Cryptographic Module Security Test Requirements (MTR-01-EN), 11 / 02 / 2009
Vendor :	PGP Corporation
Address of Vendor :	200 Jefferson Drive, Menlo Park, CA 94025 USA
Special Affairs :	None

Notes : The cryptographic module identified in this certificate has been tested at an accredited Cryptographic Module Testing Laboratory in the Japan Cryptographic Module Validation Program, and the testing results have been validated in accordance with the Cryptographic Module Testing Requirements. This certificate applies only to the specific version of the Cryptographic Module in its tested configurations and operational environments. The Cryptographic Module Tests have been conducted in accordance with the provisions of the Japan Cryptographic Module Validation Program and the conclusions of the testing laboratory in the testing report are consistent with evidence adduced. This certificate is not an endorsement of the cryptographic module by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, and no warranty of the cryptographic module by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.
The misuse of this certificate, including the use of certificate for publications, such as advertisements and catalogs, in an incorrect or misleading manner may result in withdrawal of this certificate.

Signature : Original Signed Date : March 5, 2010

Name : Koji Nishigaki

Title : Chairman

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

Cryptographic Module Validation Report

The cryptographic module identified in this report has been validated in the following.

Cryptographic Module Name : PGP Software Developer's Kit (SDK) Cryptographic Module

Version : 3.12.0

Accredited Cryptographic Module Testing Laboratory : IT Security Center, Information-technology Promotion Agency, Japan

CRYPTIPA Version : 1.2.1

Cryptographic Module Specification :	Level 1	*Cryptographic Module Ports and Interfaces :*	Level 1
Roles, Services, and Authentication :	Level 1	*Finite State Model :*	Level 1
Physical Security :	Level N/A	*Operational Environment :*	Level 1
Cryptographic Key Management :	Level 1	*EMI/EMC :*	Level 1
Self-Tests :	Level 1	*Design Assurance :*	Level 3
Mitigation of Other Attacks :	Level N/A		

tested in the following configuration(s) : Mac OS X 10.5 Apple MacBook Pro 15";
Windows XP Professional 2002 SP-2, Dell PowerEdge 860 with Dual Core Xeon 3060 processor, 1 GB RAM, DVD-ROM, and 80GB SATA hard disk drive;
Linux, 32-bit: Fedora Core 6, Dell PowerEdge 860 with Dual Core Xeon 3060 processor, 1 GB RAM, DVD-ROM, and 80GB SATA hard disk drive

Overall Level Achieved : 1

The following Approved Cryptographic Algorithms are used : DSA (CAVP #334, #335, #336) , RSA (CAVP #459, #460, #461) ,
3-key Triple DES (CAVP #753, #754, #755), AES (CAVP #951, #954, #955),
SHS (CAVP #925, #926, #927), HMAC (CAVP #529, #531, #532), RNG (CAVP #538, #539, #540)

The cryptographic module also contains the following non approved algorithms : CAST-5, IDEA, Two-Fish, Blow-Fish, ARC4-128, AES (EME2 mode; non-compliant),
MD5, HMAC-MD5, RIPEMD-160 (non-compliant),
DSA with SHA-256 (FIPS 186-3), ElGamal, Shamir Threshold Secret Sharing,
RSA Encrypt/Decrypt, OpenPGP Message Format (IETF RFC 4880)

Test Results : Pass

The cryptographic module identified in this report has been tested on the basis of the testing requirements specified by the Japan Cryptographic Module Validation Program, and has achieved the scope of conformance to the specified security requirements from the test results.

IPA

Signature : Original Signed Date : March 5, 2010

Name : Koji Nishigaki

Title : Chairman

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN