暗号モジュール認証書

暗号モジュール試験及び認証制度に基づき、以下のとおり認証する。

原　紙
押印済

平成 22 年 3 月 5 日
独立行政法人 情報処理推進機構
理事長　西垣　浩司

認証番号 F0011

日本語名：	PGP Software Developer's Kit (SDK) Cryptographic Module
英語名：	PGP Software Developer's Kit (SDK) Cryptographic Module
ハードウェアバージョン：	N/A
ファームウェアバージョン：	N/A
ソフトウェアバージョン：	3.12.0
物理形態：	マルチチップスタンドアロン型

適合規格：	JCMVP Cryptographic Module Security Requirements (MSR-01-EN), 11/02/2009
試験要件：	JCMVP Cryptographic Module Security Test Requirements (MTR-01-EN), 11/02/2009

申請者：	PGP Corporation
所在地：	200 Jefferson Drive, Menlo Park, CA 94025 USA
特記事項：	なし

注意事項：本暗号モジュール認証書で識別される暗号モジュールは、「暗号モジュール試験及び認証制度」で承認された試験機関による、暗号モジュール試験要件に基づく暗号モジュール試験結果が、適合していることを示す。本暗号モジュール認証書は、暗号モジュール試験を受けた構成及び動作環境に関して、暗号モジュールの特定のバージョンのみに適用される。暗号モジュール試験は「暗号モジュール試験及び認証制度」の規定に従って実施され、暗号モジュール試験報告書の試験機関による結論は、暗号モジュール試験に用いた提供物件にのみ対応している。この暗号モジュール認証書は独立行政法人 情報処理推進機構による暗号モジュール製品等の保証書ではない。また、独立行政法人 情報処理推進機構は、明示、黙示を問わず、本暗号モジュールを用いた暗号モジュール製品等に関していかなる保証も行わない。なお、本認証書を、不正に使用した場合、並びに誤解を招くような方法で広告又は説明等に使用した場合には、暗号モジュール認証の取消を行うことがある。

暗号モジュール認証報告書

平成 22 年 3 月 5 日
原紙
押印済
独立行政法人 情報処理推進機構
理事長　西垣　浩司

記

暗号モジュール名：　PGP Software Developer's Kit (SDK) Cryptographic Module
バージョン：　3.12.0
暗号モジュール試験機関名：　独立行政法人 情報処理推進機構 セキュリティセンター
暗号モジュール試験報告書
作成支援ツールバージョン：　1.2.1

暗号モジュール試験の結果、上記の暗号モジュールは、以下の暗号モジュールセキュリティ要件を満足することを認証したので報告します。
平成 22 年 3 月 5 日

セキュリティセンター　情報セキュリティ認証室
技術管理者　近藤　潤一

暗号モジュールセキュリティ要件：JCMVP Cryptographic Module Security Requirements (MSR-01-EN), 11/02/2009
暗号モジュール試験要件：JCMVP Cryptographic Module Security Test Requirements (MTR-01-EN), 11/02/2009

暗号モジュールの仕様：	1	暗号モジュールのポートとインタフェース：1	
役割、サービス、及び認証：	1	有限状態モデル：	1
物理的セキュリティ：	N/A	動作環境：	1
暗号鍵管理：	1	電磁妨害/電磁両立性：	1
自己テスト：	1	設計保証：	3
その他の攻撃への対処：	N/A		

全体的なセキュリティレベル：1

暗号モジュール試験時の構成：別紙に記載の通り

暗号モジュールに搭載されている承認暗号アルゴリズム：
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)

暗号モジュールに搭載されている非承認暗号アルゴリズム：
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)

結果：合格
試験に用いた試験対象の暗号モジュールは、暗号モジュール試験及び認証制度が定める所定の基準に基づく試験の結果、所定の暗号モジュールセキュリティ要件を満たした。

以上

暗号モジュール試験時の構成：

ハードウェア環境 1	Apple MacBook Pro 15"
ソフトウェア環境 1	OS　Mac OS X 10.5
ハードウェア環境 2	Dell PowerEdge 860 with Dual Core Xeon 3060 processor, 1 GB RAM, DVD-ROM, and 80GB SATA hard disk drive
ソフトウェア環境 2	OS　Windows XP Professional 2002 SP-2
ハードウェア環境 3	Dell PowerEdge 860 with Dual Core Xeon 3060 processor, 1 GB RAM, DVD-ROM, and 80GB SATA hard disk drive
ソフトウェア環境 3	OS　Linux, 32-bit: Fedora Core 6

以上