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、下記のとおり認証する。

原　紙
押印済

平成 21 年 1 月 13 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 J0007

日本語名：Keymate/Crypto JCMVP ライブラリ
(Solaris 版及びWindows 版)

英語名：

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：　04-00
物理形態：　マルチチップスタンドアロン型

適合規格：　JIS X 19790：2007 平成 19年 3月 20日
試験要件：　JIS X 5091：2007　平成 19年 3月 20日
JCMVP暗号アルゴリズム実装試験要件 平成 19年 10月 29日

申請者：　株式会社 日立製作所 情報・通信グループ ソフトウェア事業部
所在地：　神奈川県横浜市戸塚区戸塚町5030番地
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、不正にしようした場合、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

認証対象の暗号モジュールについて、以下の通り認証したことを報告する。

原　紙
押印済

平成 21 年 1 月 13 日
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：　Keymate/Crypto JCMVP ライブラリ(Solaris 版及びWindows 版)
バージョン：　04-00
暗号モジュール試験機関名：財団法人 日本品質保証機構 関西試験センター
暗号モジュール試験報告書
作成支援ツールバージョン：1.1.0

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：	N/A
自己テスト：	1	設計保証：	1
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：
ECDSA(#3)、RSA(#7)、AES(#9)、SHS(#9、#10)、HMAC(#7)、Hash_DRBG in NIST SP800-90(ベンダ自己確認)

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：なし

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

＜Keymate/Crypto JCMVP ライブラリ(Solaris 版及び Windows 版)
暗号モジュール認証報告書：別紙＞

暗号モジュール試験時の構成：

ハードウェア環境 1	Sun Blade 2000 (CPU: Ultra SPARC IIICu(900MHz), Memory: 1GB, HDD: 120GB)
ソフトウェア環境 1	OS　Solaris 10 5/08 (SunOS 5.10)
ハードウェア環境 2	HP Compaq dc7800p Small Form Factor (CPU: Intel Core2Duo CPU E8300 (2.83GHz), Memory: 4GB, HDD: 160GB)
ソフトウェア環境 2	OS　Windows Server 2008 Enterprise (バージョン 6.0, ビルド 6001：Service Pack 1)

以上