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。

平成25年8月22日
独立行政法人情報処理推進機構
理事長 藤江 一正

原　紙
押印済

認証番号 J0019

日本語名：

PCI-Expressバス対応型ハードウェアセキュリティモジュール

英語名：PCI-Express based Hardware Security Module

バージョン：　0.96
　ハードウェアバージョン　：1.34
　ファームウェアバージョン：MainCPU：1.28、SubCPU：1.3
　ソフトウェアバージョン　：N/A
物理形態：　マルチチップ組込型

適合規格：JIS X 19790	平成 21 年 10 月 20 日 改正
試験要件：JIS X 24759:2009	平成 21 年 10 月 20 日
JCMVP暗号アルゴリズム実装試験要件	平成 21 年 1 月 8 日

申請者：NTTエレクトロニクス株式会社
所在地：神奈川県横浜市神奈川区新浦島町1-1-32 ニューステージ横浜
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。

M201204-01

暗号モジュール認証報告書

平成 25 年 8 月 22 日
独立行政法人 情報処理推進機構
理事長　藤江 一正 原紙押印済

記

暗号モジュール名：　PCI-Expressバス対応型ハードウエアセキュリティモジュール

バージョン：　0.96
ハードウェアバージョン　：1.34
ファームウェアバージョン：MainCPU：1.28、SubCPU：1.3
ソフトウェアバージョン　：N/A

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　技術本部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：　1.2.2

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 24 年 8 月 22 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：JIS X 19790　平成 21 年 10 月 20 日 改正
暗号モジュール試験要件：　JIS X 24759:2009　平成 21 年 10 月 20 日

暗号モジュールの仕様：	3	暗号モジュールのポートとインタフェース：	3
役割、サービス、及び認証：	3	有限状態モデル：	3
物理的セキュリティ：	3	動作環境：	N/A
暗号鍵管理：	3	自己テスト：	3
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：3

暗号モジュール試験時の構成：別紙1の1.に記載のとおり

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：
RSA(#13)、3-key Triple DES(#7)、AES(#29)、SHS(#21)、HMAC(#13)、DRBG(#2)

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：別紙1の2.に記載のとおり

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

M201204-01

<PCI-Express バス対応型ハードウエアセキュリティモジュール 暗号モジュール認証報告書：別紙 1 >

1. 暗号モジュール試験時の構成：

ハードウェア環境	PRIMERGY TX140S1	S26361-K1379-V101, MAAN002119
ソフトウェア環境	Windows Server 2008 Standard	Windows Server バージョン 6.0 (ビルド 6002：Service Pack2)

2. 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：

RSASSA-PKCS1-v1_5 (PKCS#1 v2.1) (1,024bit)
RSA (No Padding) (1,024～4,096bit)
RSA-OAEP (PKCS#1 v2.1) (1,024～4,096bit)
RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (1,024bit)
RSA (No Padding) (1,024～4,096bit)
DES, 2-key Triple Des (SP800-67)暗号利用モード：ECB, CBC
Secure Hash Standard (SHA-1) (FIPS PUB 180-4)
MD5 (RFC1321)
HMAC-SHA-1 (FIPS PUB 198-1)
HMAC-MD5 (RFC2403)

以上