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。

平成 19 年 12 月 26 日
独立行政法人 情報処理推進機構
理事長 藤原 武平太

認証番号 F0004

日本語名： C-SELECT

英語名： C-SELECT

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： 1.1

物理形態： マルチチップスタンドアロン型

適合規格： JCMVP暗号モジュールセキュリティ要件 平成18年10月16日
試験要件： JCMVP暗号モジュール試験要件 平成18年10月16日
JCMVP暗号アルゴリズム試験要件 平成18年10月16日
申請者： キヤノン株式会社
所在地： 東京都大田区下丸子3丁目30番2号
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。

様式 12-2

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。

平成 19 年 12 月 16 日
独立行政法人 情報処理推進機構
理事長　　藤原　武平太

記

暗号モジュール名：	C-SELECT
バージョン：	1.1
暗号モジュール試験機関名：	株式会社電子商取引安全技術研究所 評価センター
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：
DSA(#2)、RSA (#3)、3key Triple-DES(#3)、AES(#4)、Camellia(#2)、SHS(#3)、HMAC (#3)、DH(#2)、RNG(#1)、CMAC(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：
DES、RC2、AES CCM mode、Elgamal、MD2、MD4、MD5、HMAC-MD5、DESMAC、TDES Key wrap、AES Key wrap、PRNG based on DES for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1

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

＜C-SELECT(バージョン:1.1) 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	CPU Celeron D330 2.66GHz、メモリ 768MB、HDD 40GB
ソフトウェア環境 1	OS　Microsoft Windows 2000 Professional 5.00.2195 SP4
ハードウェア環境 2	CPU Celeron D330 2.66GHz、メモリ 768MB、HDD 40GB
ソフトウェア環境 2	OS　Microsoft Windows XP Professional Version2002 SP2
ハードウェア環境 3	CPU Celeron D326 2.53GHz、メモリ 512MB、HDD 74.5GB
ソフトウェア環境 3	OS　Microsoft Windows Vista Ultimate
ハードウェア環境 4	CPU Celeron D330 2.66GHz、メモリ 768MB、HDD 40GB
ソフトウェア環境 4	OS　Linux Version 2.6.22.9-61.fc6 (Fedora Core 6)
ハードウェア環境 5	CPU Xeon 3.40GHz、メモリ 512MB、HDD 36.7GB
ソフトウェア環境 5	OS　Microsoft Windows XP Professional x64 Edition Version2002 SP2
ハードウェア環境 6	CPU Xeon 3.40GHz、メモリ 2048MB、HDD 80GB
ソフトウェア環境 6	OS　Microsoft Windows Vista Ultimate
ハードウェア環境 7	CPU Xeon 3.40GHz、メモリ 2048MB、HDD 80GB
ソフトウェア環境 7	OS　Linux Version 2.6.22.9-61.fc6 (Fedora Core 6)
ハードウェア環境 8	CPU Core Duo 1.83GHz、メモリ 2GB、HDD 80GB
ソフトウェア環境 8	OS　Mac OS X v10.4.10
ハードウェア環境 9	CPU PowerPC 750 350MHz、メモリ 320MB、HDD 28GB
ソフトウェア環境 9	OS　Mac OS X v10.4.10

以上