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4月10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 F0002

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： 1.0
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三丁目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

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。

修正　平成19年4月17日
平成19年4月10日
独立行政法人 情報処理推進機構
セキュリティセンター
暗号モジュール技術管理者
近藤　潤一

記

暗号モジュール名：	C-SELECT
バージョン：	1.0
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：	1.0.3

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：

ハードウェア環境1	CPU Celeron D326 2.53GHz、メモリ 512MB、HDD 74.5GB
ソフトウェア環境1	OS　Microsoft Windows Vista Ultimate
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 Service Pack 2
ハードウェア環境3	CPU Celeron D330 2.66GHz、メモリ 768MB、HDD 40GB
ソフトウェア環境3	OS　Microsoft Windows 2000 Service Pack 4 5.00.2195
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 2.6.15-1.2054-FC5 (Fedora Core 5)

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(#1)、ECDSA(#1)、RSASSA-PKCS1-v1_5(#1)、RSA-OAEP(#1)、RSAES-PKCS1-v1_5(#1)、3key Triple-DES(#2)、AES(#2)、Camellia(#1)、SHA-1(#2)、SHA-256(#2)、 SHA-384(#2)、SHA-512(#2)、HMAC-SHA-1(#2)、HMAC-SHA-256(#2)、HMAC-SHA-384(#2)、HMAC-SHA-512(#2)、DH(#1)、ECDH(#1)、PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1(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、CMAC、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