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 30 年 6 月 20 日
（初回発行日：平成 19 年 3 月 30 日）
独立行政法人情報処理推進機構
理事長　富田　達夫

原　紙
押印済

認証番号 F0001

日本語名：	東芝ソリューション暗号ライブラリ
英語名：	Toshiba Solutions Cryptographic Library
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：	1.0.0.0
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：	東芝デジタルソリューションズ株式会社
所在地：	神奈川県川崎市幸区堀川町72-34
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。

【変更履歴】

平成 19 年 3 月 30 日	申請者：　東芝ソリューション株式会社 所在地：　東京都港区芝浦一丁目１番１号
平成 30 年 6 月 20 日	（再発行理由）社名及び会社所在地が変更になったため。 変更前： 申請者：　東芝ソリューション株式会社 所在地：　東京都港区芝浦一丁目１番１号 変更後： 申請者：　東芝デジタルソリューションズ株式会社 所在地：　神奈川県川崎市幸区堀川町 72-34

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3月30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

記

暗号モジュール名：	東芝ソリューション暗号ライブラリ		
バージョン：	1.0.0.0		
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	CPU	Core Duo 1.66GHz、メモリ　2GB、HDD　74.5GB
ソフトウェア環境	OS	Microsoft Windows XP SP2 Professional Edition

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：
AES（#1）、3key Triple-DES（#1）、SHA-1（#1）、SHA-256（#1）、RSASSA-PSS（#1）、HMAC-SHA-1（#1）、HMAC-SHA-256（#1）、PRNG based on SHA-1 for general purpose in FIPS 186-2 (+change notice 1) revised 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： 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