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。

原　紙
押印済

平成 25 年 7 月 8 日
独立行政法人情報処理推進機構
理事長　　藤江　一正

認証番号 F0018

日本語名：Bluefly Processor

英語名：Bluefly Processor

ハードウェアバージョン：	3.0 (Part #950 000 003 R) [1], 4.0 (Part #950 000 004 R) [2]
ファームウェアバージョン：	1.15 [1, 2], 2.0 [1], 2.1 [1, 2], 2.2 [1, 2], 2.3 [1, 2], 2.4 [1, 2]
ソフトウェアバージョン：	-
物理形態：	シングルチップ

適合規格：Federal Information Processing Standards (FIPS) PUB 140-2
Security Requirements for Cryptographic Modules
Change Notices (12-03-2002)

試験要件：Derived Test Requirements for FIPS PUB 140-2, January 04, 2011,
Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, December 21, 2012

申請者：	イメーション株式会社
所在地：	東京都渋谷区神宮前5-52-2
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

平成 25 年 7 月 8 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：Bluefly Processor
バージョン：
　ハードウェアバージョン：3.0 (Part #950 000 003 R) [1], 4.0 (Part #950 000 004 R) [2]
　ファームウェアバージョン：1.15 [1, 2], 2.0 [1], 2.1 [1, 2], 2.2 [1, 2], 2.3 [1, 2], 2.4 [1, 2]
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 25 年 7 月 8 日

技術本部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：
暗号モジュール試験要件：

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：
　テストボード：MXI Security M200 board (no enclosure)
　OS：Microsoft Windows XP、その他ソフトウェア：Device SDK from MXI Security

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(CAVP #417, #438, #462, #485, #519), RSA(CAVP #618, #646, #710, #767, #818), AES(CAVP #1119, #1292, #1333, #1334, #1452, #1574, #1661), 3-key Triple DES(CAVP #908, #932, #983, #1031, #1081), SHS(CAVP #1186, #1220, #1315, #1394, #1456), HMAC(CAVP #752, #782, #852, #921, #976), ANSI X9.31 Appendix A.2.4 Using AES(CAVP #720, #735, #795, #848, #884), DH(CAVP #6, #7, #9, #11, #12)

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：
TRNG, DSA Key Pair Generation, MD5, HMAC-MD5, RSA PKCS #1 v1.5 Encrypt / Decrypt, RSA OAEP Encrypt / Decrypt, RSA X.509 (raw) Encrypt / Decrypt

結果：　合格

以上