Hitachi Solutions

Hitachi Solutions, Ltd.

HIBUN Cryptographic Module for User-Mode

JIS X 19790 Security Policy

Level 1 Validation

Document Version 1.6

2012/3/15

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1. INTRODUCTION 4
1.1. PURPOSE 4
1.2. REFERENCES 4
1.3. PACKAGE ORGANIZATION 4
2. CRYPTOGRAPHIC MODULE SPECIFICATION 5
2.1. OVERVIEW 5
2.2. CRYPTOGRAPHIC BOUNDARY 5
2.3. BLOCK DIAGRAM 6
2.4. MODULE ORGANIZATION 7
2.5. ALGORITHMS 7
2.6. APPROVED MODE 8
3. CRYPTOGRAPHIC MODULE PORTS AND INTERFACES 9
4. ROLES, SERVICES, AND AUTHENTICATION 9
4.1. ROLES 9
4.2. SERVICES 10
4.3. AUTHENTICATION 11
5. PHYSICAL SECURITY 11
6. OPERATIONAL ENVIRONMENT 11
7. CRYPTOGRAPHIC KEY MANAGEMENT 12
7.1. RANDOM NUMBER GENERATORS 13
7.2. CSP 14
7.3. KEY ENTRY AND OUTPUT 14
7.4. KEY STORAGE 14
7.5. ZEROIZATION OF KEY MATERIAL 14
8. SELF-TESTS 14
8.1. POWER-UP SELF-TESTS 15
8.2. CONDITIONAL SELF-TESTS 15
9. DESIGN ASSURANCE 16
9.1. CONFIGURATION 16
9.2. DELIVERY 16
9.3. GUIDANCE DOCUMENTS 16

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

10. MITIGATION OF OTHER ATTACKS 17

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1. Introduction

1.1. Purpose

本文書は，日立ソリューションズで開発した HIBUN Cryptographic Module for User-Mode と呼ばれる暗号ライブラリモジュールに関するセキュリティポリシ(以下，SP と略す)であり，HIBUN Cryptographic Module for User-Mode が JIS X 19790 の Level 1 のセキュリティ要件を満たすことを示す。

1.2. References

SP タイトル	HIBUN Cryptographic Module for User-Mode JIS X 19790 Security Policy
SP バージョン	1.6
SP 発行者	株式会社日立ソリューションズ
SP 発行日	2012/3/15
暗号モジュールタイトル	HIBUN Cryptographic Module for User-Mode
暗号モジュールバージョン	1.0 Rev. 2

1.3. Package Organization

HIBUN Cryptographic Module のパッケージは、異なる 3 つのモジュール（User-Mode モジュール、Kernel-Mode モジュール、及び Pre-boot モジュール）から成る。HIBUN Cryptographic Module のパッケージ構成を以下に示す。

(1) SP
- HIBUN Cryptographic Module for User-Mode JIS X 19790 Security Policy
- HIBUN Cryptographic Module for Kernel-Mode JIS X 19790 Security Policy
- HIBUN Cryptographic Module for Pre-boot JIS X 19790 Security Policy

(2) ガイダンス文書
- HIBUN Cryptographic Module 利用ガイダンス
- HIBUN Cryptographic Module API 外部接続仕様書

(3) 暗号ライブラリモジュール
- HIBUN Cryptographic Module for User-Mode
- HIBUN Cryptographic Module for Kernel-Mode
- HIBUN Cryptographic Module for Pre-boot

セキュリティ機能を提供する実行モジュールであり，(1)(2)はこれに関して記述している。

本 SP は HIBUN Cryptographic Module for User-Mode JIS X 19790 Security Policy である。本

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

SP が対象とする暗号ライブラリモジュールは HIBUN Cryptographic Module for User-Mode である。以下，「HIBUN Cryptographic Module」という場合は，HIBUN Cryptographic Module for User-Mode を指すものとする。

2. Cryptographic Module Specification

2.1. Overview

HIBUN Cryptographic Module は一般的なコンピュータ上で動作するソフトウェアであり，JIS X 19790 の Level 1 のセキュリティ要件を満たした暗号ライブラリモジュールである。Table 1 に HIBUN Cryptographic Module が満たすセキュリティ要件のレベルを項目別に示す。

Table 1: Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

HIBUN Cryptographic Module は，JIS X 19790 の規格では multi-chip standalone module に分類され，アプリケーションに Application Programming Interface (以下，API と略す)を通じて JCMVP で承認されたセキュリティ機能のうち対称暗号，メッセージダイジェスト，メッセージ認証，乱数生成の機能を提供する。

以下，「暗号ライブラリモジュール」という場合は，HIBUN Cryptographic Module を指すものとする。

2.2. Cryptographic Boundary

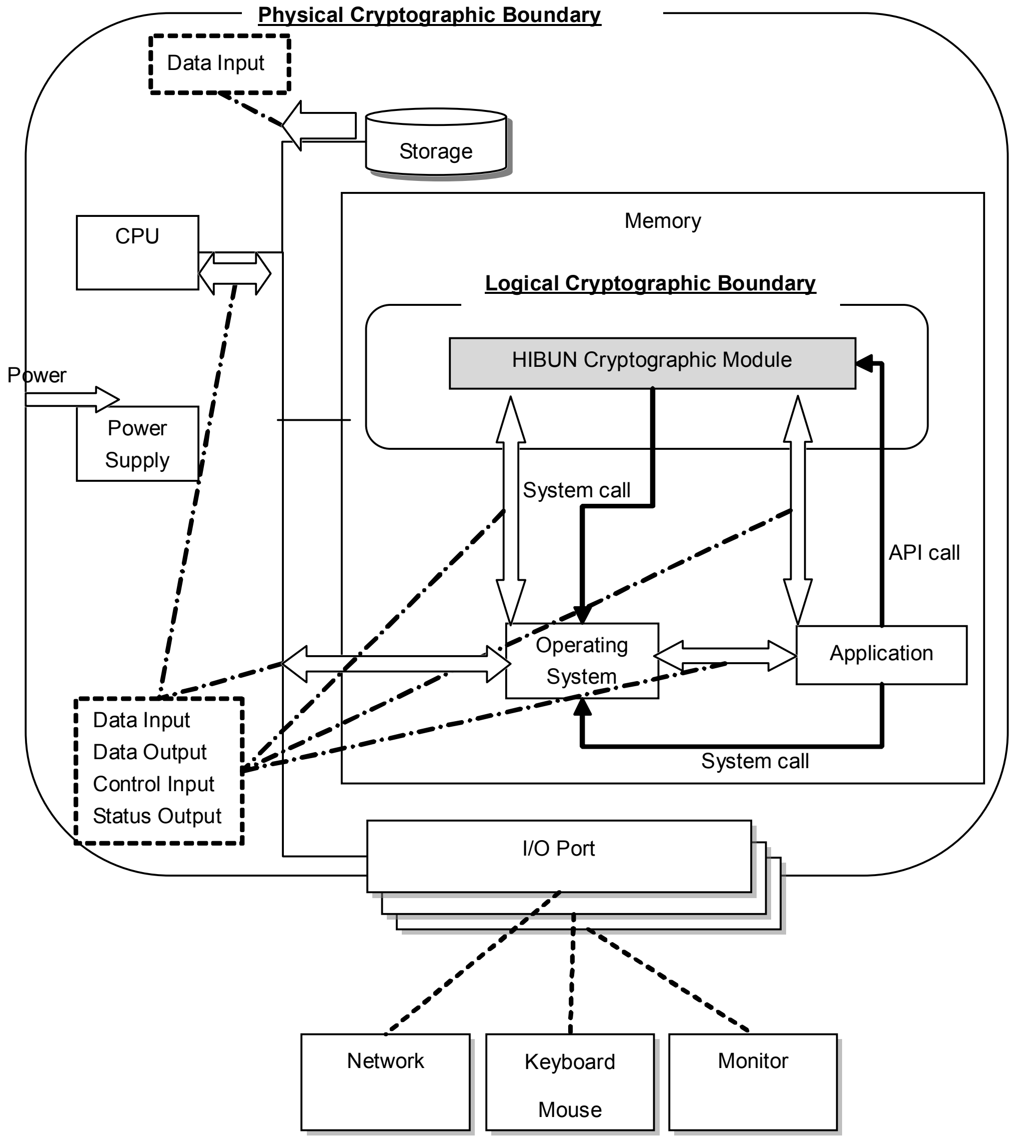
暗号ライブラリモジュールの物理的な暗号境界は，暗号ライブラリモジュールが動作するコンピュータ全体の境界である。

暗号ライブラリモジュールの論理的な暗号境界は，暗号ライブラリモジュールの機能全体の境界である。

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.3. Block Diagram

暗号ライブラリモジュールのブロック図を Figure 1 に示す。Figure 1 では, 暗号境界の他, 入出力ポートも示す。



The cryptographic library module does not input data from Operating System or output data to Operating System.

I/O ports include followings:

- Input physical ports: keyboard port, mouse port, network port
- Output physical ports: monitor port, network port

Figure 1: Block Diagram of the Cryptographic Boundary

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.4. Module Organization

暗号ライブラリモジュールのモジュール構成を Figure 2 に示す。暗号ライブラリモジュールは，Figure 2 の通り，Microsoft[1] Windows[2]オペレーティングシステム（以下，OS と略す）の 32 ビットユーザモード，64 ビットユーザモード，Linux[3] OS の 32 ビットユーザモードの環境で動作するアプリケーションにセキュリティ機能を提供する。Figure 2 では暗号ライブラリモジュールとアプリケーションの呼び出し関係を矢印で示している。

また，上記すべての暗号ライブラリモジュールに，Table 1 で示したすべてのセキュリティ要件が適用される。

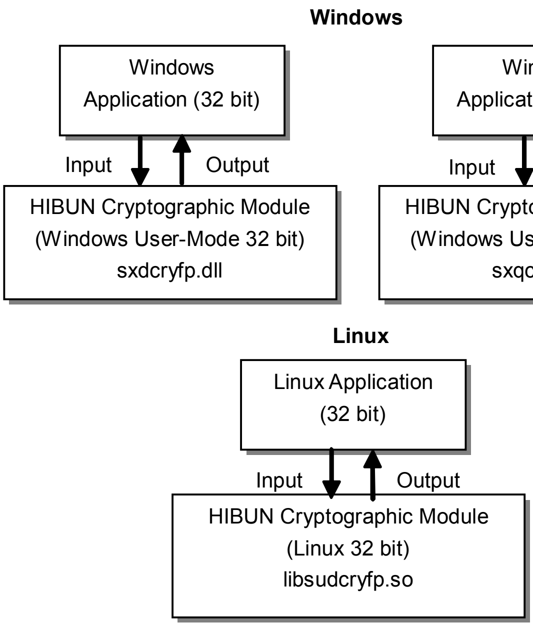


Figure 2: Relations between the HIBUN Cryptographic Module and OS

2.5. Algorithms

暗号ライブラリモジュールは，JCMVP で承認されたセキュリティ機能のうち対称暗号，メッセージダイジェスト，メッセージ認証，乱数生成の機能を有する。暗号ライブラリモジュールが実装する JCMVP で承認されたセキュリティ機能一覧を Table 2 に示す。

[1] Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
[2] Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
[3] Linux は，Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 2: Approved Algorithms

Type	Algorithm	Mode	JCMVP Approved	Publication	Algorithm Certificate Number
Symmetric Cipher	AES Encrypt/Decrypt (128 bit)	ECB, CBC, CFB 8 bit, CFB 128 bit, OFB	Yes	FIPS 197	22
	AES Encrypt/Decrypt (192 bit)	ECB, CBC, CFB 8 bit, CFB 128 bit, OFB	Yes	FIPS 197	
	AES Encrypt/Decrypt (256 bit)	ECB, CBC, CFB 8 bit, CFB 128 bit, OFB	Yes	FIPS 197	
Message Digest	SHA-224	N/A	Yes	FIPS 180-3	16
	SHA-256	N/A	Yes	FIPS 180-3	
	SHA-384	N/A	Yes	FIPS 180-3	
	SHA-512	N/A	Yes	FIPS 180-3	
Message Authentication	HMAC-SHA224	N/A	Yes	FIPS 198	9
	HMAC-SHA256	N/A	Yes	FIPS 198	
	HMAC-SHA384	N/A	Yes	FIPS 198	
	HMAC-SHA512	N/A	Yes	FIPS 198	
Deterministic Random Bit Generation	HMAC_DRBG	N/A	Yes	SP 800-90	Vendor affirmed

2.6. Approved Mode

暗号ライブラリモジュールは，JCMVP で承認されたセキュリティ機能のみを有する。Windows 用暗号ライブラリモジュールは，LoadLibrary 関数を呼び出すことによって承認された動作モードで動作する。Linux 用暗号ライブラリモジュールは，Load_Module サービスを呼び出すことによって承認された動作モードで動作する。

Windows 用暗号ライブラリモジュールでは，暗号ライブラリモジュールをメモリからアンロードするまでの間に一度だけ Load_Module サービスを呼び出すようにアプリケーションを設計しなければならない。暗号ライブラリモジュールをメモリからアンロードせずに Load_Module サービスを再度呼び出すようにアプリケーションが設計されている場合、その暗号ライブラリモジュールは認証モジュールとはみなされない。Linux 用暗号ライブラリモジュールでは, Unload_Module を呼び出すまでの間に一度だけ Load_Module サービスを呼び

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

出すようにアプリケーションを設計しなければならない。Unload_Module を呼び出さずに Load_Module サービスを再度呼び出すようにアプリケーションが設計されている場合、その暗号ライブラリモジュールは認証モジュールとはみなされない。

3. Cryptographic Module Ports and Interfaces

暗号ライブラリモジュールは，API を通じて論理的なインターフェースを提供する。JIS X 19790 の論理的なインターフェース，物理的ポートおよび暗号ライブラリモジュールによって提供される API の対応を Table 3 に示す。

Table 3: Interfaces

JIS X 19790 Logical Interfaces	Physical ports	Module Mapping
Data Input Interface	Keyboard port, mouse port, network port, etc.	Parameters passed to the module via the API
Data Output Interface	Monitor port, network port, etc.	Data returned by the module via the API
Control Input Interface	Keyboard port, mouse port, network port, etc.	Control input through the API and the API function calls
Status Output Interface	Monitor port, network port, etc.	Information returned via the API

4. Roles, Services, and Authentication

4.1. Roles

暗号ライブラリモジュールでは，クリプトオフィサ役割とユーザ役割がサポートされる。

クリプトオフィサ役割は，暗号ライブラリモジュールをインストールする際に担う役割である。ユーザ役割は，クリプトオフィサが導入した暗号ライブラリモジュールを使用する際に担う役割である。

各役割の内容を Table 4 に示す。

Table 4: Roles

Role	Description
Crypto Officer (CO)	The administrator who installs or uninstalls the module (CO can use the same services as the user role) - The crypto officer role is implicitly assumed when the application requests installation or uninstallation of the module.
User	General user who uses the module

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

	- The user role is implicitly assumed when the application requests services implemented by the module.

4.2. Services

暗号ライブラリモジュールで提供するサービスを Table 5 に示す。

Table 5: Services Provided by the Cryptographic Library Module

Type	Algorithm	Description	Service		Exported to
			Name	Description	Windows 32/64-bit User Mode and Linux 32 bit
Symmetric Cipher	AES	Encrypt/ decrypt data using AES algorithm	aes_create	Create AES instance	CO/User
			aes_init	Initialize AES instance	CO/User
			aes_encrypt_term	Complete AES encryption	CO/User
			aes_decrypt_term	Complete AES decryption	CO/User
			aes_mode	Set AES mode	CO/User
			aes_encrypt	AES data encryption	CO/User
			aes_decrypt	AES data decryption	CO/User
			aes_destroy	Destroy AES instance	CO/User
Message Digest	SHA-2	Generate message digests	shs_init	Create SHA instance	CO/User
			shs_term	Destroy SHA instance	CO/User
			shs_update	Get hash	CO/User
Message	HMAC	Generate	hmac_init	Create HMAC	CO/User

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Authentication		MAC values		instance	
			hmac_term	Destroy HMAC instance	CO/User
			hmac_ update	Get HMAC value	CO/User
Deterministic Random Bit Generation	DRBG	Generate random numbers	drbg_init	Create DRBG instance	CO/User
			drbg_term	Destroy DRBG instance	CO/User
			drbg_reseed	Reseed DRBG	CO/User
			drbg_ generate	Get random bit	CO/User
Show Status	-	Get result of status	Get_Status	Get status	CO/User
Load Module	-	Load module	Load_ Module	Create module instance	CO/User
Unload Module	-	Unload module	Unload_ Module	Change to unload status	CO/User

4.3. Authentication

暗号ライブラリモジュールは，CO および，User の認証のメカニズムを提供しない。JIS X 19790 の Level 1 のセキュリティ要件では，CO および，User の認証のメカニズムは要求されない。

5. Physical Security

暗号ライブラリモジュールは，コンピュータで動作するソフトウェアであり，物理的セキュリティは暗号ライブラリモジュールが動作するコンピュータに依存している。従って，暗号ライブラリモジュールの物理的セキュリティ要件は，適用対象外である。

6. Operational Environment

暗号ライブラリモジュールは，以下の動作環境で試験を実施し，JIS X 19790 の Level 1 のセキュリティ要件を満たしていることを確認している。

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

PC：HP[4] Compaq 8100 Elite CMT Business PC

CPU：インテル Core[5] i5-650 プロセッサ (3.2 GHz)

メモリ：2GB

OS：

・ Windows XP Professional Service Pack 3 32 bit
・ Windows Vista[6] Ultimate Service Pack 2 32 bit
・ Windows 7 Ultimate 32 bit
・ Windows 7 Ultimate 64 bit
・ Linux Kernel 2.6 32 bit

暗号ライブラリモジュールは，上記に加えて以下の動作環境もサポートする。（暗号ライブラリモジュールは、以下の動作環境を使用しての FIPS 140-2 レベル 1 のセキュリティ要件の試験又は認証を受けていない。しかし、FIPS 140-2 implementation guidance の G.5 によって、モジュールをこれらの動作環境で使用することが許可されており、認証は維持される。）

・ Windows Server[7] 2003 32 bit
・ Windows Server 2003 64 bit
・ Windows Server 2008 32 bit
・ Windows Server 2008 64 bit
・ Windows Server 2008 R2

暗号ライブラリモジュールは単一オペレータ動作モードの制限下で動作させる。暗号ライブラリモジュールを利用するアプリケーションが複数のクライアントに対応していても，暗号ライブラリモジュールにとってはアプリケーションが単一のユーザとなる。
本暗号モジュールをマルチスレッドで使用する場合，暗号モジュールのオブジェクトは一つだけ生成すること。

7. Cryptographic Key Management

Table 6 に暗号ライブラリモジュールで扱うクリティカルセキュリティパラメータ（以下，CSP と略す）を暗号アルゴリズムごとに示す。Table 6 の Input or Generate は CSP が暗号ライブラリモジュールに入力されるか暗号ライブラリモジュールで生成されるかを示す。Access Type は暗号ライブラリモジュールが CSP にどのようにアクセスするかを示す。

---

4 HP は，Hewlett-Packard Company の会社名です。
5 インテルおよび Intel Core は，米国およびその他の国における Intel Corporation の商標です。
6 Windows Vista は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
7 Windows Server は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 6: CSP

Type	Algorithm	Service	CSP	Input or Generate	Access Type
Symmetric Cipher	AES	aes_create	Secret Key	Input	Read
		aes_init	N/A	N/A	N/A
		aes_encrypt_term	Secret Key	Input	Read
		aes_decrypt_term	Secret Key	Input	Read
		aes_mode	N/A	N/A	N/A
		aes_encrypt	Secret Key	Input	Read
		aes_decrypt	Secret Key	Input	Read
		aes_destroy	Secret Key	Input	Write
Message Digest	SHA-2	shs_init	N/A	N/A	N/A
		shs_term	N/A	N/A	N/A
		shs_update	N/A	N/A	N/A
Message Authentication	HMAC	hmac_init	Secret Key	Input	Read
		hmac_term	Secret Key	Input	Read/Write
		hmac_update	Secret Key	Input	Read
Deterministic Random Bit Generation	DRBG	drbg_init	Internal State	Generate	Read/Write
			Entropy Input	Generate	Read/Write
			Nonce	Generate	Read/Write
		drbg_term	Internal State	Input	Write
		drbg_reseed	Internal State	Generate	Read/Write
			Entropy Input	Generate	Read/Write
		drbg_generate	Internal State	Generate	Read/Write
			Entropy Input	Generate	Read/Write
Show Status	-	Get_Status	N/A	N/A	N/A
Load Module	-	Load_Module	N/A	N/A	N/A
Unload Module	-	Unload_Module	N/A	N/A	N/A

7.1. Random Number Generators

暗号ライブラリモジュールでは，SP 800-90 で規定されている HMAC-DRBG を使用して

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

乱数生成を行う。

7.2. CSP

暗号ライブラリモジュールで管理している CSP を、Table 6 に示す。

7.3. Key Entry and Output

暗号鍵は，暗号ライブラリモジュールの論理的な暗号境界の外であるアプリケーションから，論理的なインターフェースである API を通じて暗号ライブラリモジュールに渡される。なお，暗号ライブラリモジュールは，暗号鍵およびシードをアプリケーションに渡さない。

7.4. Key Storage

暗号ライブラリモジュールは鍵格納を行わない。

7.5. Zeroization of Key Material

暗号ライブラリモジュールでは，CSP が使用されなくなった段階で，CSP をゼロ化する。暗号ライブラリモジュールが CSP をゼロ化するタイミングを下記に示す。

- aes_destroy 実行時（暗号鍵）
- hmac_term 実行時（暗号鍵）
- drbg_init 実行時（エントロピーインプット，ナンス）
- drbg_reseed 実行時（エントロピーインプット）
- drbg_term 実行時（内部状態）
- 暗号ライブラリモジュールで内部エラーが発生したとき（暗号鍵，DRBG の内部状態）

8. Self-Tests

暗号ライブラリモジュールは，JIS X 19790 の要件であるパワーアップ自己テストと条件自己テストの機能を有する。暗号ライブラリモジュールの自己テストで実施するテストを Table 7 に示す。

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 7: Self-Tests

Type	Algorithm	Test method	Power-Up Self-Tests	Conditional Self-Tests
Algorithm Testing	AES	Known Answer Test	Yes	N/A
	SHA-2	Known Answer Test	Yes	N/A
	HMAC	Known Answer Test	Yes	N/A
	DRBG	Known Answer Test	Yes	N/A
Integrity Testing	HMAC-SHA256	Known Answer Test	Yes	N/A
SP 800-90 Testing	DRBG	SP 800-90 Health Testing	Yes	Yes
		Entropy Test	Yes	N/A
RBG Testing	DRBG	Continuous RBG Test	N/A	Yes

Note: Algorithm Testing の SHA-2 と HMAC は DRBG の Algorithm Testing の一部として行う。
Note: SP 800-90 Health Testing における Known Answer Test については、SP 800-90 の 11.3.1 に規定されている。

8.1. Power-Up Self-Tests

パワーアップ自己テストは，暗号ライブラリモジュールがロードされたときに自動的に実行される。オンデマンドでパワーアップ自己テストを行うには，暗号ライブラリモジュールをアンロードしてロードするという操作を行う。

パワーアップ自己テストの結果は，状態出力インターフェースから出力できる。完全性テストを含めたパワーアップ自己テストの失敗時、状態出力インタフェース（Get_Status()）はパワーアップエラーの状態を返す。SXDCRYFP_STATUS_POWERUPERROR がそのインジケータである。

パワーアップ自己テストの失敗時，暗号ライブラリモジュールはエラー状態となり，Get_Status()，Load_Module()，Unload_Module()の API 以外は使用不可となる。Windows 用暗号ライブラリモジュールでは，エラー状態からの回復は，暗号ライブラリモジュールをメモリからアンロードし，再度暗号ライブラリモジュールをロードする必要がある。Linux 用暗号ライブラリモジュールでは，エラー状態からの回復は，Unload_Module サービスを実行し，再度暗号ライブラリモジュールの Load_Module サービスを実行する必要がある。

8.2. Conditional Self-Tests

条件自己テストは，Table 7 の SP 800-90 Health Testing と Continuous RBG Test を行う。SP 800-90 Health Testing については SP 800-90 の Health Testing に従い，パワーアップ時，およびリシード時（drbg_reseed()）に実行される。Continuous RBG Test については，乱数生成時（drbg_generate()）に実行される。

条件自己テストの結果は，状態出力インターフェースから出力できる。条件自己テスト

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

の失敗時、状態出力インタフェース（Get_Status()）は条件エラーの状態を返す。SXDCRYFP_STATUS_CONDITIONALERROR がそのインジケータである。

条件自己テストの失敗時，暗号ライブラリモジュールはエラー状態となり，Get_Status(), Load_Module()，Unload_Module()以外の API は使用不可となる。Windows 用暗号ライブラリモジュールでは，エラー状態からの回復は，暗号ライブラリモジュールをメモリからアンロードし，再度暗号ライブラリモジュールをロードする必要がある。Linux 用暗号ライブラリモジュールでは，エラー状態からの回復は，Unload_Module サービスを実行し，再度暗号ライブラリモジュールの Load_Module サービスを実行する必要がある。

9. Design Assurance

9.1. Configuration

暗号ライブラリモジュールの設計および開発に関係する要素は，以下で構成される。

- ソースコード
- 暗号ライブラリモジュール
- SP
- ガイダンス文書
- その他設計文書

上記に示す要素は Microsoft 社製のバージョン管理ソフト Microsoft Visual SourceSafe[8]（以下，VSS と略す）により管理されている。VSS に格納された各要素は，バージョンごとに一意的に識別できる情報がつけられて管理される。VSS に格納された各要素は，限定された開発者のみに修正を許可するようなアクセス制御を行っている。

9.2. Delivery

暗号ライブラリモジュールとガイダンス文書は，CD-ROM によって開発者へ配布する。SP については，CD-ROM による配布の他，JIS X 19790 の Level 1 の認証を取得した SP を認証機関の認証製品リスト(Web)でも公開する。

9.3. Guidance Documents

「HIBUN Cryptographic Module 利用ガイダンス」の「クリプトオフィサガイダンス」にて暗号ライブラリモジュールの入手方法，完全性確認方法，インストール方法について説明し，「HIBUN Cryptographic Module 利用ガイダンス」の「ユーザガイダンス」と「HIBUN Cryptographic Module API 外部接続仕様書」にて暗号ライブラリモジュールが提供するサービスの使用方法を説明している。

---

[8] Visual SourceSafe は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

10. Mitigation of Other Attacks

暗号ライブラリモジュールは，その他の攻撃への対処は含まない。

All Rights Reserved. Copyright © 2012, Hitachi Solutions, Ltd.
This document may be freely reproduced and distributed whole and intact including this copyright notice.