Hitachi Solutions

Hitachi Solutions, Ltd.

HIBUN Cryptographic Module for User-Mode

FIPS 140-2 Security Policy

Level 1 Validation

Document Version 1.7

02/14/2012

1. Introduction

1.1. Purpose

This document provides the cryptographic library module security policy (SP) for the HIBUN Cryptographic Module for User-Mode from Hitachi Solutions, Ltd. This document describes how the HIBUN Cryptographic Module for User-Mode meets the level 1 security requirements of FIPS 140-2.

1.2. References

SP Title:	HIBUN Cryptographic Module for User-Mode FIPS 140-2 Security Policy
SP Version:	1.7
SP Publisher:	Hitachi Solutions, Ltd.
SP Published date:	02/14/2012
Cryptographic library module title:	HIBUN Cryptographic Module for User-Mode
Cryptographic library module version:	1.0 Rev. 2

1.3. Package Organization

The HIBUN Cryptographic Module package is comprised of three distinct modules (User-Mode module, Kernel-Mode module, and Pre-boot module). The HIBUN Cryptographic Module package includes the following:

(1) SP
- HIBUN Cryptographic Module for User-Mode FIPS 140-2 Security Policy
- HIBUN Cryptographic Module for Kernel-Mode FIPS 140-2 Security Policy
- HIBUN Cryptographic Module for Pre-boot FIPS 140-2 Security Policy

(2) Guidance documents
- HIBUN Cryptographic Module Guidance
- HIBUN Cryptographic Module API specification

(3) Cryptographic library module
- HIBUN Cryptographic Module for User-Mode
- HIBUN Cryptographic Module for Kernel-Mode
- HIBUN Cryptographic Module for Pre-boot

The executable modules that provide security functions. The document (1) and (2) describes these modules.

This document is HIBUN Cryptographic Module for User-Mode FIPS 140-2 Security Policy. The

cryptographic library module that this SP describes is HIBUN Cryptographic Module for User-Mode. For the purposes of this document, “HIBUN Cryptographic Module” is referred to as “HIBUN Cryptographic Module for User-Mode”.

2. Cryptographic Module Specification

2.1. Overview

The HIBUN Cryptographic Module is a software module which resides on a general purpose computer, and is a cryptographic library module which meets the level 1 security requirements of FIPS 140-2. The HIBUN Cryptographic Module meets each of the security requirements as shown in the Table 1.

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
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

HIBUN Cryptographic Module is classified as a multi-chip standalone module, and provides symmetric key cipher, message digest, message authentication, and pseudo-random number generation of the security functions approved by FIPS 140-2. The security functions are provided via the Application Programming Interface (API) to applications.

For the purposes of this document, “cryptographic library module” is referred to as “HIBUN Cryptographic Module”.

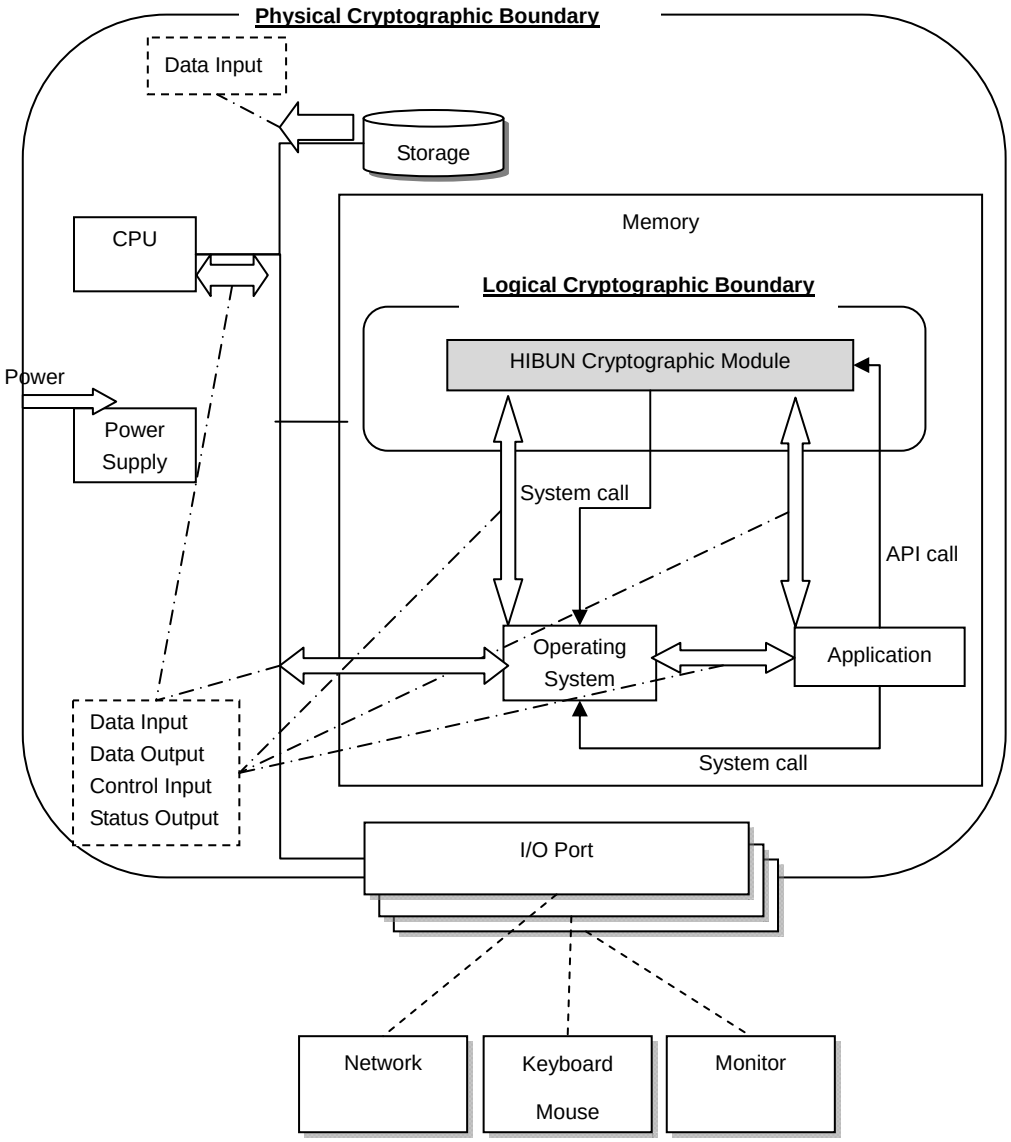
2.2. Cryptographic Boundary

The physical cryptographic boundary for the cryptographic library module is defined as the enclosure of the computer on which the cryptographic library module runs.

The logical cryptographic boundary for the cryptographic library module is defined as the whole cryptographic library module functions.

2.3. Block Diagram

A block diagram of the cryptographic library module is shown in Figure 1. Figure 1 shows the cryptographic boundaries and I/O ports.



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

2.4. Module Organization

Figure 2 shows the module organization of the cryptographic library module. The cryptographic library module provides security functions to applications running on Microsoft [1] Windows [2]

[1] Microsoft is a registered trademark of Microsoft Corp. in the U.S. and other countries.

[2] Windows is a registered trademark of Microsoft Corp. in the U.S. and other countries.

operating system (OS) 32-bit user mode/64-bit user mode, and Linux[3] OS 32-bit user mode as in Figure 2. In Figure 2, each arrow indicates the relationship between the cryptographic library module and calling applications.

All the security requirements in Table 1 are applied to all the cryptographic library modules above.

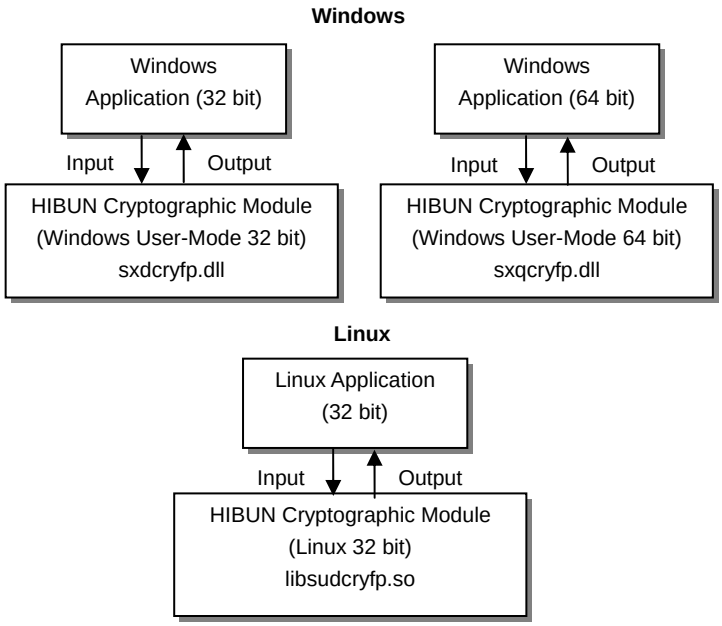


Figure 2: Relations between the HIBUN Cryptographic Module and OS

2.5. Algorithms

The cryptographic library module provides symmetric key cipher, message digest, message authentication, and pseudo-random number generation of the security functions approved by FIPS 140-2. Table 2 shows the FIPS 140-2 approved security functions provided by the cryptographic library module.

Table 2: Approved Algorithms

Service	Algorithm	Mode	FIPS140-2 Approved	Publication	Algorithm Certificate Number
Symmetric Cipher	AES Encrypt/Decrypt (128 bit)	ECB, CBC, CFB 8 bit, CFB 128 bit, OFB	Yes	FIPS 197	1780

[3] Linux is a registered trademark of Linus Torvalds.

	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	1562
	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	1045
	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	125

2.6. Approved Mode

The cryptographic library module implements only FIPS 140-2 approved security functions. The cryptographic library module for Windows runs in a FIPS 140-2 approved mode by calling LoadLibrary. The cryptographic library module for Linux runs in a FIPS 140-2 approved mode by calling Load_Module service.

If the cryptographic library module is running on Windows, the calling application must be designed to call Load_Module service only once before unloading the cryptographic library module from memory. If the calling application is designed to call Load_Module service before unloading the cryptographic library module from memory, the cryptographic library module is assumed not to be a validated module. If the cryptographic library module is running on Linux, the calling application must be designed to call Load_Module service only once before calling Unload_Module. If the calling application is designed to call Load_Module service before calling Unload_Module, the cryptographic library module is assumed not to be a validated module.

3. Cryptographic Module Ports and Interfaces

The cryptographic library module provides logical interfaces via APIs. Table 3 shows the mapping

of the FIPS 140-2 logical interfaces, physical ports, and APIs provided by the cryptographic library module.

Table 3: Interfaces

FIPS140-2 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

The cryptographic library module supports crypto officer role and user role.

In the crypto officer role, the crypto officer can install the cryptographic library module. In the user role, the user can use the cryptographic library module installed by crypto officer.

Table 4 shows description of each role.

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

4.2. Services

The cryptographic library module provides the services shown in Table 5.

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 Authentication	HMAC	Generate MAC values	hmac_init	Create HMAC instance	CO/User

			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

The cryptographic library module does not support any authentication for CO or user. The level 1 security requirements of FIPS 140-2 do not require any authentication mechanism for CO or user.

5. Physical Security

Since the cryptographic library module is one of the software modules residing on a general purpose computer, the physical security shall be provided by the computer the cryptographic library module is running on. Therefore the physical security requirement of the cryptographic library module is not applicable.

6. Operational Environment

The cryptographic library module is tested and validated to the level 1 security requirements of

FIPS 140-2 using following operational environments:

- Windows XP Professional
- Windows Vista[4] Ultimate
- Windows 7 Ultimate
- Windows 7 Ultimate 64 bit
- Linux Kernel 2.6 (Fedora 12)

The cryptographic library module also supports following operational environments (The cryptographic library module is not tested or validated to the level 1 security requirements of FIPS 140-2 using following operational environments. But according to FIPS 140-2 implementation guidance G.5, the module is allowed to be ported to these operational environments and the validation is maintained):

- Windows XP 32 bit
- Windows Vista 32 bit
- Windows 7 32 bit
- Windows 7 64 bit
- Windows Server[5] 2003 32 bit
- Windows Server 2003 64 bit
- Windows Server 2008 32 bit
- Windows Server 2008 64 bit
- Windows Server 2008 R2
- Linux Kernel 2.6 32 bit

The operating system is restricted to a single operator mode of operation. The application that makes calls to the cryptographic library module is the single user of the cryptographic library module, even when the application is serving multiple clients.
When the cryptographic library module is used with multithreaded applications, the object of the cryptographic library module should be created once.

7. Cryptographic Key Management

Table 6 shows the critical security parameters (CSPs) in each algorithm used by the cryptographic library module. The “Input or Generate” column specifies whether the CSP is provided to the

[4] Windows Vista is a registered trademark of Microsoft Corporation in the United States and/or other countries.
[5] Windows Server is a registered trademark of Microsoft Corporation in the United States and/or other countries.

cryptographic library module or the cryptographic library module generates the CSP. The “Access Type” column specifies how the cryptographic library module accesses the CSP.

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

The cryptographic library module generates pseudo-random numbers as specified in HMAC-DRBG in the SP 800-90.

7.2. CSP

The CSP which cryptographic library module manages is shown in the Table 6.

7.3. Key Entry and Output

Cryptographic keys are passed to the cryptographic library module via the APIs (logical interfaces) from a calling application, which is outside of the logical boundary of cryptographic library module. The cryptographic library module passes neither cryptographic keys nor seeds.

7.4. Key Storage

The cryptographic library module stores no keys.

7.5. Zeroization of Key Material

The cryptographic library module performs zeroization of the CSP when the CSP is no longer used. The cryptographic library module zeroizes the CSP at:

- aes_destroy performed (Encryption key)
- hmac_term performed (Encryption key)
- drbg_init performed (Entropy input and nonce)
- drbg_reseed performed (Entropy input)
- drbg_term performed (Internal state)
- An internal error in the cryptographic library module (Encryption key, Internal state of DRBG)

8. Self-Tests

The cryptographic library module implements both power-up self-tests and conditional self-tests as required by FIPS140-2. Table 7 shows the tests that the cryptographic library module performs.

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: The Algorithm Testing of SHA-2 and HMAC are tested as a part of the Algorithm Testing of DRBG.

Note: Known Answer Test in Health Testing is specified in Section 11.3.1 of the SP 800-90.

8.1. Power-Up Self-Tests

Power-up self-tests are performed automatically when the cryptographic library module is loaded. To perform power-up self tests on demand, unload and load again the cryptographic library module. The result of the power-up self-tests is output via the status output interface. If the power-up self-tests, including integrity testing, failed, the status output interface (Get_Status()) returns state of power-up error. The indicator is SXDCRYFP_STATUS_POWERUPERROR.

When the power-up self-tests fail, the cryptographic library module enters an error state where no API calls are permitted except the following: Get_Status(), Load_Module(), Unload_Module(). If the cryptographic library module is running on Windows, to recover the cryptographic library module from the error state, it is required to unload the cryptographic library module from memory and load the cryptographic library module into memory again. If the cryptographic library module is running on Linux, to recover the cryptographic library module from the error state, it is required to perform Unload_module service and Load_Module service again.

8.2. Conditional Self-Tests

The cryptographic library module performs SP 800-90 Health Testing and Continuous RBG Test in Table 7 as conditional self-tests. SP 800-90 Health Testing is performed when the module is powered up or reseeding is performed (drbg_reseed()) as required by the Health Testing in SP 800-90. Continuous RBG Test is performed when pseudo-random number is generated (drbg_generate()). The result of the conditional self-tests is output via the status output interface. If the conditional self-tests failed, the status output interface (Get_Status()) returns state of conditional error. The indicator is SXDCRYFP_STATUS_CONDITIONALERROR.

When the conditional self-tests fail, the cryptographic library module enters an error state where no API calls are permitted except the following: Get_Status(), Load_Module(), Unload_Module(). If the cryptographic library module is running on Windows, to recover the cryptographic library module from the error state, it is required to unload the cryptographic library module from memory

and load the cryptographic library module into memory again. If the cryptographic library module is running on Linux, to recover the cryptographic library module from the error state, it is required to perform Unload_module service and Load_Module service again.

9. Design Assurance

9.1. Configuration

The items related to the designing and development of the cryptographic library module include the following:

- Source code
- Cryptographic library module
- SP
- Guidance documents
- Other design documents

Microsoft Visual SourceSafe[6] (VSS) is used to provide configuration management to all the items above. VSS is a version control system by Microsoft. Each version of the item in VSS database is labeled uniquely. The items in VSS database are access controlled and modification is permitted to authorized developers only.

9.2. Delivery

The cryptographic library module and the guidance documents are delivered on a CD-ROM. The SP is also available on the FIPS 140-2 Validation List web site.

9.3. Guidance Documents

The crypto officer guidance in the HIBUN Cryptographic Module Guidance describes how to obtain the module, how to verify the integrity of the module, and how to install the module. The user guidance in the HIBUN Cryptographic Module Guidance and the HIBUN Cryptographic Module API specification describe how to use the services provided by the cryptographic library module.

10. Mitigation of Other Attacks

The module does not contain security mechanisms to mitigate other attacks.

[6] Visual SourceSafe is a registered trademark of Microsoft Corporation in the United States and/or other countries.