HiPKI SafGuard 1200 HSM

Hardware version HSM-HW-20

Firmware version HSM-SW-20

FIPS 140-2 Non–Proprietary Security Policy

Level 3 Validation

Version 2.7

February 5, 2013

中華電信研究院
Chunghwa Telecom Laboratories

Version Control Table

Version	Date	Reason for Change	Author
1.0	March 23, 2012		Chunghwa Telecom
2.0	April 26, 2012	Update services	Chunghwa Telecom
2.1	May 2, 2012	Update algorithms validation numbers	Chunghwa Telecom
2.2	May 11, 2012	Amended comments from lab	Chunghwa Telecom
2.3	May 16, 2012	Amended comments from lab	Chunghwa Telecom
2.4	October 25, 2012	Amended comments from NIST	Chunghwa Telecom
2.5	November 2, 2012	Amended comments from NIST	Chunghwa Telecom
2.6	December 24, 2012	Amended comments from NIST	Chunghwa Telecom
2.7	February 5, 2013	Amended comments from NIST	Chunghwa Telecom

中華電信研究院
Chunghwa Telecom Laboratories

Table of Contents

Version Control Table i
Table of Contents ii
1. Introduction 1
Purpose 1
References 1
2. HiPKI SafGuard 1200 HSM 1
Algorithm 1
Modes Used 1
2.1 Module Ports and Interfaces 6
2.2 Roles and Services 7
2.3 Finite State Model 10
2.4 Physical Security 10
2.5 Cryptographic Key Management 11
2.6 EMI/EMC 13
2.7 Self-Tests 14
2.8 Design Assurance 15
2.9 Approved Mode of Operation 16

中華電信研究院
Chunghwa Telecom Laboratories

1. Introduction

Purpose

This is a non-proprietary security policy developed for the Chunghwa Telecom Laboratories HiPKI SafGuard 1200 HSM (hardware version HSM-HW-20 and firmware version HSM-SW-20). It describes how the HiPKI SafGuard 1200 meets the requirements for a FIPS 140-2 level 3 validation as specified in the FIPS 140-2 standard. This Security Policy is part of the evidence documentation package to be submitted to the validation lab.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2) specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections. For more information about the standard visit http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

References

This Security Policy describes how this module complies with the eleven sections of the standard. For more information on the FIPS 140-2 standard and validation program please refer to the NIST website at http://csrc.nist.gov/groups/STM/cmvp/index.html

For more information about Chunghwa Telecom Laboratories please visit http://www.chttl.com.tw.

2. HiPKI SafGuard 1200 HSM

The Chunghwa Telecom Laboratories HiPKI SafGuard 1200 HSM is a hardware security module used in a PKI system. The hardware security module (HSM) provides rapid cryptographic functionality to the operators of the system. Crypto Officers(COs) and Users are authenticated using a smart card and PIN. The smart card reader is located within the boundary of the module. The boundary of the HiPKI SafGuard 1200 HSM is the physical hardware box itself. All cryptographic module components are included inside this boundary.

The Approved cryptographic functions supported are as follows:

Algorithm	Modes Used	Certificate Number
RSA	FIPS 186-2:	#1039

	Key(gen)(MOD: 1024 , 2048 PubKey Values: 65537) ALG[RSASSAPKCS1_V1_5]; SIG(gen); SIG(ver); 1024 , 2048 , SHS: SHA-1 , SHA-224 , SHA-256 , SHA-384 SHA-512 FIPS 186-3: Key(gen)(MOD: 1024 , 2048 PubKey Values: 65537) ALG[RSASSAPKCS1_V1_5]; SIG(gen); SIG(ver); 1024 , 2048 , SHS: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512 FIPS 186-2: Key(gen)(MOD:3072 ,4096 PubKey Values: 65537) ALG[RSASSAPKCS1_V1_5]; SIG(gen); SIG(ver); 1024 , 2048 , SHS: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512 FIPS 186-3: Key(gen)(MOD:,3072 PubKey Values: 65537) ALG[RSASSAPKCS1_V1_5]; SIG(gen); SIG(ver); 3072 , SHS: SHA-256 , SHA-384 , SHA-512	#1043
ECDSA	FIPS186-2: PKG: CURVES(P-192 P-224 P-256 P-384 P-521) PKV: CURVES(P-192 P-224 P-256 P-384 P-521) SIG(gen): CURVES(P-192 P-224 P-256 P-384 P-521 SIG(ver): CURVES(P-192 P-224 P-256 P-384 P-521) FIPS186-3: PKG: CURVES(ALL-P) PKV: CURVES(ALL-P) SigGen: CURVES(P-192:	#290

	(SHA-1) P-224 (SHA-224) P-256: (SHA-256) P-384: (SHA-384) P-521: (SHA-512) SigVer: CURVES(P-192: (SHA-1) P-224 (SHA-224) P-256: (SHA-256) P-384: (SHA-384) P-521: (SHA-512)	
SHA-1,SHA-224,SHA-256,SHA-384,SHA-512	Byte – Oriented	#1760
Triple-DES 2-key, 3-key	ECB , CBC and CMAC	#1296
AES 128-bit,192-bit and 256-bit	ECB and CBC	#2010
DRBG	DRBG SP800-90 HMAC_DRBG	#187
HMAC	SHA-1,SHA-224,SHA-256,SHA-384,SHA-512	#1215

A photograph of the HiPKI SafGuard 1200 HSM which is approximately to scale, is included below.

Figure 1 - Front View of HiPKI SafGuard 1200 HSM

Figure 2 - Rear View of HiPKI SafGuard 1200 HSM

2.1 Module Ports and Interfaces

The HSM is considered to be a multi chip standalone module. The module has the following interfaces:

- **Data input:**
  - USB which connects the HiPKI SafGuard 1200 to the Host
  - Smart Card Interface
- **Data output:**
  - USB to Host, and
  - Smart Card Interface
- **Control input:**
  - USB, and
  - Keypad (front of module)
- **Status output:**
  - LCD messages (on front of module), which indicate the state of the module (ex. success or failure of self-tests, error messages)
  - LEDs (on front of module), and
  - USB message to Host.
- **Power interface:**
  - AC power source interfaces to the Adapter Tech STD-05030U Power Module

The table below describes the relationship between the interfaces.

Table 1: Mapping Physical Interfaces

Interface	Physical Interface
Data Input Interface	USB, Smart Card Interface
Data Output Interface	USB, Smart Card Interface
Control Input Interface	USB
	Front Panel Key pad
Status Output Interface	LCD
	LEDs on front of module
	USB
Power Interface	Adapter Tech STD-05030UPower Module

2.2 Roles and Services

The module supports a Crypto Officer and a User role. The HiPKI SafGuard 1200 HSM implements identity–based authentication using a combination of smart cards and PINs. Identity-based authentication occurs by entering a smart card and 8 digits PIN for each smart card. Each Crypto Officer smart card, upon successful entry of a PIN, performs a signature with a private key stored on the smart card in the HSM to authenticate to the role. The same process occurs for the User Role. The number of User Role smart cards needed to authenticate is according to the number of user to activate key in ACL.

The services available to one authenticated Crypto Officer will be able to:

- Change Crypto Officer's smart card PIN;

The services available to any two of three Crypto Officers authenticated are required:

- Generate Master key
- Export Master Key share onto smartcards
- Generate hardware RSA Key
- Create users
- Generate User private/public keys
- Generate Application Keys (AP Key)
- Set Group User
- Set AP Key ACL
- Backup AP Keys to smartcards
- Erase AP Key
- Erase Back up Smart Card
- Restore AP Keys from smartcards

- Create Crypto Officers
- Set real-time clock
- Send self test command to the module
- Switch to initialization state (zeroization)
- Write Application data
- Update Firmware

The services available to one authenticated User will be able to:

- Change User's smart card PIN;

The services available to authenticated Users in ACL are required:

- Use symmetric Application Keys(Triple-DES,AES) for data encryption and decryption
- Use asymmetric Application private keys (RSA, ECDSA) for generating signatures to sign a document or a certificate.
- Use asymmetric Application public keys (RSA,ECDSA) for verifying signatures of a document or a certificate signed by a Certificate Authority (CA)
- Get Application RSA public key
- Get Application ECDSA public key
- Get Application key status

Non-Authenticated Services

- Do Hash function
- Generate random number
- Get Application data
- View Hardware and Firmware version

The table below shows the services available to each role.

Table 2: Services Table

Crypto Officer	Authentication	Services	Access
There are up to 3 Crypto Officers. The Services and Authentication information is true for CO1, CO2 and CO3 i.e. all COs	Identity – based using RSA signature on a smart card and an 8 digit PIN.	**Single CO Services** ▪ Change smart card PIN	**r/w/x**
	Identity – based using	**Two CO authenticated**	

	a RSA signature on smart cards and a corresponding 8 digit PINs to check the possession of private key of any two of three Crypto Officers smart card and public keys store in the module.	**Services** ▪ Backup Master Key to smart cards ▪ Generate Module RSA Key ▪ Create User smart card ▪ Generate Application Keys (AP Key) ▪ Set User Group ▪ Set AP Key ACL ▪ Backup AP Keys to smart cards ▪ Erase AP Key ▪ Erase All AP key ▪ Erase Back up Smart Card ▪ Import AP Keys ▪ Create Crypto Officers (COs) ▪ Set Real Time Clock ▪ Send self-test command to module ▪ Switch to Initialization state (zeroization of module) ▪ Write Application data ▪ Update Firmware	**w/x** **w/x** **w/x** **w/x** **w/x** **w/x** **r/x** **r/w/x** **w/x** **w/x** **w/x** **w/x** **w/x** **x** **r/w/x** **w/x** **w/x**
User	**Authentication**	**Services**	**Access**
	Identity – based using a RSA signature on a smart card and an 8 digit PIN.	**Single User Services** ▪ Change smart card PIN	**r/w/x**
	Identity – based using a RSA signature on smart cards and a corresponding 8 digit PINs to check the possession of private key.	**User in ACL Authenticated Services** ▪ Use symmetric Application Keys(Triple-DES,AES) for data encryption and decryption ▪ Use asymmetric Application private keys (RSA, ECDSA) for generating signatures to sign a document or a certificate. ▪ Use asymmetric Application public keys (RSA,ECDSA) for verifying signatures of a document or a certificate signed by a Certificate Authority (CA) ▪ Get AP RSA public key ▪ Get AP ECDSA public key ▪ Get AP key status	**x** **x** **x** **r** **r** **r**
others	**Non-**	**Services**	**Access**

	Authentication		
		▪ Generate random ▪ Do Hash function ▪ Get Application data ▪ View Hardware and Firmware version	**x** **x** **r** **r**

2.3 Finite State Model

The HiPKI SafGuard 1200 HSM has been designed to meet the requirements of the FSM**.** A detailed FSM has been submitted as part of the validation process to the lab. The HiPKI SafGuard 1200 HSM consists of the following states:

- Power Off,
- Power On,
- Self Tests,
- Initialization
- Idle,
- CO,
- User, and
- Error.

2.4 Physical Security

The HiPKI SafGuard 1200 HSM is defined as a multi chip standalone module. The module consists of production grade components, which include standard passivation techniques. The HiPKI SafGuard 1200 HSM is being validated against FIPS 140-2 level 3. It has no removable covers or doors and is encased in a strong, enclosure, which is opaque in direct sun light. The HiPKI SafGuard 1200 HSM has a mechanism for tamper detection and response, which zeroizes both keys and CSPs stored internally to the module in NVRAM if an attempt is made to open the enclosure. The tamper detection and response circuit is backed up by battery housed internally in the HiPKI SafGuard 1200 HSM in case of power failure to the module. If the top casing is restored after an attempt is made to remove it, the LED lights will continue to flash and the module will be returned to the factory settings when the power is restarted.

Chunghwa Telecom Laboratories has a process for secure delivery of HSM's to the customer. The delivery of HSM's occur in a two phase process. The first is to send to the customer the smart cards and software for the host by bonded courier. The second phase is to actually deliver the HSM to the customer personally if the customer is local. If the customer is not local, then a bonded courier is used.

2.5 Cryptographic Key Management

The HiPKI SafGuard 1200 HSM in Approved mode provides cryptographic functionality using the following algorithms:

- RSA (1024, 2048,3072 and 4096 bit keys),
- ECDSA (P-192,P-224,P-256,P-384 and P-521 keys)
- SHA-1, SHA-224,SHA-256,SHA-384,SHA-512
- Triple-DES (2-key and 3-key ECB ,CBC), and
- AES (ECB and CBC 128, 192 and 256 bit keys).
- HMAC
- HMAC_DRBG

*As of January 2011 the following algorithms are restricted or deprecated: 1024-bit RSA and SHA-1. Please refer to NIST Special Publication 800-131A for more information.

To use the two-key Triple-DES algorithm to encrypt data or wrap keys in an Approved mode of operation, the module operator shall ensure that the same two-key Triple-DES key is not used for encrypting data (or wrapping keys) with more than 220 plaintext data (or plaintext keys).

Table 3: Key Management indicates the key generation method, usage and storage. All keys stored in NVRAM are zeroized if the tamper response switch is activated or if the CO returns the module to the "initialization" state as it is referred to by Chunghwa Telecom's documentation. The HiPKI SafGuard 1200 HSM returns to the same state as it was when shipped from the factory and must be reconfigured in order to continue operation. Two internal independent actions are always required to output keys or CSPs in cipher text. Keys are not output in plaintext.

Table 3: Cryptographic Keys and CSP's

Key	Generation	Storage	Use	Role
Application Keys Triple-DES, AES, RSA and ECDSA Private Keys	The HiPKI SafGuard 1200 HSM generates these internally using a DRBG compliant to NIST SP 800-90	Stored in NVRAM	Triple-DES and AES Application Keys (APK) used for data encryption and decryption. RSA and ECDSA Private keys are used for Signature	User CO

Key	Generation	Storage	Use	Role
RSA and ECDSA Public Keys			Generation to sign a document or a certificate. RSA and ECDSA Public keys are used for Signature Verification of a document or a certificate signed by a Certificate Authority (CA)	
Master Key AES 256 bit	The HiPKI SafGuard 1200 HSM generates these internally using a DRBG compliant to NIST SP 800-90	Stored in NVRAM	Used to encrypt application keys during a backup/restore operation using a "Backup smart card"	CO
Session Key Triple-DES 2-key and 3-key	Generated outside of the HiPKI SafGuard 1200.	Stored in SRAM	Triple-DES key used to authenticate the host with the HSM. Used to produce a MAC to verify originality of data from host to HSM.	CO User
Manufacturer's Key RSA 1024 bit public key	Generated outside of the HiPKI SafGuard 1200.	Stored in Serial Flash	Manufacturer's key (RSA 1024) is stored in Serial Flash To verify software integrity at startup.	User CO
Module Keys RSA 1024 bit keys (public and private key)	The HiPKI SafGuard 1200 HSM generates the key pair internally using a DRBG compliant to NIST SP 800-90.	The public key is stored in NVRAM on the module. The private key is stored in NVRAM on the module.	The public key is sent to the Host. The Host uses the Public key to wrap the session key. The private key is used to unwrap the session key that	User CO

Key	Generation	Storage	Use	Role
			was wrapped on the host.	
HMAC_DRBG internal state	Generates these internally	Stored in SRAM	Generate random number	User CO
HMAC_DRBG Entropy Input	Generates these internally	Stored in SRAM	Generate random number	User CO
HMAC_DRBG Nonce	generates these internally	Stored in SRAM	Generate random number	User CO
Crypto Officer's Public Key RSA 1024 bit key	Generated by a Smart Card outside of the cryptographic boundary.	Stored in NVRAM	Public key on unit used for authentication to the private key on Crypto Officers smart card.	CO
Users Public Key RSA 1024 bit key	Generated by a Smart Card outside of the cryptographic boundary.	Stored in NVRAM	Public key on unit used for authentication to the private key on User's Smart Card.	User
PIN's	N/A	Stored on smart card	Authentication	CO User

The hardware –based NDRNG uses Johnson noise as the physical noise source. The noise originates in a combination of resistor noise, in an external resistor, and in resistance in the input stage of the first amplifier. Johnson noise has a frequency distribution shaped according to the pass band of the amplifier; the noise is bandwidth-limited by the amplifier's bandwidth. Johnson noise is also well known to have very low amplitude. A very high gain, disturbance free, amplification is needed. The R300 use six stages of analog amplification.

More information can be obtained from: http://www.protego.se/pdf/r300a.pdf

2.6 EMI/EMC

The HiPKI SafGuard 1200 HSM complies with EMI/EMC requirements as specified by 47 Code of Federal Regulations, Part 15 Subpart B Class B (home use). The FCC number assigned to this validation is RPXTLHSM1200 and the certificate has been presented as evidence in the FIPS 140-2 validation of the Chunghwa Telecom Laboratories HiPKI SafGuard 1200 HSM.

2.7 Self-Tests

If the self-tests all pass, a status message, “Self tests OK” is displayed on the LCD. If any of the self-tests fail, the module transitions to error state and must be rebooted.

The module performs the following power-up self-tests:

- Software/Firmware integrity Test
- KAT Algorithm Test for RSA
- KAT Algorithm Test for ECDSA
- KAT for SHA-1,SHA-256,SHA-512
- Pairwise Consistency Test for RSA
- Pairwise Consistency Test for ECDSA
- KAT Algorithm Test for AES encrypt/decrypt
- KAT Algorithm Test for Triple-DES MAC
- KAT Algorithm Test for Triple-DES encrypt/decrypt
- KAT Algorithm Test for HMAC
- KAT Algorithm Test for HMAC_DRBG
- Health Test for NIST SP 800-90A HMAC_DRBG

The module performs the following conditional self-tests:

- Firmware load Test RSA digital signature verification (1024 bit key)
- Pairwise Consistency Test for RSA
- Pairwise Consistency Test for ECDSA
- CRNG Test for HMAC_DRBG
- CRNG Test for the NDRNG
- Health Tests for NIST SP 800-90A HMAC_DRBG

Cryptographic Algorithm KATs

Known Answer Tests (KATs) are run at power-up for:

- KAT Algorithm Test for RSA
- KAT Algorithm Test for ECDSA
- KAT for SHA-1,SHA-256,SHA-512
- KAT Algorithm Test for AES encrypt/decrypt
- KAT Algorithm Test for Triple-DES MAC
- KAT Algorithm Test for Triple-DES encrypt/decrypt
- KAT Algorithm Test for HMAC

- KAT Algorithm Test for HMAC_DRBG
- Health Test for NIST SP 800-90A HMAC_DRBG

Software/Firmware Integrity Test

At start up, the HiPKI SafGuard 1200 HSM firmware code is signed by an RSA private key and compared to a value stored in FLASH. The test fails if the calculated value does not equal the stored value.

RNG Test

A Known answer test for RNG at power on test and a continuous test at key generation process.

A continuous random number generator test is run as part of the self-test suite both at module startup and when generates random number. The test is as follows: The module generates a 16-byte block of data at power on and stores the data as previous_random. As part of the self-test, the module generates a 16-byte block and compares it with the previous_random block of data. The test passes if both values are different. The new random value then replaces the previous_random block of data. The module will continue to generate blocks up to 10 times to clear the error. If the two compared blocks are equal after 10 tries, the module enters the error state.

A RNG KAT test is run as part of the self-test suite at module startup. The test is use fix seed to generate random number and compared to a value stored in FLASH.

2.8 Design Assurance

The Chunghwa Telecom Inc. HiPKI SafGuard 1200 HSM satisfies the design assurance requirements as described in the FIPS 140-2 standard by the adoption and use of the following methodologies:

- Configuration Management specifications for secure design of the HiPKI SafGuard 1200 HSM,
- Secure delivery specifications for distributing the module to authorized operators,
- Secure installation, generation and start-up procedures specifications for configuring the HiPKI SafGuard 1200 HSM to run in Approved mode,
- Specification of the rules of operation for Approved mode,
- Implementation developed using commented, high level code (C-language and VHDL) Design specifications for hardware and firmware

- Crypto Officer specifications for key management, authentication procedures, port and IP address configuration and user creation,
- Specifications for secure administration of the HiPKI SafGuard 1200 HSM,
- Specifications of assumptions for Users for operation in Approved mode,
- User manual which describes roles, services, interfaces (physical and logical) and error and exception handling, and
- Specifications of User responsibilities to maintain security of operations in Approved mode of operation.

The Vendor Evidence document lists all of the specifications documentation and all evidence documentation for use in the FIPS 140-2 level 3 validation of the HiPKI SafGuard 1200 HSM.

2.9 Approved Mode of Operation

To operate the module in Approved mode the CO has to configure the module in the following manner:

- An RSA 1024 bit key is installed at manufacture. This key is used to verify firmware integrity.

- Upon receipt of the HiPKI SafGuard 1200 HSM from Chunghwa Telecom Laboratories the HiPKI SafGuard 1200 HSM is configured as documented in the *Approved Mode of Operation for Security Policy* document. This configuration is the following series of steps:
  1. Select “Initialize” from the HiPKI SafGuard 1200 host application. This synchronizes the system time on the host with the RTC on the HSM.
  2. Set the configuration of the HiPKI SafGuard 1200. This entails setting the following parameters:
     - RTC
  3. A master key (AES 256) must be generated by the HSM.
  4. The master key must then be written to the master key backup smart card in split key format.
  5. Generate an RSA Key Pair for each Crypto Officer smart card.
  6. Generate a Module Key (RSA) that is used to wrap the session key (Triple-DES) from the HSM to the Host.
  7. Generate the Application Key (Triple-DES or AES) and assign it to the CO or User group.
  8. Activate the Application Key. This requires authenticating to the HSM in the CO or user role. Input a session key (Triple-DES) wrapped with the Module Key, into the HSM.

The module is now operational in FIPS mode. This is indicated by the module's two LEDs both on and the "FIPS Mode" message on the module's LCD.

The HiPKI SafGuard 1200 HSM provides the following Approved mode algorithms for use:

- Triple-DES (2-key and 3-key ECB and CBC mode) for encryption and decryption,
- AES (ECB and CBC mode 128 ,192 and 256 bit keys) for encryption and decryption,
- RSA (1024, 2048,3072 and 4096 bit keys) for digital signatures,
- ECDSA (P-192, P-224,P-256,P-384 and P-521 keys) for digital signatures,
- Random number generator and
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512(hash for signatures).
- RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength)

When the HiPKI SafGuard 1200 HSM is operating in Approved mode, the LCD screen displays the message "FIPS mode" and the two LEDs (ST1 and ST2) on the front panel are on.