中華電信股份有限公司
Chunghwa Telecom Co., Ltd.

HiPKI SafGuard 1000 HSM

Hardware version HSM-HW-10

Firmware version HSM-SW-T8051.10

FIPS 140-2 Non–Proprietary Security Policy

Level 3 Validation

Version 1.3

October 8th, 2008

中華電信股份有限公司
Chunghwa Telecom Co., Ltd.

Version Control Table

Version	Date	Reason for Change	Author
1.0	May 1, 2008	Draft Submission to Lab	Chunghwa Telecom
1.1	June 27, 2008	Edits from Lab Comments	Chunghwa Telecom
1.2	Sept 29, 2008	Edits from Lab Comments	Chunghwa Telecom
1.3	Oct. 8, 2008	Name Change	Chunghwa Telecom

中華電信股份有限公司
Chunghwa Telecom Co., Ltd.

Table of Contents

中華電信股份有限公司
Chunghwa Telecom Co., Ltd.

1. Introduction

Purpose

This is a non-proprietary security policy for the Chunghwa Telecom Co., Ltd. Telecommunication Laboratories HiPKI SafGuard 1000 HSM (hardware version HSM-HW-10 and firmware version HSM-SW-T8051.10). Chunghwa Telecom Co., Ltd Telecommunication Laboratories is a Division of Chunghwa Telecom Co., Ltd. It describes how the HiPKI SafGuard 1000 meets the requirements for a FIPS 140-2 level 3 revalidation 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 Co., Ltd. Telecommunication Laboratories please visit http://www.chttl.com.tw/english/index.php

2. HiPKI SafGuard 1000 HSM

The Chunghwa Telecom Co., Ltd. Telecommunication Laboratories HiPKI SafGuard 1000 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[1] (COs) and Users are authenticated using a smart card and password. The smart card reader is located within the boundary of the module. The boundary of the HiPKI SafGuard 1000 HSM is the physical hardware box itself. All cryptographic module components are included inside this boundary.

[1] The documentation uses Security Officer and Crypto Officer interchangeably to discuss the Crypto Officer role.

The Approved cryptographic functions supported are as follows:

Algorithm	Modes Used	Certificate Number
RSA	ALG[ANSIX9.31]; Key(gen)(MOD: 1024 , 2048 , PubKey Values: 3 , 17 , 65537) ALG[RSASSAPKCS1_V1_5]; SIG(gen); SIG(ver); 1024 , 2048 , SHS: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512	#362
SHA-1,SHA-224,SHA-256,SHA-384,SHA-512	Byte - Oriented	#770
Triple DES, 3-key	ECB and CBC	#668
Triple DES MAC		#668 vendor affirmed
AES 128-bit,192-bit and 256-bit	ECB and CBC	#763
RNG	ANSI X9.31 Appendix A.2.4 Using the AES Algorithms	#439

A photograph of the HiPKI SafGuard 1000 HSM which is approximately to scale, is included below.

Figure 1 HiPKI SafGuard 1000 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 1000 to the Host
- **Data output:**
  - USB to Host
- **Control input:**
  - USB, and
  - Keypad (front of module)
- **Status output:**
  - LCD message (on front of module),
  - LEDs (on front of module), and
  - USB message to Host.
- **Power interface:**
  - AC power source interfaces to the Adapter Tech STD-05025U Power Module

The table below describes the relationship between the interfaces.

Table 1: Mapping Physical Interfaces

Interface	Physical Interface
Data Input Interface	USB
Data Output Interface	USB
Control Input Interface	USB
	Front Panel Key pad
Status Output Interface	LCD
	LEDs on front of module
	USB
Power Interface	Adapter Tech STD-05025U Power Module

2.2 Roles and Services

The module supports a Crypto Officer and a User role. The HiPKI SafGuard 1000 HSM implements identity–based authentication using a combination of smart cards and passwords[2]. Identity-based authentication occurs by entering a smart card and 8 digits PIN for each smart card, of at least 2 Crypto-Officers and up to a maximum of 3 Crypto Officers. 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 with a minimum of 2 User Role smart cards and up to 9 User Role smart cards needed to authenticate.

The services available to the CO are as follows:

- Change smart card PIN
- Export Master Key to smart cards
- Import Master Key from smart cards
- Generate Module RSA Key
- Create User
- Generate Application Keys (AP Key)
- Set AP Key ACL
- Export AP Keys to smart cards
- Erase AP Key
- Erase All AP key
- Erase Back up Smart Card

[2] Password and PIN are used interchangeably in the documentation but both refer to the 8-digit password used during the authentication process.

- Import AP Keys
- Create Security Officers (COs)
- Set Real Time Clock
- Send self-test command to module
- Switch to Initialization state (zeroization of module)
- Write Application data

The services available to the User are as follows:

- Change smart card PIN.
- Use symmetric AP Keys for encryption and decryption
- Use asymmetric AP keys for generating and verifying signatures

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 a RSA signature on smart cards and a corresponding 8 digit PINs to check the validity of 2<= n but <=3 key pairs stored within the module.	▪ Change smart card PIN ▪ Export Master Key shares to smart cards ▪ Generate Module RSA Key ▪ Create User smart card ▪ Generate Application Keys (AP Key) ▪ Set AP Key ACL ▪ Export AP Keys to smart cards ▪ Erase AP Key ▪ Erase All AP keys ▪ Erase Back up Smart Card ▪ Import AP Keys ▪ Create Security Officers (COs) ▪ Set Real Time Clock ▪ Send self-test command to module ▪ Switch to Initialization state (zeroization of module) ▪ Write Application data ▪ Import Master Key from Smart cards	**w/x** **r/x** **w/x** **w/x** **w/x** **w/x** **w/x** **w/x** **w/x** **w/x** **w/x** **w/x** **w/x** **r/w/x** **w/x** **w/x** **r/x**

User	Authentication	Services	Access
	Identity – based using a RSA signature on smart cards and a corresponding 8 digit PINs to check the validity of n > 2 but <=9 key pairs stored within the module.	▪ Change smart card PIN ▪ Use symmetric AP Keys for encryption and decryption ▪ Use asymmetric AP keys for generating and verifying signatures	**w/x** **x** **x**

Unauthenticated role :

- View Status
- View Serial No. and Version of Firmware
- View AP RSA public key
- View AP key status
- Do Hash function
- Generate random number
- Get Application data

Unauthenticated User	Authentication	Services	Access
	None	▪ View Status ▪ View serial number and version of firmware ▪ View AP RSA public key ▪ View AP key status ▪ Generate random number ▪ Do Hash function ▪ Get Application data	**r** **r** **r** **r** **r/x** **x** **x**

2.3 Finite State Model

The HiPKI SafGuard 1000 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 1000 HSM consists of the following states:

- Power Off,
- Power On,
- Uninitialized ,
- Self Tests,
- Idle/ operational ,
- CO,
- Key Entry,
- User, and
- Error.

2.4 Physical Security

The HiPKI SafGuard 1000 HSM is defined as a multi chip standalone module. The module consists of production grade components, which include standard passivation techniques. The HiPKI SafGuard 1000 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 1000 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 1000 HSM in case of power failure to the module.

2.5 Cryptographic Key Management

The HiPKI SafGuard 1000 HSM in Approved mode provides cryptographic functionality using the following algorithms:

- RSA (1024, and 2048 keys),
- SHA-1, SHA-224,SHA-256,SHA-384,SHA-512
- Triple-DES (3-key ECB and CBC),
- Triple-DES MAC (Vendor affirmed)
- AES (ECB and CBC 128, 192 and 256 bit keys) and
- RNG (ANSI X9.31 Appendix 2.4).

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 1000 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 plaintext using split knowledge procedures.

Table 3: Cryptographic Keys and CSP’s

Key	Generation	Storage	Use	Role
Application Keys Triple-DES, AES, and RSA	The HiPKI SafGuard 1000 HSM generates these internally using a PRNG compliant to ANSI X9.31.	Stored in NVRAM	Triple -DES and AES Application Keys (APK) used for data encryption and decryption. RSA Application keys are used for Signature Generation and Verification	User CO
Master Key	The HiPKI SafGuard 1000	Stored in	Used to encrypt Security	User

Key	Generation	Storage	Use	Role
AES 256 bit	HSM generates these internally using a PRNG compliant to ANSI X9.31.	NVRAM	Officer Private Key	CO
Session Key Triple-DES 192 bit	Generated outside of the HiPKI SafGuard 1000.	Stored in NVRAM	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
Manufacturing Key RSA 2048 bit public key	Generated outside of the HiPKI SafGuard 1000.	Stored in Serial Flash	Manufacturer's key (RSA 1024) is stored in Serial Flash to verify software integrity at startup.	User CO
Module Key RSA 1024 bit keys	The HiPKI SafGuard 1000 HSM generates these internally using a PRNG compliant to ANSI X9.31.	The private key is stored in NVRAM on the module and the public key is stored on the Host.	A RSA key pair is used to wrap a Triple-DES Session key from host to HSM.	CO
Security Officer's Public Key RSA 1024 bit key	The HiPKI SafGuard 1000 HSM generates by smart card .	Stored in NVRAM	Public key on unit used for authentication to the private key on Security Officers smart card.	CO
Users Public Key RSA 1024 bit key	The HiPKI SafGuard 1000 HSM generates by smart card .	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

2.6 EMI/EMC

The HiPKI SafGuard 1000 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 RPX 71251000 and the certificate has been presented as evidence in the FIPS 140-2 validation of the Chunghwa Telecom HiPKI SafGuard 1000 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:

- KAT Algorithm Test for Triple-DES encrypt/decrypt
- KAT Algorithm Test for Triple-DES MAC
- KAT Algorithm Test for AES encrypt/decrypt
- KAT Algorithm Test for RSA (sign and verify)
- KAT Test for RNG
- Software/Firmware integrity Test RSA signature verification
- KAT Algorithm Test for SHA-1, SHA-256, SHA-512

The module performs the following conditional self-tests:

- Pair-wise consistency test for RSA
- RNG continuous test

2.8 Design Assurance

The Chunghwa Telecom Inc. HiPKI SafGuard 1000 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 1000 HSM,
- Secure delivery specifications for distributing the module to authorized operators,
- Secure installation, generation and start-up procedures specifications for configuring the HiPKI SafGuard 1000 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 1000 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 1000 HSM.

2.9 Approved Mode of Operation

Upon receipt of the HiPKI SafGuard 1000 HSM from Chunghwa Telecom Co., Ltd. Telecommunication Laboratories, the HiPKI SafGuard 1000 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 1000 host application. This synchronizes the system time on the host with the RTC on the HSM.
2. Set the configuration of the HiPKI SafGuard 1000. 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 blue LEDs and the “FIPS Mode” message on the module’s LCD.

When the HiPKI SafGuard 1000 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.