中華電信股份有限公司
Chunghwa Telecom Co., Ltd.

SafGuard 200 HSM

Hardware version HSM-HW-0312.02

Firmware version HSM-SW-ARM-FRTO.01

FIPS 140-2 Non–Proprietary Security Policy

Level 3 Validation

Version 6.0

June 23, 2004

Developed for: Chunghwa Telecom Co., Ltd

By: AEPOS Technologies Corporation

Date: June 23, 2004

Version Control Table

Version	Date	Reason for Change	Author
0.1	September 11, 2003	Document creation	AEPOS Technologies Corporation
0.2	November 20, 2003	First draft to DOMUS	AEPOS Technologies Corporation
1.0	December 19, 2003	Final draft to DOMUS	AEPOS Technologies Corporation
2.0	February 17, 2004	Final to DOMUS	AEPOS Technologies Corporation
3.0	February 19, 2004	Amended from comments	AEPOS Technologies Corporation
4.0	May 26, 2004	Comments from NIST	Chunghwa Telecom
5.0	June 9, 2004	Comments from NIST	Chunghwa Telecom
6.0	June 23, 2004	Comments from NIST	Chunghwa Telecom

中華電信股份有限公司
Chunghwa Telecom Co., Ltd.

Table of Contents

Version Control Table i
Table of Contents ii
1.0 Introduction 1
1.1 Purpose 1
1.2 References 1
2.0 SafGuard 200 HSM 1
Algorithm 2
Modes Used 2
2.1 Module Ports and Interfaces 3
Physical Interface 4
2.2 Roles and Services 4
2.3 Finite State Model 6
2.4 Physical Security 7
2.5 Cryptographic Key Management 7
Master Key 8
Session Key 8
Manufacturing Key 8
Module Key 8
Security Officer's Public Key 8
2.6 EMI/EMC 9
2.7 Self-Tests 9
2.8 Design Assurance 10
2.9 Approved Mode of Operation 11

中華電信股份有限公司
Chunghwa Telecom Co., Ltd.

1.0 Introduction

1.1 Purpose

This is a non-proprietary security policy developed by AEPOS Technologies Corporation for the Chunghwa Telecom Ltd. SafGuard 200 HSM (hardware version HSM-HW-0312.02 and firmware version HSM-SW-ARM-FRTO.01). It describes how the SafGuard 200 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.

1.2 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/cryptval/.

For more information about Chunghwa Telecom Co. Ltd. please visit http://www.cht.com.tw.

2.0 SafGuard 200 HSM

The Chunghwa Telecom Co., Ltd. SafGuard 200 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 SafGuard 200 HSM is the physical hardware box itself. All cryptographic module components are included inside this boundary.

The Approved cryptographic functions supported are as follows:

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

Algorithm	Modes Used	Certificate Number
RSA	Digital Signatures	Vendor Affirmed to FIPS 186-2
SHA-1	Byte - Oriented	201
Triple DES, 3-key	ECB and CBC	224
AES 192-bit and 256-bit	ECB and CBC	111

In Non-Approved mode, the SafGuard 200 HSM supports RC6 encryption.

A photograph of the SafGuard 200 HSM which is approximately to scale, is included below.

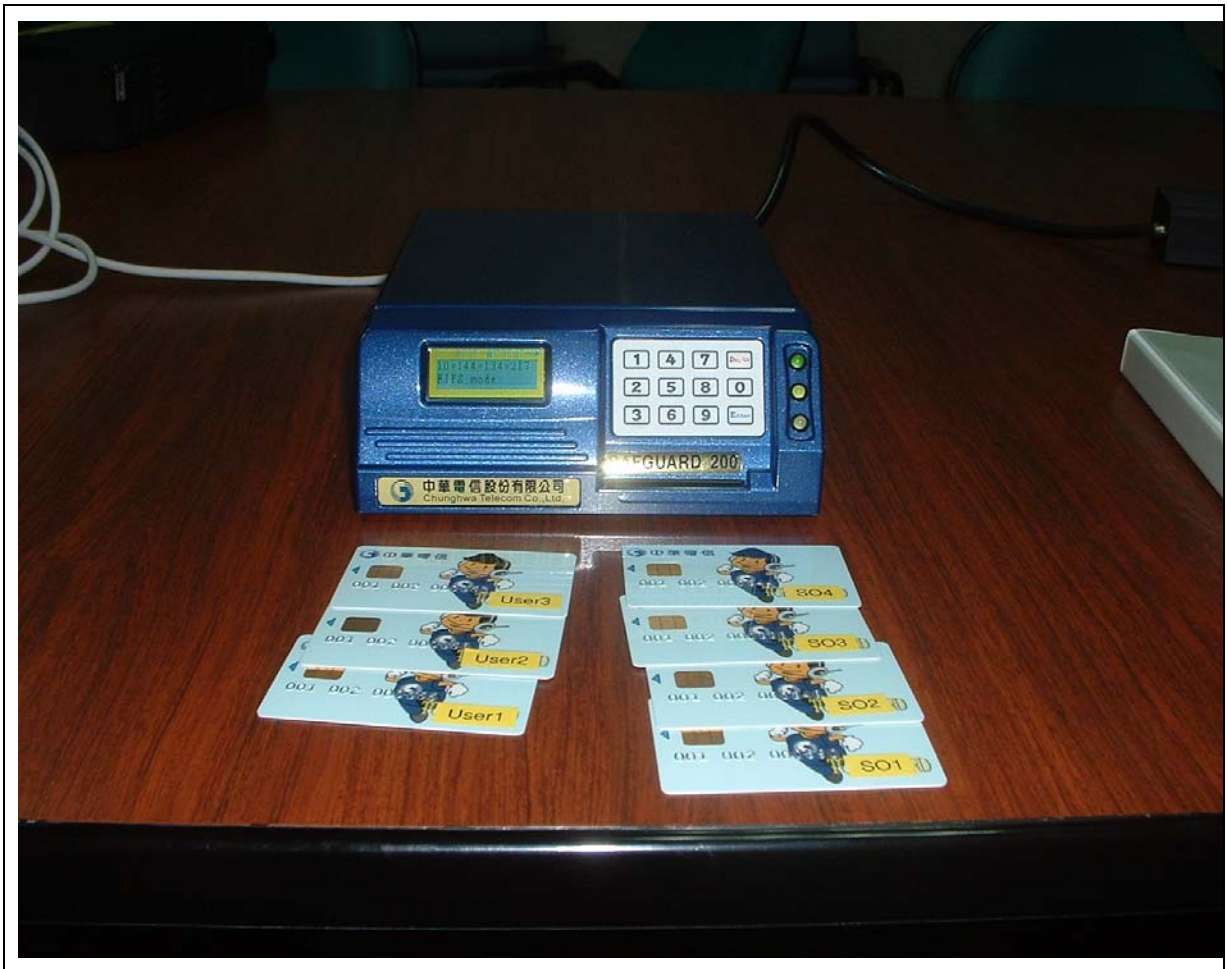

Figure 1 Chunghwa Telecom Co. SafGuard 200 HSM

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:**
  - 10/100 Ethernet which connects the SafGuard 200 to the Host
- **Data output:**
  - 10/100Ethernet to Host, and
- **Control input:**
  - 10/100 Ethernet, and
  - Keypad (front of module)
- **Status output:**
  - LCD message (on front of module),
  - LEDs (on front of module), and
  - 10/100 Ethernet message to Host.
- **Power interface:**
  - AC power source interfaces to the Chi-Sam CH-1253TA Power Module

The table below describes the relationship between the interfaces.

Table 1: Mapping Physical Interfaces

Interface	Physical Interface
Data Input Interface	10/100 Ethernet
Data Output Interface	10/100 Ethernet
Control Input Interface	10/100 Ethernet
	Front Panel Key pad
Status Output Interface	LCD
	LEDs on front of module
	10/100 Ethernet
Power Interface	Chi-Sam CH-1253TA Power Module

2.2 Roles and Services

The module supports a Crypto Officer and a User role. The SafGuard 200 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 4 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
- Import Master Key from smart cards
- Export Master Key share to smart cards
- Generate hardware RSA Key
- Create Users
- Create User private/public keys
- Generate Application Keys (AP Key)
- Set AP Key ACL
- Backup AP Keys to smart cards
- Erase AP Key
- Erase Back up Smart Card
- Restore AP Keys from smart cards

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

- Create Security Officers (COs)
- Set Real Time Clock
- Set network configuration
- Send self-test command to module
- Switch to Initialization state (zeroization of module)
- Write CA software version information
- Update firmware

The services available to the User are as follows:

- Change smart card PIN
- View serial number and version of firmware
- View network settings
- Use symmetric AP Keys for encryption and decryption
- Use asymmetric AP keys for generating and verifying signatures
- Send self-test command to the module

The table below shows the services available to each role.

Table 2: Services Table

Crypto Officer	Authentication	Services	Access
There are up to 4 Crypto Officers. The Services and Authentication information is true for CO1, CO2, CO3 and CO4, i.e. all COs	Identity – based using an RSA private key stored on a smart card and an 8 digit PIN.	**Single CO Services** ▪ Change password ▪ View Status ▪ View Serial No. and Version of Firmware	 **r/w/x** **r** **r**
	Identity – based using RSA private keys stored on smart cards and a corresponding 8 digit PINs to check the validity of 2<= n but <=4 key pairs stored within the module.	**CO authenticated Services** ▪ Import Master Key from smart cards (3DES) ▪ Export Master Key share to smart cards ▪ Generate hardware RSA Key ▪ Create User private/public keys ▪ Generate AES and 3DES Application Keys (AP Key) ▪ Set AP Key ACL ▪ Backup AP Keys to smart cards ▪ Erase AP Key ▪ Erase Back up Smart Card ▪ Restore AP Keys from smart cards ▪ Create Security Officers (COs)	 **w/x** **w/x** **w/x** **w/x** **w/x** **r/w/x** **w/x** **r/x** **r/x** **w/x** **r/w/x**

		▪ Set Real Time Clock ▪ Set network configuration ▪ Send self-test command to module ▪ Switch to Initialization state (zeroization of module) ▪ Write CA software version information ▪ Update firmware	**r/w/x** **r/w/x** **r/x** **r/x** **r/w/x** **r/w/x**
User	**Authentication**	**Services**	**Access**
	Identity – based using an RSA private key stored on a smart card and an 8 digit PIN.	**Single User Services** ▪ Change smart card PIN ▪ View serial number and version of firmware ▪ View network settings	 **r/w/x** **r** **r**
	Identity – based using RSA private keys stored on smart cards and a corresponding 8 digit PINs to check the validity of n > 2 but <=9 key pairs stored within the module.	**User Authenticated Services** ▪ Encrypt/decrypt using AES or 3DES Application Keys (APKs)s that are available according to the User's profile established at setup ▪ Run self-tests ▪ Generate RSA signature ▪ Verify RSA signature	 **x** **x** **x** **x**

2.3 Finite State Model

The SafGuard 200 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 SafGuard 200 HSM consists of the following states:

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

2.4 Physical Security

The SafGuard 200 HSM is defined as a multi chip standalone module. The module consists of production grade components, which include standard passivation techniques. The SafGuard 200 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 SafGuard 200 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 SafGuard 200 HSM in case of power failure to the module.

2.5 Cryptographic Key Management

The SafGuard 200 HSM in Approved mode provides cryptographic functionality using the following algorithms:

- RSA (1024, 2048 and 4096 bit keys),
- SHA-1,
- Triple DES (3-key ECB and CBC), and
- AES (ECB and CBC 192 and 256 bit 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 SafGuard 200 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 out 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, and RSA is supported in FIPS Mode RC6 is supported in non-FIPS mode.	The SafGuard 200 HSM generates these internally using a PRNG compliant to ANSI X9.31.	Stored in NVRAM	Triple DES, RC6 and AES Application Keys (APK) used for data encryption and decryption. RSA Application keys are used for Signature Generation and	User CO

Key	Generation	Storage	Use	Role
			Verification	
Master Key Triple DES	The SafGuard 200 HSM generates these internally using a PRNG compliant to ANSI X9.31.	Stored in NVRAM	Used to encrypt Security Officer Private Key	User CO
Session Key Triple DES	Generated outside of the SafGuard 200.	Stored in DRAM	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 1024 bit public key	Generated outside of the Safguard 200.	Stored in EEPROM	Manufacturer's key (RSA 1024) is stored in EEPROM to verify software download. The public key is also used to verify firmware integrity at startup.	User CO
Module Key RSA 1024 bit keys	The SafGuard 200 HSM generates these internally using a PRNG compliant to ANSI X9.31.	A RSA key pair is used to transmit a 3DES Session key. The private key is stored in NVRAM on the module and the public key is stored on the Host.	Wrap the session key.	CO CO
Security Officer's Public Key RSA 1024 bit key	The SafGuard 200 HSM generates these internally using a PRNG compliant to ANSI X9.31.	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 SafGuard 200 HSM generates these internally using a PRNG compliant to ANSI X9.31.	Stored in NVRAM	Public key on unit used for authentication to the private key	User

Key	Generation	Storage	Use	Role
			on User's Smart Card.	
PIN's	N/A	Stored on smart card	Authentication	CO User

2.6 EMI/EMC

The SafGuard 200 HSM complies with EMI/EMC requirements as specified by 47 Code of Federal Regulations, Part 15 Subpart B (home use). The FCC number assigned to this validation is RPXCHTS200202 and the certificate has been presented as evidence in the FIPS 240-2 validation of the Chunghwa Telecom SafGuard 200 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 3DES encrypt/decrypt
- KAT Algorithm Test for AES encrypt/decrypt
- KAT Algorithm Test for RSA
- Pair-wise consistency test for RSA
- RNG Test
- Software/Firmware integrity Test
- KAT SHA-1

Cryptographic Algorithm KATs

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

- 3-key Triple DES (ECB and CBC mode) used for data encryption/decryption,
- 192 and 256 bit AES (ECB and CBC mode) used for data encryption/decryption,
- SHA-1 hash, and
- RSA asymmetric keys (1024, 2048 and 4096 bit keys) used for digital signature, signing/verifying and wrapping session key.

Firmware Downloads

An RSA key 1024 – bit public key is stored in EEPROM at the time of manufacture. This key is used for verification of firmware downloads to the SafGuard 200 HSM.

Software/Firmware Integrity Test

At start up, the SafGuard 200 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 continuous random number generator test is run as part of the self-test suite both at module startup and when the self-test command is issued by the CO or the User. The test is as follows: The module generates a 20 byte block of data at power on and stores the data as previous_random. As part of the self-test, the module generates a 20 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.

2.8 Design Assurance

The Chunghwa Telecom Inc. SafGuard 200 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 SafGuard 200 HSM,
- Secure delivery specifications for distributing the module to authorized operators,
- Secure installation, generation and start-up procedures specifications for configuring the SafGuard 200 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 some use of Assembly language for performance in the DSP (Math board),
- 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 SafGuard 200 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 SafGuard 200 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 upgrades.

- Upon receipt of the SafGuard 200 HSM from Chunghwa Telecom Ltd., the SafGuard 200 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 SafGuard 200 host application. This synchronizes the system time on the host with the RTC on the HSM.
  2. Set the network configuration of the SafGuard 200. This entails setting the following parameters:
     - IP Address;
     - Subnet Mask;
     - Gateway Address; and
     - Set FIPS Mode Flag. (This action disables the non-FIPS approved algorithm RC6)
  3. After these parameters have been set, the HSM must be reset.
  4. A master key (Triple DES) must be generated by the HSM.
  5. The master key must then be written to the Crypto-Officers smart card in split key format. To do this, each Crypto-Officer must authenticate to the smart card.
  6. Generate an RSA Key Pair for each smart card and write the private key to the smart card wrapped with the Master Key (Triple DES).
  7. Generate a Hardware Key (RSA) that is used to wrap the session key (Triple DES) from the HSM to the Host. The module must now be rebooted.
  8. Authenticate to the HSM in the Crypto Officer role and create User keys.
  9. Activate the group (i.e. CO and User).
  10. Generate the Application Key (3DES or AES) and assign it to the CO or User group.
  11. Activate the Application Key. This requires authenticating to the HSM in the CO role.
  12. Input a session key (3DES) wrapped with the Hardware Key, into the HSM.
  13. The module is now operational in FIPS mode. This is indicated by the module’s 3 green LEDs and the “FIPS Mode” message on the module’s LCD.

The SafGuard 200 HSM provides the following Approved mode algorithms for use:

- Triple DES (3-key ECB and CBC mode) for encryption and decryption,

- AES (ECB and CBC mode 192 and 256 bit keys) for encryption and decryption,
- RSA (1024, 2048 and 4096 bit keys) for digital signatures, and
- SHA-1 (hash for signatures).

When the SafGuard 200 HSM is operating in Approved mode, the LCD screen displays the message “FIPS mode” and the three LEDs on the front panel are green.