Chunghwa Telecom Co., Ltd.
HiCOS PKI Native Smart Card Cryptographic Module
Security Policy

FIPS 140-2 Level 2 Validation

Hardware: HD65255C1 and HD65257C1
HardMask: Version 2.1
SoftMask: Version 1.0

April 17, 2013
Version 1.1

© 2013, Chunghwa Telecom Co., Ltd. All rights reserved.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

© 2013, Chunghwa Telecom Co., Ltd. All rights reserved.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

© 2013, Chunghwa Telecom Co., Ltd. All rights reserved.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1 Introduction

This document is the Security Policy for the Chunghwa Telecom Co., Ltd. HiCOS PKI Native Smart Card cryptographic module. This module, hereafter called the HiCOS PKI native smart card cryptographic module, or simply, the module, is a single chip module that is used to provide user authentication and cryptographic services.

This Security Policy specifies the security rules under which the module must operate to meet the requirements of FIPS 140-2 Level 2. It describes how the module functions to meet the FIPS requirements, and the actions that operators must take to maintain the security of the module.

This Security Policy describes the features and design of the Chunghwa Telecom Co., Ltd. HiCOS PKI Native Smart Card cryptographic module using the terminology contained in the FIPS 140-2 specification. *FIPS 140-2, Security Requirements for Cryptographic Modules* specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2 and other cryptography-based standards. Validated modules are accepted by the Federal agencies of both the USA and Canada for the protection of unclassified but sensitive information. Many other governments, private organizations, and financial institutions also recognize FIPS-validated modules.

The FIPS 140-2 standard, and information on the CMVP, can be found at http://csrc.nist.gov/groups/STM/cmvp/index.html.

This Security Policy contains only non-proprietary information. All other documentation submitted for FIPS 140-2 conformance testing and validation is deemed proprietary and is releasable only under appropriate non-disclosure agreements.

1.1 Security Levels

The HiCOS PKI Native Smart Card cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2. The individual security requirements specific for FIPS 140-2 meet the level specification indicated in the Table 1.

Table 1 - Security Requirements Specific to FIPS 140-2.

Security Requirements Section	*Level*
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self Tests	2
Design Assurance	3
Mitigation of other attacks	2

For the physical testing at Level 3, the module hardness testing was only performed at ambient temperature of 72 °F and no assurance is provided for Level 3 hardness conformance at any other temperature.

1.2 Acronyms and Abbreviations

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Data Encryption Standard
EDC	Error Detection Code
EF	Elementary File
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
PRNG	Pseudo Random Number Generator
PUB	Publication
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman Public Key Algorithm
SHA-1	Secure Hash Algorithm
SRDI	Security Related Data Item
X.509	Digital Certificate Standard RFC 2459

2 Chunghwa HiCOS PKI Native Smart Card cryptographic module

2.1 Functional Overview

The HiCOS PKI Native Smart Card cryptographic module cryptographic module contains an implementation of native operation environment (limited operational environment), the security policy is based on the file system created. PINS and keys that have been securely loaded at card issuance authenticate the roles of the Crypto Officer and User (Card Holder).

2.2 Cryptographic Module Specification

The HiCOS PKI Native Smart Card cryptographic module is a single chip implementation of a cryptographic module. Figure 1 shows a physical view of the module configured into a smart card. Figure 1 shows only the module contact faceplate. The chip is located directly under the faceplate within the outline shown.

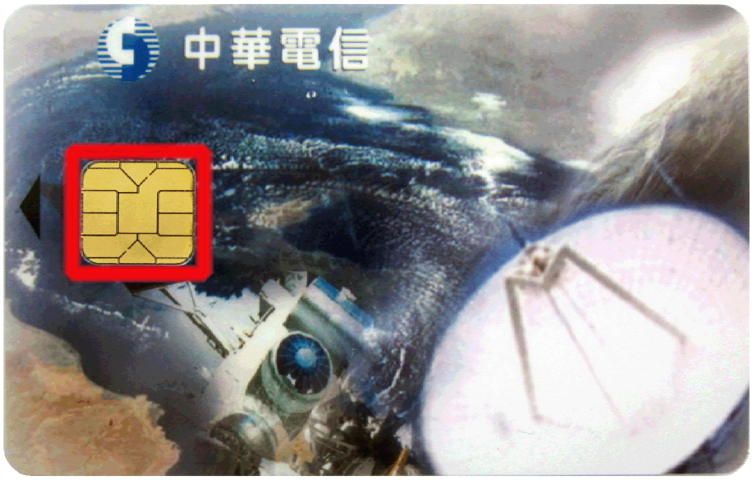

Figure 1. Physical View of the Cryptographic Module.

The HiCOS PKI Native Smart Card cryptographic module is mounted in an ID-1 class smart card body that adheres to ISO/IEC specifications for Integrated Circuit Chip (ICC) based identification cards. The “cryptographic boundary” for the module with respect to the FIPS 140-2 validation is the “module edge”. The module consists of the chip (ICC), the contact faceplate, and the electronic connectors between the chip and contact pad, all contained within an epoxy substrate. The module is constructed so as to provide the tamper evidence required in the FIPS 140-2 physical Level 3 validation for single-chip implementations.

The hardware base is the Renesas AE55C1 and AE57C1 smartcard IC that is validated under the Common Criteria at EAL4+.

The HiCOS PKI Native Smart Card cryptographic module consists of the following elements:

- Renesas HD65255C1 and HD65257C1 microcomputer. This IC is a standard, production-quality IC.
- System firmware is installed in Read Only Memory (ROM) as part of the chip manufacturing process (known as the Hard Mask) and in Electrically Erasable, Programmable Read Only Memory (EEPROM) for system option (known as the Soft Mask). The firmware is then designated: HardMask version 2.1; SoftMask version 1.0. These HardMask and SoftMask version identifiers are returned in the Answer To Reset (ATR) character string following the issuing of a RESET signal to the module (the ATR is: 3B BA 13 00 81 31 FA 52 48 69 43 4F 53 56 33 33 **10 21** A8). Bold numbers in the string are the SoftMask and HardMask version identifiers.

Critical Security Parameters are stored in the EEPROM as part of the module personalization operation.

- The chip is encased in hard opaque epoxy-resin using standard passivation techniques such that any attempt to gain physical access to the components would critically damage the module with a high probability of making the module unusable (the module will not function). The resin material is opaque within the visible spectrum.

2.3 Operational Environment

The HiCOS PKI Native Smart Card cryptographic module has a limited operational environment consisting of a native system operating on a Renesas HD65255C1 and HD65257C1 Smartcard Integrated Circuit chip. The module does not support firmware update as this function is performed at the factory.

2.4 Module Ports and Interfaces

2.4.1 PHYSICAL PORT DESCRIPTION

The HiCOS PKI Native Smart Card cryptographic module supports eight contacts that lead to pins on the chip. Only five of these contacts are used. The location of the contacts complies with ISO/IEC 7816-2 standard. Minimum contact surface area is 1.7 mm by 2.0 mm.

Contact dimensions are standard credit card compliant as per ISO/IEC 7816-1 standard:

Table 2. Smart Card Chip Contact Area.

Dimensions	*Value*
Length	85.5mm
Width	54.0mm
Thickness	0.80mm

Figure 2 shows the physical layout of the contacts.

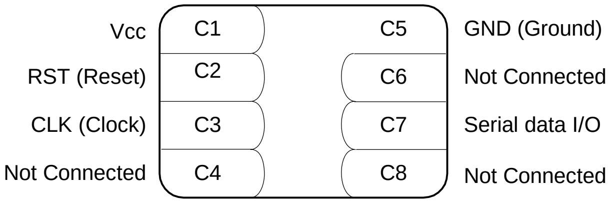

Figure 2. Physical Layout of the Contacts.

2.4.2 SPECIFIC FUNCTIONS OF CHIP CONTACTS

Table 3. Functional Specifications of Chip Contacts.

Contact	*Function*	*FIPS 140-2 Logical Interface*
C1	Vcc supply voltage 2.7 to 3.3V +/-0.5 V or 4.5 to 5.5V +/-0.5 V	Power Port
C2	RST (Reset)	Control Input Port
C3	CLK (Clock)	Control Input Port

C4	Not Connected to the chip	N/A
C5	GND (Ground)	Power Port
C6	Not Connected to the chip	N/A
C7	Serial data input and serial data output.	Data Input Port, Data Output, Control Input PortStatus Output Port
C8	Not Connected to the chip	N/A

2.4.3 ICC Supply current

- Maximum Value: 10mA at 5Mhz
- Typical Value: 3mA at 5Mhz

2.4.4 MODULE SECURITY AND KEY ACCESS COMMAND SET

Module security and key access command set defined by the following specifications:

- Chunghwa Telecom HiCOS PKI Native Smart Card cryptographic module User's Manual V3.3.
- Chunghwa Telecom HiCOS PKI Native Smart Card cryptographic module Operator Guidance v1.0.

2.4.5 EMI/EMC

The base cryptographic module has been tested by Advance Data Technology Corporation, and found in compliance with the requirement of the following standards.

- FCC Part 15 : 2005 Subpart B, Class B.(Section 15.31,15.107 and 15.109)
- CISPR 22: 1997,Class B.(Section 5,6,9 and 10)
- ICES-003: 2004,Class B.(Section 4 and 5)
- ANSI C63.4-2003 (Section 7 and 8)

2.4.6 CAD TO MODULE COMMUNICATIONS PROTOCOLS

Card Accepting Device (CAD) to module communication protocols is defined by ISO/IEC 7816-3 & 4. This is based on a standardized, half-duplex character transmission, ISO 7816 protocol. Protocol T=1 is supported.

2.4.7 LOGICAL INTERFACE DESCRIPTION

The I/O port (C7) of the platform (refer to Table 3) provides the following logical interfaces:

- Data In (I/O bidirectional line)
- Data Out (I/O bidirectional line)
- Control In (CLK, RST, and I/O bidirectional line)
- Status Out (I/O bidirectional line)

The APDU command protocol and synchronization timing controls, provided in part by way of the platform CLK clock input, manage the separation of logical interfaces that use the same physical port.

Electrical (physical) contact and data link layer contact is established between the smart card chip and the CAD by the CAD issuing a RESET signal to the smart card chip which then responds with an "Answer To Reset (ATR)" containing the version numbers of the hard mask contained on the smart card chip. From this point on, the card functions as a "slave" processor to implement and respond to the CAD's "master" commands. The card adheres to a well defined set of state transitions. Within each state, a specific set of commands is accessible.

The details of these commands are defined in the Chunghwa Telecom HiCOS PKI Native Smart Card cryptographic module User's Manual V3.3 and ISO 7816-4.

3 Roles, Services, and Authentication

3.1 Roles

The HiCOS PKI Native Smart Card cryptographic module uses identity-based access control. Access control rules provide services to operators who identify themselves by demonstrating knowledge of a cryptographic key set, or PIN.

The module defines three distinct roles that are supported by the on-card cryptographic system: the Crypto Officer role, a Card Holder role, and an unauthenticated role.

- Crypto Officer is a role authenticated by demonstrating knowledge of a key set and key ID.
- Card Holder is a User role authenticated by possession of the card and knowledge of the Card Holder PIN.
- The unauthenticated role is assumed by any unauthenticated operator who has access to the host application.

The module ensures the authentication of off-card entities (Cryptographic Officer and Card Holder) and provides them with cryptographic services according to their role. Operators may not change roles without re-authenticating in the new role. All previous authentications are cleared when the module powers down.

The HiCOS PKI Native Smart Card cryptographic module does not allow multiple concurrent operators or support a maintenance role.

3.1.1 Cryptographic Officer Role

It is the on-card security controller and establishes his/her identity on the HiCOS PKI Native Smart Card cryptographic module in Triple-DES verification of a key set stored in card. Through mutual authentication (Based on the key ID specified in file attribute) between the Crypto Officer and the card, he/she could process this file (It could be MF, PDF, CDF or EF) by commands defined according to each file attribute (ex. Under MF, CREATE FILE command could be used)

3.1.2 Card Holder

It is the card holder, responsible for ensuring the ownership of his/her card and for not communicating the PIN. The User Role operator is authenticated by verification of a PIN. After successful authentication of User, he/she could generate RSA key, read insensitive data from file.

3.1.3 Unauthenticated

It is assumed by any unauthenticated operator who has access to the card. The operator can only read non-security relevant card information.

3.2 Module Services

3.2.1 *Module Services*

Crypto Officer Administrative Services

A crypto officer can make changes on the card using commands that are available after the crypto officer role is authenticated. The crypto officer authenticates to his role by proving knowledge of a crypto officer key set associated with the card and using the key set to establish a secure channel.

Roles, Basic Card Services, and Access Controls for Cryptographic Keys and CSPs

Each role has access to specific basic card services. The basic card services, in turn, may use or operate on cryptographic keys or critical security parameters (CSPs). The following table shows the relationship between roles, services and indicates the type of access provided to various cryptographic keys and CSPs.

Table 4. Card Services

Role	***Services***	***Cryptographic Keys and CSPs accessed***	***Type(s) of Access***
Crypto-Officer	SELECT FILE	None	Execute
	CREATE FILE	None	Write
	READ BINARY	None	Read
	UPDATE BINARY	None	Write
	ERASE BINARY	None	Write
	READ RECORD	None /RSA Public Key	Read
	UPDATE RECORD	None	Write
	APPEND RECORD	None	Write
	READ VALUE	None	Read
	ADD VALUE	None	Write
	SUBSTRACT VALUE	None	Write
	NEW VALUE	None	Write
	GET CHALLENGE	None	Execute
	EXTERNAL AUTHENTICATE	Triple-DES Key	Execute
	INTERNAL AUTHENTICATE	Triple-DES Key	Execute
	LOAD KEY	PIN, Triple-DES Key, RSA Public/Private Key	Write
	CHANGE KEY	Triple-DES Key, RSA Public/Private Key	Read/Write
	UNLOCK KEY	PIN, Triple-DES Key	Write
	GENERATE RSA KEY PAIR	RSA Public/Private Key	Write
	GENERATE HASH	None	
	RSA CRYPTOGRAPHY	RSA Public/Private Key	Execute
	GET RSA RESULT	None	Read
	FIPS KNOW ANSWER TEST	None	Execute
	GET DATA	None	Read
	FREE MEM	None	Read
	ERASE ALL	All the PINs, Triple-DES Keys, RSA Public/Private Keys and any CSPs will be erased	Write
	GET COS INFO	None	Read
	Obtain FIPS Approved mode of operation indicator: SELECT FILE 0x001 followed by READ BINARY	Card Number EF file	Read
User	SELECT FILE	None	Read
	READ BINARY	None	Read
	UPDATE BINARY	None	Write
	ERASE BINARY	None	Write
	READ RECORD	None /RSA Public Key	Read
	UPDATE RECORD	None	Write
	APPEND RECORD	None	Write
	READ VALUE	None	Read
	ADD VALUE	None	Write
	SUBSTRACT VALUE	None	Write
	VERIFY	PIN	Execute
	GET CHALLENGE	None	Execute

	GENERAT HASH	None	Execute
	CHANGE KEY	PIN	Write
	GENERATE RSA KEY PAIR	RSA Public/Private Key	Write
	RSA CRYPTOGRAPHY	RSA Public/Private Key	Execute
	GET RSA RESULT	None	Read
	FIPS KNOW ANSWER TEST	None	Execute
	GET DATA	None	Read
	FREE MEM	None	Read
	GET COS INFO	None	Read
	Obtain FIPS Approved mode of operation indicator: SELECT FILE 0x001 followed by READ BINARY	Card Number EF file	Read
Unauthenticated	SELECT	None	Execute
	GET CHALLENGE	None	Execute
	EXTERNAL AUTHENTICATE	Triple-DES Key	Execute
	VERIFY	PIN	Execute
	GET DATA	None	Read
	FREE MEM	None	Read
	GET COS INFO	None	Read
	GENERATE HASH	None	Read
	FIPS KNOW ANSWER TEST	None	Execute

3.3 *Authentication*

HiCOS PKI Native Smart Card cryptographic module provides 3 authentication mechanisms, external authentication., internal authentication and PIN verification, external authentication is used to authenticate Crypto Officer , internal authentication is used to authenticate smart card and PIN verification is used to authenticate User role.

There may be several Crypto Officer and User roles in card. Each PDF, CDF and EF may belong to individual Crypto Officer and the key ID for these PDF, CDF and EF may be different. Each EF may belong to individual User and the key under these EFs may be different. The file attribute for MF, PDF, CDF and EF will specify the presence of key or PIN for authentication is needed or not and which key or PIN is used for authentication.

3.3.1 Mechanisms:

To authenticate a Crypto Officer, he/she should apply SELECT FILE command to select the MF, PDF or CDF belong to him/her first. Then Crypto Officer should issue GET CHALENGE command to get a random number from card and encrypt the random number by the key which the key ID is specified in file attribute of MF, PDF or CDF, finally apply EXTERNAL AUTHENTICATE command to send back the encrypted random number to accomplish the authentication process.

To authenticate a card, Crypto Officer applies INTERNAL AUTHENTICATION command to send a random number to smart card and then verifies the returned cryptography from smart card to a accomplish the authentication process.

To authenticate a User, he/she should apply SELECT FILE command to select the EF belong to him/her first. Then the User applies VERIFY command to accomplish the authentication process.

3.3.2 Strength:

The following table provides rough estimates of the strengths of the module's authentication mechanisms.

Authentication Type	Strength
External Authentication	This mechanism applies Triple-DES 3-key, the probability of randomly guessing the correct sequences is 1 in 2^{168}.
Internal Authentication	This mechanism applies Triple-DES 3-key, the probability of randomly guessing the correct sequences is 1 in 2^{168}.
PINs	The minimum length of PIN is 8 bytes and the value is not limited to digital number. The maximum length of the PIN is specified by the application when the password is created. The maximum length of the PIN is ultimately limited by the maximum length of the password field, which is 253 bytes. Assuming that the PIN was only integers between 0-9, the probability of randomly guessing the correct sequences is 1 in 10^{8}.

3.3.3 Strength for multiple attempts:

External Authentication:

To attempt a brute force attack on the module, an attacker has to send APDU commands in a serial fashion to the module, and wait for the corresponding APDU response to each APDU command. Each APDU command must be responded to before the next APDU command can be sent. An attacker must send a minimum 13 byte APDU to the card, and get a resulting 2-byte response. As there is a single I/O port on the module, each attack is bottlenecked through this port. Each attack, that is, each attempt to authorize with a different Triple-DES key requires 15 bytes of data to be clocked in or out of the card. The maximum data rate for the module is 38,400Kbps through this single port. Ignoring the processing time required on the module to process the Triple-DES key, we can compute the maximum number of attempts which could occur within a 60 second interval:

- 15 bytes of I/O at 8bits/byte = 120bits/attempt
- 120bits/attempt divided by 38,400bits/second = .003125 seconds/attempt
- 60seconds/minute divided by .003125 seconds/attempt = 19,200attempts/minute

As the Triple-DES key space is over 2^{168} possible values, it follows that 19,200 attempts in a 60 second interval will not significantly traverse the space of possible values. As a result, the module far exceeds the requirement of 1 in 100,000 for multiple attempts in a 60 second interval.

Internal Authentication:

To try a key against the module, an attacker must send a minimum 14 byte APDU to the card, and get a resulting 10-byte response. As there is a single I/O port on the module, each Triple-DES key attempt requires 24 bytes of data to be clocked in or out of the card. The maximum data rate for the module is 38,400Kbps through this single port. Ignoring the processing time required on the module to process the Triple-DES key, we can compute the maximum number of attempts which could occur within a 60 second interval:

- 24 bytes of I/O at 8bits/byte = 192bits/attempt
- 192bits/attempt divided by 38,400bits/second =0 .005 seconds/attempt
- 60seconds/minute divided by 0.005 seconds/attempt = 12,000attempts/minute

As the Triple-DES key space is over 2^{168} possible values, it follows that 12,000 attempts in a 60 second interval will not significantly traverse the space of possible values. As a result, the module far exceeds the requirement of 1 in 100,000 for multiple attempts in a 60 second interval.

PIN Verification:

The minimum length of the User PIN is a string of 8-digit. PINs contain the digits 0 to 9 yielding a maximum of 10,000,000 possible PINs. This far exceeds the 1 in a million test.

To try a PIN against the module, the attacker must send a 13byte APDU to the card, and get a resulting 2-byte response. As there is a single I/O port on the module, this means that each PIN attempt requires 15 bytes of data to be clocked in or out of the card. The maximum data rate for the module is 38,400Kbps through this single port. If we ignore the processing time required on the module to check the PIN, we can compute the maximum number of PIN attempts which could occur within a 60 second interval:

- 15 bytes of I/O at 8bits/byte = 120 bits/attempt
- 120 bits/attempt divided by 38,400bits/second = .003125 seconds/attempt
- 60seconds/minute divided by .003125 seconds/attempt = 19,200 attempts/minute

As the minimum length PIN results in 10 million possible values, it follows that 19,200 attempts in a 60 second interval will not significantly traverse the space of possible PIN values. As a result, the module far exceeds the requirement of 1 in 100,000 for multiple attempts in a 60 second interval.

Moreover, an 8-bit counter internal to the Access Control applet further limits the number of failed PIN attempts an attacker could perform by blocking the card if the counter limit (3 attempts per PIN) is exceeded.

4 FIPS Approved Mode of Operation

The module only supports FIPS Approved mode of operation.

The module is shipped in a manufactured state, which is a partially initialized state.
During the initialization ("personalization") process of the module, the Crypto-Officer executes the required steps (please see below) to put the module in FIPS Approved mode, which is the only operational mode of the module.

The Crypto-Officer and the User roles can execute the following two commands to obtain the FIPS Approved mode of operation indicator. This is accomplished by querying the status of a special Elementary File (EF) with file ID 0x001, named Card Number:

SELECT FILE 0x001

READ BINARY

If the module has been initialized / personalized, the READ BINARY command will display a unique non-zero value, which means the module is in FIPS Approved mode.

The following procedures have to be performed to put the manufactured module in the FIPS mode of operation:

1. Pre-Personalization the HiCOS PKI Native Smart Card cryptographic module by:
   a. initialize the card;
   b. load the transport key (Triple-DES) and perform the GET CHALLENGE and EXTERNAL AUTHENTICATE commands. If the key is authenticated, the card is fully initialized;
2. Issue CREATE FILE command to create the basic file system(MF, Card Number EF and DES Key EF)
3. Issue LOAD KEY command to load default Triple-DES keys
4. Issue CREATE FILE command to create the other necessary files on the module and configure the file system when accessing security sensitive data or keys, secure messaging must be turned on.

5 Module Cryptographic Functions

The purpose of the HiCOS PKI Native Smart Card cryptographic module is to provide a FIPS validated module for card that may in turn provide cryptographic services to end-user. Cryptographic keys and CSPs (PINs) represent the roles involved in controlling the card. A variety of FIPS 140-2 validated algorithms are used in the HiCOS PKI Native Smart Card cryptographic module to provide cryptographic services; these include:

- Triple-DES for internal/external authentication, PIN verification, and encrypting keys input to the module using the LOAD KEY and CHANGE KEY command within the secure channel.
- RSA Sign and Verify.
- SHA-1, SHA-256, SHA-384 and SHA-512 Hashing.
- DRBG used for cryptographic key generation.

Details of cryptographic functions are shown in this table:

Table 5. Module Cryptographic Functions.

Type	Algorithm	FIPS Approved	Certificate
Public Key	RSA. Key size: 1024 and 2048 bits.	Yes (PKCS#1))	957
Symmetric Key	Triple-DES (ECB, CBC) 2 keys Triple-DES. Triple-DES (ECB, CBC) 3 keys Triple-DES.	Yes (FIPS 46-3)	1219
Keyed Hash	Triple-DES MAC (vendor affirmed)	Yes	1219
Digest	SHA-1	Yes (FIPS 180-3)	1649
	SHA-256		1649
	SHA-384		1649
	SHA-512		1649
RNG	DRBG (NIST SP 800-90 Hash_DRBG)	Yes	155
	NDRNG (HARDWARE RNG)	No	

Note:

1. *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.*
2. *From January 1, 2011 through December 31, 2015, the use of two-key Triple-DES for encryption is restricted: the total number of blocks of data encrypted with the same cryptographic key shall not be greater than 220. After December 31, 2015, two-key Triple-DES shall not be used for encryption. Please refer to NIST Special Publication 800-131A for more information.*

6 Cryptographic Key Management

The module contains a variety of keys and CSPs does not input or output plaintext cryptographic key components, plaintext authentication data, or other unprotected CSPs.

6.1 Card Manufacturing Keys

Card Manufacturing Authentication Key, **K_{TRAN}** Triple-DES key (192 bits) used only for the Card Manufacturing and ERASE ALL command (The module zeroizes) by card vendor's (Chunghwa Telecom Co., Ltd)

6.2 Secure messaging Keys

- Command/Response Encryption Key , **K_{ENC}** Triple-DES key (192 bits) used for data encryption/ decryption in CBC mode (to protect confidentiality of command data and response data when using secure messaging)
- Command/Response MAC Key, **K_{MAC}** Triple-DES key (192 bit) for data authentication (to protect data authenticity of command data and response data when using secure messaging)

6.3 Authentication Keys

- External Authentication Key, **$K_{EXTAUTH}$** Triple-DES key (192 bits) used to Authenticates the host using specific keys.
- Internal Authentication Key, **$K_{INTAUTH}$** Triple-DES key (192 bits) used to authenticate cryptographic module to host system
- Unlock Key Triple-DES key, **K_{UNLOCK}** (192 bits) is treated as a kind of External Authentication Key used to Unlock the locked DES key or PIN

6.4 PKI Key Pairs

RSA Public and private keys can be generated on the card using the GENERATE KEY PAIR command. Alternatively the keys may be loaded onto the card using the LOAD KEY command and be changed using the CHNANGE KEY command.

K_{SIGN} (PKI Key pair)

- RSA Public Sign Key, **$K_{PUBSIGN}$** for signature verification operations.
- RSA Private Key for Sign operations KPRIVSIGN

6.5 Cryptographic Key Generation

RSA key pairs may be generated using the GENERATE KEY PAIR function along with a key ID. The public key can be read from the READ RECORD COMMAND and may be used externally from the module by being included on a digital certificate establishing the relationship between the public-key and the identity of the Card Holder. The private-key, which is retained securely within the Key File, is used to establish the identity of the Card Holder by verifying a digital signature.

RSA key pairs are generated according to NIST SP 800-90A DRBG. A key is produced by the on board hardware RNG and that is used as entropy-input to the DRBG instantiation process to generate internal values, *V* and *C*, which are parameters to generate the random number. The module use Hash-DRBG mechanism and does not use optional data: personalization string and additional input.

The values *V* and *C* are critical values of the internal state of the Hash-based DRBG which are kept plaintext in the memory during the random number generation process and never leave the module. The values *V* and *C* are only derived from DRBG instantiation process and only used in the DRBG mechanism and never accessed by non-DRBG functions.

6.6 Cryptographic Key Entry

The Card Manufacturing Authentication Key is input to module EEPROM by the vendor during module manufacturing.

Triple-DES Keys are input to the DES Key File in encrypted format using the LOAD KEY command with secure messaging. During this process, the keys are encrypted (using the Command/Response Encryption Key)

The public-key is used externally from the module by being included on a digital certificate establishing the relationship between the public-key and the User. The certificate containing the public key may be stored on the card in a RSA public key file. The private-key, which is retained securely within the RSA private key file, is used to establish the identity of the Card Holder by forming a digital signature.

6.7 Cryptographic Key Storage

All secret and private keys are stored in plaintext format in EEPROM. The module uses the key ID to associate each key with the correct entity.

The following keys are stored on the module:

- **K_{TRAN}**(Triple-DES Card Manufacturing External Authentication Key)
- **K_{ENC}** (Triple-DES Command Encryption Key)
- **K_{MAC}** (Triple-DES MAC verification Key)
- **$K_{INTAUTH}$** (Triple-DES Internal Authentication Key)
- **$K_{EXTAUTH}$** (Triple-DES external Authentication Key)
- **K_{UNLOCK}** (Triple-DES external Authentication Key)
- **$K_{PUBSIGN}$** (RSA Public Key for signature verification operations)
- **$K_{PRIVSIGN}$** (RSA Private Key for Sign operations)

All keys and the Card Holder PIN are stored in plaintext format in EEPROM.

6.8 Cryptographic Key Destruction

The module zeroizes all secret and private cryptographic keys and CSPs using the ERASE ALL command.

7 Self Tests

7.1 Power Up Self Tests

The HiCOS PKI Native Smart Card cryptographic module performs the required set of self-tests at power-up. When the module is inserted into a smart card reader and power is applied to the module (contact) interface, a “Reset” signal is sent from the reader to the module. The module responds (as specified by ISO/IEC 7816) with an Answer To Reset (ATR) packet of information. When the first APDU command comes into the module, the module performs a series of power-on self tests. These tests include:

- Firmware integrity check CRC32 (integrity test)
- Algorithm (known answer) tests for:
  - Triple-DES (CBC mode encrypt/decrypt)
  - Triple-DES MAC
  - RSA PKCS1 (1024/2048 bits)sign
  - RSA PKCS1 (1024/2048 bits) verify
  - DRBG(NIST SP 800-90 Hash_DRBG)
  - SHA1 (Performed in RSA PKCS1 sign and verify test)
  - SHA256 (Performed in DRBG test)
  - SHA384

- SHA512

If any of these tests fail, the module will respond with a status indication of self-test error. Then, the module will go into an Error state. While in the error state, the module does not perform any operations and does not output any data.

The implementation of self-tests does not output data from the module. There is only result of self-tests output via status output interface.

After power up the module and receive the first APDU command, the module will execute Power up Self Tests automatically. If the Power up Self Tests passes, then the module process the first received APDU command, and output the normal execution result of first received APDU command. If the result of Power up Self Tests is failed, the module returns the error indicator and enters into error state. The module will never process any received APDU command afterward if the module is still in error state.

Power up self-tests could be also initiated by “FIPS KNOW ANSWER TEST” APDU command.

Known answer tests for encryption/decryption or hashing, function by encrypting (or hashing) a string for which the calculated output is known and stored within the cryptographic module. An encryption or hashing test passes when the calculated output matches the expected (stored) value. The test fails when the calculated output does not match the expected value. The test then decrypts the cipher-text string. A decryption test passes when the calculated output matches the plaintext value. A test fails when the calculated output does not match the plaintext value.

Known answer tests for Random Number Generators function by seeding the RNG with known values and checking that the output matches the pre-calculated value stored within the cryptographic module. The test passes when the generated output matches the pre-calculated value. A test fails when the generated output does not match the pre-calculated value.

7.2 Conditional Tests

RSA Key generation:

- A pair wise consistency check is performed during key generation which consists of a sign/verify operation.

  The pair wise consistency check for sign/verify calculates and verifies a digital signature. If the digital signature cannot be verified, the test fails.

Random Number Generator:

- Continuous RNG Test for the non-Approved NDRNG(HRNG, Hardware-based RNG): A continuous RNG test is performed during each use of the Hardware non-deterministic RNG to ensure that it is not generating the same value as previous one. The NDRNG is used to generate seed values to feed the DRNG.
- Continuous RNG Test for the SP 800-90A DRBG: A continuous RNG test is also performed during each use of the FIPS140-2 Approved Hash-based DRBG to ensure that it is not generating the same value as previous one.

8 Security Rules

8.1 Operational Security Rules

The following specific actions are required on the part of the Crypto Officer along with a restriction within the module usage environment to ensure the module operates in FIPS Approved mode.

1. The Crypto Officer must set all file security attribute to require a PIN for all Sign operations.
2. The Crypto Officer must set all file security attribute to require External Authenticate for all write operations.

3. The Crypto Officer must set all security attribute of key file to require External Authenticate and Key Encryption for all key update operations.
4. The Crypto Officer must set the minimum length of PIN as 8 digits.
5. The firmware of smart card inhibits the read capability of key files (except RSA public key).
6. The Crypto Officer must set the PIN Policies for the Crypto Officer and Card Holder to have a minimum length of eight bytes (characters).
7. The Crypto Officer must set the incorrect PIN counter to three failed attempts before locking the card.
8. The Card Holder must enter a valid PIN.

8.2 Physical Security Rules

The physical security of the HiCOS PKI Native Smart Card cryptographic module is designed to meet FIPS 140-2 level 3 requirements. A hard opaque epoxy is used to encapsulate the module to meet level 3 requirements. From the time of its manufacture, the card is in possession of the Crypto Officer until it is ultimately issued to the end user.

8.3 Mitigation of Attacks Security Policy

The HiCOS PKI smart card module has been designed to mitigate the following attacks:

High Frequency
High Voltage
High Temperature
Low Frequency
Low Voltage
Low Temperature
Illegal Access
Illegal Instruction
Power On Reset Function
RNG Failure

9 Security Policy Check List Tables

9.1 Roles & Required Authentication

Table 6. Roles and Required Authentication.

Role	*Type of Authentication*	*Authentication Data*
Crypto Officer	Triple-DES authentication	Triple-DES keys
User	PIN	PIN

9.2 Strength of Authentication Mechanisms

Table 7. Strength of Authentication Mechanisms.

Authentication Mechanism	*Strength of Mechanism*
PINs	The minimum length of PIN is 8 bytes and the value is not limited to digital number. Assuming that the PIN was only integers between 0-9, the probability of randomly guessing the correct sequences is 1 in 10^8.
Internal Authentication	This mechanism applies Triple-DES 3-key, the probability of randomly guessing the correct sequences is 1 in 2^{168}.
External Authentication	This mechanism applies Triple-DES 3-key, the probability of randomly guessing the correct sequences is 1 in 2^{168}.

9.3 Access Rights within Services

Table 8. Access Rights Within Services.

Service	*CSP*	*Type of Access (eg. Read, Write, Execute)*
Crypto Officer		
INTERNAL AUTHENTICATE	Triple-DES Crypto Officer Keys	Execute
EXTERNAL AUTHENTICATE	Triple-DES Crypto Officer Keys	Execute
LOAD KEY	Triple-DES Crypto Officer Keys, PIN, RSA Public/Private Key	Write
CHANGE KEY	PIN, Triple-DES Key, RSA Public/Private Key	Write
UNLOCK KEY	Triple-DES Crypto Officer Keys, PIN	Write
GENERATE RSA KEY PAIR	RSA K_{PRIV}, RSA K_{PUB}	Write
READ RECORD	RSA K_{PUB}	Read
RSA CRYPTO	RSA $\mathbf{K}_{\mathbf{PRIVSIGN}}$	Execute
User		
VERIFY PIN	PIN	Read
CHANGE KEY	PIN	Write

RSA CRYPTO	RSA $\mathbf{K}_{\mathbf{PRIVSIGN}}$	Execute
GENERATE RSA KEY PAIR	RSA K_{PRIV}, RSA K_{PUB}	Write
READ RECORD	RSA K_{PUB}	Read

9.4 Mitigation of Other Attacks

Table 9. Mitigation of Other Attacks

Other Attacks	*Mitigation Mechanism*	*Specific Limitations*
High Frequency	Countermeasures against high frequency	None
High Voltage	Countermeasures against high voltage	None
High Temperature	Countermeasures against high temperature	None
Low Frequency	Countermeasures against low frequency	None
Low Voltage	Countermeasures against low voltage	None
Low Temperature	Countermeasures against low temperature	None
Illegal Access	Countermeasures against illegal access	None
Illegal Instruction	Countermeasures against illegal instruction	None
EWE Interrupt	Countermeasures using EWE interrupt	None
Power On Reset Function	Countermeasures against Power On Reset Function attack	None
RNG Failure	Countermeasures against RNG Failure attack	None

- Low/High Frequency: a hardware clock watchdog is used to detect tampering with the clock frequency and fight power analysis attacks by discarding results during tampering.
- Low/High Voltage: an integrated voltage sensor is used to detect voltage which is outside of the operating voltage range, and shutdown the module in such instances.
- Low/High Temperature: an integrated temperature sensor is used to detect extreme temperatures at which the module is not intended to operate, and shut down the module in such instances.
- Timing Analysis, SPA, DPA, DFA Attacks: A high performance cryptographic coprocessor implementing multifunctional Advanced Cryptographic Library (ACL) is available containing secure RSA calculations, various hash functions and key generation with highest protection against all currently known attacks such as SPA (Simple Power Analysis), DPA (Differential Power Analysis), DFA (Differential Fault Analysis), timing attacks and other possible hardware or software attacks.
- Power Analysis Attacks: The module has a random current generation function which will randomly disturb the current consumption of the device while in operation. Also, the module has a random bus cycle function which inserts arbitrary dummy bus cycles as counter measures to mitigate current consumption analysis.
- EWE Interrupt: Every time the module writes to EEPROM, it generates a non-maskable interrupt (the EWE interrupt.) When this interrupt occurs, execution is passed to a user-definable address held in the EVE vector. A user can therefore add code at this location to carry out a variety of checks, for example to confirm the integrity of data, or the context in which certain areas of EEPROM are being written.
- Fault Attacks: the module is fabricated using a MONOS (Metal Oxide Nitride Oxide Silicon) EEPROM structure. MONOS advantages compared to standard EEPROM structures are high resistance to radiation disturbance, high reliability and endurance.
- RNG Failure: A Continuous RNG Test (CRNGT) is implemented to ensure that the DRBG generates a different value on each invocation.

10 Cryptographic Module References

1. Smart Card Operating System HiCOS Version 3.3 User's Manual

11 Standard FIPS References

National Institute of Standards and Technology, FIPS PUB 140-2: Security Requirements for Cryptographic *Modules*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex A: Approved Security Functions*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex B: Approved Protection Profiles*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex C: Approved Random Number Generators*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex D: Approved Key Establishment Techniques*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology and Communications Security Establishment, *Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *DES Modes of Operation*, Federal Information Processing Standards Publication 81, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-3, available at URL: http://www.nist.gov/cmvp.

NIST Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, January 2012.

NIST Special Publication 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011.