Chunghwa Telecom

Chunghwa Telecom Co., Ltd.
HICOS PKI Smart Card
Security Policy

FIPS 140-2 Level 2 Validation

Hardware: HD65145C1
HardMask: Version 1.0
SoftMask: Version 3.0

GINA Applet Version 1.0
PKI Applet Version 1.0
FISC II Applet Version 1.2

December 15, 2005
Version 1.01

1 Introduction

This document is the Security Policy for the Chunghwa Telecom Co., Ltd. HICOS PKI Smart Card. This module, hereafter called the HICOS PKI 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 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 products 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 products.

The FIPS 140-2 standard, and information on the CMV program, can be found at http://csrc.nist.gov/cryptval.

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 smart card 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 2.

Table 2 - 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

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
TDES	Triple DES (see DES)
X.509	Digital Certificate Standard RFC 2459

2 Chunghwa HICOS PKI Smart Card

2.1 Functional Overview

The HICOS PKI Smart Card cryptographic module contains an implementation of the Open Platform (OP) Version 2.0.1 specification defining a secure infrastructure for post-issuance programmable smart card chips. OP-compliant modules have a life cycle defined by the OP specification. Transitions between different life cycle states have well defined sequences of operation. 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 smart card 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 dashed outline shown.

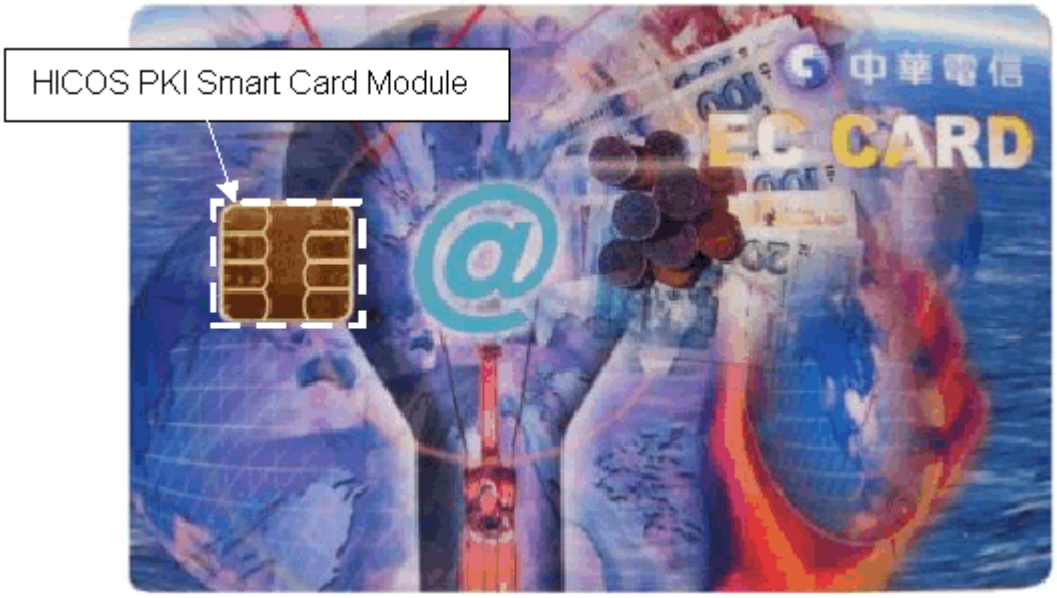


Figure 1. Physical View of the Cryptographic Module.

The HICOS PKI smart card 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 Hitachi AE45C1 smartcard IC that is validated under the Common Criteria at EAL4.

The HICOS PKI smart card module consists of the following elements:

- Renesas HD65145C1 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 and additional customized software (known as the Soft Mask). The firmware is then designated: HardMask version 1.0; SoftMask version 3.0. 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 FF 13 00 FF 00 48 69 43 4F 53 50 4B

49 43 61 72 64 30 10 02). Bold numbers in the string are the SoftMask and HardMask version identifiers.

- Three HICOS PKI smart card applets are loaded into the EEPROM of the module. The applet version can be determined by a call to the applet command GET VERSION. The module has the following applets:
  - FISCII applet version 1.2 – Provides financial information services
  - GINA applet version 1.0 – Provides a secure environment to log on to Microsoft Windows 2000 and Microsoft Windows XP operating systems
  - PKI applet version 1.0 – Provides RSA signing and verification services

Each of these providers (Applets) offers additional commands that the card supports, in addition to those commands provided by the basic resident (ROM-stored) software on the card. The resident ROM-stored software is referred to as the card manager. The Gina Applet provides support for several commands that enable the secure storage and retrieval of account and password information for login operations on Windows platforms. The FISCII Applet provides support for commands that enable credit card and ATM financial transactions over the internet. The PKI Applet provides support for signing and verification commands in support of off-card public key infrastructures. These specific applet versions are validated. Loading any other applets on the card, invalidates the validation of the card.

- 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 smart card module has a limited operational environment consisting of a Java Virtual Machine operating on a Hitachi HD65145C1 Smartcard Integrated Circuit chip. The module does not support software/firmware updates as this function is performed at the factory. The module does allow applets to be loaded, however loading of any other applets that have not been validated to FIPS 140-2 invalidates this FIPS 140-2 validation.

2.4 Module Interfaces

2.4.1 PHYSICAL INTERFACE DESCRIPTION

The HICOS PKI smart card 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.

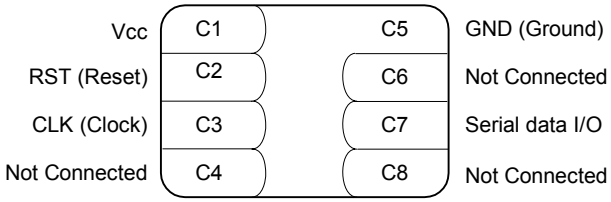
Contact dimensions are standard credit card compliant as per ISO/IEC 7816-1 standard:

Table 3. 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 4. 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 Interface
C2	RST (Reset)	Control Input Interface
C3	CLK (Clock)	Control Input Interface
C4	Not Connected to the chip	N/A
C5	GND (Ground)	Power Interface
C6	Not Connected to the chip	N/A
C7	Serial data input and serial data output.	Data Input Interface, Data Output Interface, Control Input Interface Status Output Interface
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:

- ISO/IEC 7816-4.
- Global Platform – Open Platform – Card Specification v2.0.1 – 7 April 2000.

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=0 is supported.

2.4.7 LOGICAL INTERFACE DESCRIPTION

The I/O port (C7) of the platform (refer to Table 4) 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 and soft masks 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 Open Platform 2.0.1 Specification and ISO 7816-4.

3 Roles, Services, and Authentication

3.1 Roles

The HICOS PKI smart card 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.

Through on-card applets, services are provided to the Card Holder based on his authenticating to his role. The Card Holder authenticates his role to an applet by proving knowledge of a Personal Identification Number (PIN) stored within the applet. Individual applets perform their own authentication of the Card Holder. The Global PIN is always 8 bytes. The applet PIN lengths are as follows:

- The FISC II applet PIN length is 8 bytes.
- The GINA applet PIN length is 8 bytes
- The PKI applet PIN length is 8 bytes.

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 reauthenticating in the new role. All previous authentications are cleared when the module powers down.

The HICOS PKI smart card does not allow multiple concurrent operators or support a maintenance role.

3.1.1 Cryptographic Officer Role

The Cryptographic Officer is the card administrator. The crypto officer authenticates his role on the card by demonstrating to the card manager that he possesses the knowledge of the Secure Channel Encryption Key ($\mathbf{K_{ENC}}$), Secure Channel Message Authentication Code Key ($\mathbf{K_{MAC}}$), and Key Encryption Key ($\mathbf{K_{KEK}}$) and the key ID stored within the card manager. By successfully executing a series of commands, the Cryptographic Officer establishes a secure channel to the card manager; establishment of this channel includes mutual authentication of roles between the Cryptographic Officer and the card manager. Once established, authorization (on the card) to access information and services is granted by the card manager. The card manager security domain corresponds to the card issuer security domain.

3.1.2 Card Holder

The Card Holder (User) is responsible for ensuring the ownership of his card and for not communicating his PIN. The Card Holder is authenticated by verification of a PIN selected at issuance. The PIN is provided by each applet.

3.1.3 Unauthenticated

An unauthenticated user is any unauthenticated operator having access to the host application. The operator can only select an applet and read non-security relevant card information.

3.2 Module Services

3.2.1 *Basic Module Services*

Crypto Officer Administrative Services

A crypto officer can make changes on the card or within applets 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 manager applet and using the key set to establish a secure channel. Available commands are:

DELETE: this Open Platform command is used to delete a single Load File (package) or an Application (applet instance) in the module.

ERASE ALL: this private command is used to zeroize all EEPROM contents of card.

EXTERNAL AUTHENTICATE: Open Platform command used by the module to authenticate the crypto officer, to establish a Secure Channel. A previous and successful execution of the **INITIALIZE UPDATE** command is required prior to processing this command.

GET DATA: this Open Platform command is used to retrieve a single, tagged data object from the Card Manager. Card Manager data objects are define in the OPv2.0.1 specification.

GET STATUS: this Open Platform command is used to retrieve Card Manager, Executable Load File and Application related life cycle status information according to a given search criteria.

INITIALIZE UPDATE: this Open Platform command is used to initiate a Secure Channel with the Card Manager. Card and host session data are exchanged, and session keys ($\mathbf{K_{enc}}$ & $\mathbf{K_{mac}}$) generated by the card. The Secure Channel is considered open upon completion of a successful **EXTERNAL AUTHENTICATE** command that must immediately follow the **INITIALIZE UPDATE** command.

INSTALL: this Open Platform command is used to install an application or a Security Domain and requires the invocation of several different module functions. The command is used to instruct a Security Domain or the Card Manager as to which installation step it shall perform during an application installation process.

LOAD: this Open Platform command is used to load the byte-codes of a Load File (package).

PIN CHANGE/UNBLOCK: this command is used to set the PIN value, retry limit, or retry counter of the Global PIN. The Crypto Officer establishes the secure channel for this command.

PUT DATA: this Open Platform command stores or replaces one tagged data object modifies the life cycle state of the card or the lifecycle state of an application defined in the OPv2.0.1 specification.

PUT KEY: this Open Platform command is used to add or replace Security Domain key sets. A PUT KEY command with a key-set of all 0xFF will zeroize specified Security Domain key sets.

User Services

An operator authenticates in a user role by proving knowledge of a PIN. Available commands are:

GET DATA: this Open Platform command is used to retrieve a single, tagged data object from the Card Manager. Card Manager data objects are define in the OPv2.0.1 specification.

SELECT: this Open Platform command is used for selecting an application (Card Manager or Applet).

Unauthenticated Services
Any operator with access to the host application can give some commands that do not require any authentication. These commands are:

GET DATA: this Open Platform command is used to retrieve a single, tagged data object from the Card Manager. Card Manager data objects are define in the OPv2.0.1 specification.

SELECT: this Open Platform command is used for selecting an application (Card Manager or Applet).

SELF TEST: this command will run self-tests on demand.

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 5. Basic Card Service Access Controls

Role	*Authorized Services*	*Cryptographic Keys and CSPs*	*Type(s) of Access*
Crypto-Officer	PUT DATA	None	Write
	GET STATUS	None	Read
	SET STATUS	None	Write
	INSTALL	None	Execute
	LOAD	Data Authentication Pattern Key	Execute
	DELETE	None	Execute
	PUT KEY	Encryption Key, MAC Key, Key Encryption Key	Write
	EXTERNAL AUTHENTICATE	Encryption Key, MAC Key,MAC Key	Execute
	INITIALIZE UPDATE	Encryption Key, MAC Key, MAC Key	Execute
	PIN CHANGE/UNBLOCK	Encryption Key, MAC Key, MAC Key;	Execute,
		PIN	Write
	ERASE ALL	Encryption Key, MAC Key, MAC Key	Execute, Write
	SELECT	None	Execute
User	GET DATA	None	Read
	SELECT	None	Execute
Unauthenticated	SELECT	None	Execute
	GET DATA	None	Read
	SELF TEST	None	Execute

3.2.2 *GINA Applet Services*

The Gina applet provides users a secure environment to log on to Microsoft Windows 2000 and Windows XP operation systems. The applet manages login information (an account name and a password) in an on-card data store.

The GINA applet services are:

SELECT APPLET: This APDU is used to select the area in which user account, password and domain name information is stored within this applet.

READ RECORD: Read data from smart card by this applet.

UPDATE RECORD Modify data on the smart card.

VERIFY PIN: Check the accuracy of the PIN CODE which user types, comparing it with the PIN CODE stored in the smart card by this applet.

APPEND RECORD: This APDU is used to insert data to smart card by this applet.

CHANGE APPLET PIN: This APDU is used to change the old PIN CODE stored in the smart card by this applet to the new one input by user.

UNLOCK APPLET PIN: This APDU is used to unlock the PIN while PIN is locked.

GET APPLET VERSION: This APDU is used to return this GINA applet's version.

GET APPLET STATE: This APDU is used to return this GINA applet's state.

PERSONALIZE APPLET: This APDU is used to initialize the applet.

INITIALIZE UPDATE: This APDU is used to initialize the secure channel. This command must combine with "Secure channel EXTERNAL AUTHENTICATE" command to build up a complete secure channel.

EXTERNAL AUTHENTICATE: This APDU is used to do an external authentication to build a secure channel.

The authenticated card holder has access to GINA applet services. The services, in turn, may use or operate on cryptographic keys or critical security parameters (CSPs). The following table shows the relationship between roles and services, and indicates the type of access provided to various cryptographic keys and CSPs. In cases where the Cryptographic Keys and CSPs are "None", the Type(s) of Access identifies the type of operation.

Table 6. GINA Applet Service Access Controls

Role	*Authorized Services*	*Cryptographic Keys and CSPs*	*Type(s) of Access*
Crypto-Officer	UNLOCK APPLET PIN	PIN	Execute
	PERSONALIZE APPLET	Encryption Key, MAC Key, MAC Key	Execute
	INITIALIZE_UPDATE	Encryption Key, MAC Key, MAC Key	Execute
	EXTERNAL_AUTHENTICATE	Encryption Key, MAC Key, MAC Key	Execute
User	VERIFY PIN	PIN	Execute
	SELECT APPLET	None	Execute
	APPEND RECORD	None	Write
	UPDATE RECORD	None	Write
	READ_RECORD	None	Read
	CHANGE APPLET PIN	PIN	Write
	GET APPLET VERSION	None	None
	GET APPLET STATE	None	Read
	INITIALIZE_UPDATE	Encryption Key, MAC Key, MAC Key	Execute
	EXTERNAL_AUTHENTICATE	Encryption Key, MAC Key, MAC Key	Execute

3.2.3 *PKI Applet Services*

The PKI applet provides RSA sign and verify services to authenticated users. The PKI applet services are:

SELECT FILE: Select file from the PKI Applet storing the key or PIN values. This may be an RSA public key file, private file, or certificate file.

CREATE FILE: Create file accessible to the PKI Applet.

READ BINARY: Read binary data from a Transparent EF (elementary file).

UPDATE BINARY: Write binary data into a Transparent EF.

VERIFY PIN: Verify the PIN value presented by user with the PIN value stored inside the PKI Applet.

UNBLOCK PIN: Unblock the user PIN.

INITIALIZE UPDATE: This APDU is used to initialize the secure channel. This command must combine with "Secure channel EXTERNAL AUTHENTICATE" command to build up a complete secure channel.

EXTERNAL AUTHENTICATE: This APDU is used to do an external authentication to build a secure channel.

GENERATE KEY PAIR: Create a new RSA key pair.

GENERATE HASH: Create a HASH (SHA-1) of the given data.

RSA CRYPTOGRAPHY: Compute RSA Modulus Exponentiation with an RSA public key or private key.

PERSONALIZE APPLET: This command is used to initialize the applet.

READ RECORD: Read RSA public key form an RSA public key file.

UPDATE RECORD: Import/update RSA public/private key form an RSA public/private key file.

CHANGE PIN: Change the user PIN

GET VERSION: Get the version of the PKI Applet

GET STATUS: Get the life cycle of the PKI applet

DELETE FILE: Delete file created by CREATE FILE command.

The authenticated card holder has access to PKI applet services. The services, in turn, may use or operate on cryptographic keys or critical security parameters (CSPs). The following table shows the relationship between roles and services, and indicates the type of access provided to various cryptographic keys and CSPs. In cases where the Cryptographic Keys and CSPs are "None", the Type(s) of Access identifies the type of operation.

Table 7. PKI Applet Service Access Controls

Role	***Authorized Services***	***Cryptographic Keys and CSPs***	***Type(s) of Access***
Crypto-officer	SELECT FILE	None	Execute
	CREATE FILE	None	Write
	READ BINARY	None	Read
	UPDATE BINARY	None	Write
	UNBLOCK PIN	PIN	Execute
	PERSONALIZE APPLET	None	Execute
	UPDATE RECORD	RSA Public/Private Key Pair	Write
	GENERATE HASH	SHA-1	Execute
	CHANGE PIN	PIN	Write
	GET VERSION	None	Read
	GET STATUS	None	Read
	DELETE FILE	None	Execute
	INITIALIZE_UPDATE	Encryption Key, MAC Key, MAC Key	Execute
	EXTERNAL_AUTHENTICATE	Encryption Key, MAC Key, MAC Key	Execute
User	SELECT FILE	None	Execute
	VERIFY PIN	PIN	Execute
	READ RECORD	RSA Public Key	Read
	READ BINARY	None	Read

	GENERATE KEY PAIR	RSA Public/Private Key Pair	Execute
	RSA CRYPTOGRAPHY	RSA Public/Private Key Pair	Execute
	GENERATE HASH	SHA-1	Execute
	GET VERSION	None	Read
	GET STATUS	None	Read
Unauthenticated	SELECT FILE	None	Execute
	READ BINARY	None	Read
	GET VERSION	None	Read
	GET STATUS	None	Read
	GENERATE HASH	SHA-1	Execute

3.2.4 *FISC II Applet Services*

The FISC II Applet provides financial information services in Taiwan following FISC (Financial Information Services Company) Specification Version II. All of the keys in this applet are issued by the financial institution (bank). The FISC II applet services (APDUs) are:

SELECT APPLET. Select this applet instance. This is the first command for Card Manager. The applet fixed ID is A000000172950001h.

GET APPLET VERSION. Get applet version number. Response is one byte: 0x12.

SELECT FILE. Select an EF by file ID.

INITIALIZE UPDATE: This APDU is used to initialize the secure channel. This command must combine with “Secure channel EXTERNAL AUTHENTICATE” command to build up a complete secure channel.

EXTERNAL AUTHENTICATE: This APDU is used to do an external authentication to build a secure channel.

READ RECORD. Read one or more records of an EF.

WRITE RECORD WITH SNUM AND TAC. Write a record with a transaction serial number (SNUM) and transaction authentication code (TAC).

UPDATE RECORD. Update the date of a record.

GENERATE RANDOM. Generate an 8-byte random number.

TERMINAL AUTHENTICATION. Authenticate with a terminal. This command must execute the GENERATE RANDOM command first.

VERIFY PIN. Verify the card holder PIN code.

UNLOCK KEY/PIN. Unlock a blocked key set or PIN code. Used when PIN is locked due to 3 incorrect attempts or when key set is locked due to 2 incorrect attempts.

SET SESSION KEY. Set the session key.

UPDATE/WRITE RECORD CIPHERED. Update or write record with ciphered data.

Table 8. FISCII Applet Service Access Controls.

Role	***Authorized Services***	***Cryptographic Keys and CSPs***	***Type(s) of Access***
Crypto-officer	UNLOCK KEY/PIN	PIN, Encryption Key, MAC Key, MAC Key	Execute
User	SELECT APPLET	None	Read
	GET APPLET VERSION	None	Read
	SET SESSION KEY	Session Key	Write

	UPDATE/WRITE RECORD CIPHERED	Session Key	Write
	UPDATE RECORD	None	Write
	TERMINAL AUTHENTICATION	None	Write
	SELECT FILE	None	Read
	READ RECORD	None	Read
	WRITE RECORD WITH SNUM AND TAC	None	Write
	VERIFY PIN	PIN	Execute
	GENERATE RANDOM	None	Execute
	INITIALIZE_UPDATE	Encryption Key, MAC Key, MAC Key	Execute
	EXTERNAL_AUTHENTICATE	Encryption Key, MAC Key, MAC Key	Execute
Unauthenticated	SELECT APPLET	None	Read
	GET APPLET VERSION	None	Read
	SELECT FILE	None	Execute
	READ RECORD	None	Read
	GENERATE RANDOM	None	Execute

3.3 Authentication

3.3.1 Triple DES keys

Each of the three-key Triple DES keys used by the CO has an effective key length of 112 bits (which is 2^{112} possible keys per key or 2^{348}). As all three keys are required, this far exceeds the 1 in a million test requirement.

To try a key against the module, 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 Triple DES key 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. 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^{348} 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.

3.3.2 Global PIN and User PIN

The length of the Global PIN and the User PIN is a string of 8 digits. PINs contain the digits 0 to 9 yielding a maximum of 100,000,000 possible PINs. This far exceeds the 1 in a million test.

An 8-bit counter internal to the Access Control applet 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. This far exceeds the requirement of 1 in 100,000 for multiple attempts in a 60 second interval.

4 FIPS-Approved Mode of Operation

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

1. Pre-Personalize the HICOS PKI smart card by the following steps.

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 the PUT KEY command to generate a new key set;
3. Select the issuer security domain;
4. Load the applet verification key into the Card Manager;
5. Create a secure session using the INITIALIZE UPDATE and EXTERNAL AUTHENTICATE commands
6. Issue the PUT KEY command to create a new Applet Verification Key;
7. Set the Applet Verification Secure Domain to the Personalization State;
8. Configure the applets by:

   a. setting a cardholder PIN.

From this point, the module and applets are in FIPS approved mode.

5 Module Cryptographic Functions

The purpose of the HICOS PKI smart card module is to provide a FIPS validated module for applets that may in turn provide cryptographic services to end-user applications. 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 smart card module to provide cryptographic services; these include:

- TDES for establishing a secure channel, and encrypting keys input to the module using the PUT KEY command within the secure channel.
- HMAC-SHA1 used for integrity-protecting data sent within the secure channel.
- AES for encrypting data stored within the applet.
- RSA Sign and Verify.
- SHA-1 Hashing.
- RNG used for cryptographic key generation.

Details of cryptographic functions are shown in this table:

Table 9. Module Cryptographic Functions.

Type	Algorithm	FIPS-Approved	Certificate
Public Key	RSA. Key size: 1024 bits.	Yes (FIPS 186-2)	72
Symmetric Key	TDES (ECB, CBC) 2 keys TDES. Key size 128 bits. TDES (ECB, CBC) 3 keys TDES. Key size 192 bits.	Yes (FIPS 46-3)	355
	HMAC-SHA1	Yes (FIPS 198)	87
	AES (CBC) Key Sizes 128,192,256 bits.	Yes (FIPS 197)	272
Digest	SHA-1	Yes (FIPS 180-1)	357
RNG	DRNG (FIPS 186 appendix 3.1)	Yes (FIPS 186-2)	107
	NDRNG (HARDWARE RNG)	No	

6 Cryptographic Key Management

The module contains a variety of keys and CSPs defined by the Global Platform specification and by the applet design documents. The module does not input or output plaintext cryptographic key components, plaintext authentication data, or other unprotected CSPs.

6.1 Crytographic Keys

The HICOS PKI smart card module includes the following keys:

- Initialization Key, $\mathbf{K_{init}}$ Triple DES key (128 bits) used only for the first Card Manager key-set loading.
- Applet Load Key, $\mathbf{K_{ALD}}$ Triple DES MAC key used to create a MAC on an applet loaded on the smart card to verify its authenticity.
- Crypto Officer Security Domain double-length keys ($\mathbf{K_{ENC}}$, $\mathbf{K_{MAC}}$, & $\mathbf{K_{KEK}}$).

A Security Domain key set is structured to contain three types of TDES keys:

a. $\mathbf{K_{ENC}}$, used to generate TDES session key $\mathbf{K_{enc}}$ for the encrypted mode of the secure channel,
b. $\mathbf{K_{MAC}}$, used to generate TDES session key $\mathbf{K_{mac}}$ for MAC mode of the secure channel authentication,
c. $\mathbf{K_{KEK}}$, used to encrypt keys to be imported into the module.

Security Domains allow a number of distinct identities to be established on the HICOS PKI smart card module. These identities control access to the various applets stored on the module. A Security Domain represents the identity of the Crypto Officer.

6.2 Public Keys

Public and private keys can be generated on the card using the PKI applet GENERATE KEY PAIR command. Alternatively the keys may be loaded onto the card using the UPDATE RECORD command.

$\mathbf{K_{SIGN}}$ (PKI Key pair)

- RSA Public Sign Key, $\mathbf{K_{PUBSIGN}}$ for signature verification operations.
- RSA Private Key for Sign operations $\mathbf{K_{PRIVSIGN}}$

6.3 Cryptographic Key Generation

RSA key pairs may be generated using the GENERATE KEY PAIR (PKI applet) function along with a key ID. The public key is returned from the function 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 PKI container, is used to establish the identity of the Card Holder by verifying a digital signature.

RSA key pairs, TDES and AES keys are generated according to FIPS 186-2 Appendix 3.1. A key is produced by the on board hardware RNG and that is used as input to the deterministic PRNG. The module does not use an optional seed. The function G is calculated using SHA-1.

6.4 Cryptographic Key Entry

Security Domain Keys are input to the Card Manager in encrypted format, using the PUT KEY command within a secure channel. During this process, the keys are double encrypted (using the TDES Session Key $\mathbf{K_{enc}}$ and the $\mathbf{K_{KEK}}$ 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 PKI applet container. The private-key, which is retained securely within the PKI container, is used to establish the identity of the Card Holder by forming a digital signature.

6.5 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:

- $\mathbf{K_{ENC}}$ (TDES Encryption Key)
- $\mathbf{K_{MAC}}$ (TDES MAC Key)

- **K_{KEK}** (TDES Key Encryption Key)
- **K_{ALD}** (TDES MAC Applet Load Key)

Symmetric session keys reside in RAM only and become invalid when a secure channel session ends.

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

6.6 Cryptographic Key Destruction

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

The PUT KEY command can be used to zeroize the crypto-officer key set by specifying a key value of all “F”s for all crypto-officer keys.

7 Self Tests

7.1 Power Up Self Tests

The HICOS PKI smart card module performs the required set of self-tests at power-up time. 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:

- RAM functional test and clearing at Reset
- Firmware integrity check (CRC32)
- Algorithm (known answer) tests for:
  - TDES (CBC mode encrypt/decrypt)
  - TDES MAC
  - AES (CBC mode encrypt/decrypt)
  - HMAC (using the $K_{(MAC)}$ key)
  - RSA PKCS1 sign and verify
  - DRNG

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.

No data of any type is transmitted from the module to the reader while self-tests are being performed. The firmware self-test operations do not implement any capability to output data from the module. The only output is status data indicating self-test success or failure**.** If the self-test operation is successful, the module will execute the first received APDU command, and output the normal execution result of first received 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 ciphertext 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:

- HRNG: A continuous RNG test is performed during each use of the Hardware non-deterministic RNG to verify that it is not generating the same value. The HRNG is used to generate seed values to feed the DRNG.
- DRNG: A continuous RNG test is also performed during each use of the FIPS140-2 approved deterministic RNG to verify that it is not generating the same value.

Software/Firmware load test

- A TDES CBC MAC is verified each time an applet is loaded onto the HICOS PKI Smart Card module. (Only validated applets may be loaded onto the HICOS PKI Card. Loading of non-validated applets will invalidate the module's FIPS 140-2 Certification.) The HiCOS PKI Smart Card does not support firmware upgrades. This has to be performed at the factory.

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 instantiate all card applets to require a PIN for all Sign operations.
2. The Crypto Officer must instantiate all container applets to require External Authenticate or Global Platform secure channel for all write operations.
3. The Crypto Officer must set the PIN Policies for the crypto officer and Card Holder to have a minimum length of eight bytes (characters).
4. The Crypto Officer must set the incorrect PIN counter to three failed attempts before locking the card.
5. The Card Holder must enter a valid PIN.
6. The Card Holder must generate or upload an RSA key pair to configure the PKI applet to generate or verify digital signatures.
7. For key and CSP zeroization purposes, a crypto officer may use the ERASE ALL command

8.2 Physical Security Rules

The physical security of the HICOS PKI smart card 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 module has security logic which detects any condition that is outside of normal operational parameters. When one of these conditions occurs, all internal functions are reset, which zeroizes the module. The module must be reinitialized as per Section 4 of the Security policy. The operational parameters for temperature, voltage, and frequency are as follows;

Temperature: -25 to +85oC
Frequency: 1MHz - 10MHz
Voltage: 2.7V - 5.5V

When one of these conditions occurs, the module performs a power cycle.

Illegal Access
Illegal Instruction
EWE Interrupt
Power On Reset Function
RNG Failure

9 Security Policy Check List Tables

9.1 Roles & Required Authentication

Table 10. Roles and Required Authentication.

Role	*Type of Authentication*	*Authentication Data*
Crypto Officer	TDES authentication	TDES keys (Crypto Officer Security Domain) $\mathbf{K_{ENC}}$, $\mathbf{K_{MAC}}$ & $\mathbf{K_{KEK}}$
User	PIN	Global PIN, Card Holder PIN

9.2 Strength of Authentication Mechanisms

Table 11. Strength of Authentication Mechanisms.

Authentication Mechanism	*Strength of Mechanism*
TDES authentication	High (Far exceeds the 1 in a million test)
PIN-based authentication	High (Far exceeds the 1 in a million test)

Access Rights within Services

Table 12. Access Rights Within Services.

Service	*CSP*	*Type of Access (eg. Read, Write, Execute)*
Crypto Officer		
EXTERNAL AUTHENTICATE (Secure Channel)	TDES Crypto Officer Keys	Execute
PUT KEY	TDES Crypto Officer Keys	Write
PIN CHANGE/UNBLOCK	TDES Crypto Officer Keys	Write
User		
Verify PIN	Card Holder PIN	Read
RSA CRYPTO	RSA $\mathbf{K_{PRIVSIGN}}$	Execute
RSA CIPHER	RSA $\mathbf{K_{PRIVSIGNF}}$	Execute

9.3 Mitigation of Other Attacks

Table 13. 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 against EWE interrupt	None
Power On Reset Function	Countermeasures against Power On Reset Function attack	None
RNG Failure	Countermeasures against RNG Failure attack	None

10 Cryptographic Module References

1. Application Programming Interface Java Card™ Platform, Version 2.2.1 – October 21, 2003.

2. Global Platform – Open Platform – Card Specification v2.0.1 – 7 April 2000.

3. Appendix One of Financial Information System Design Specification V1.4 – 1 August 2003

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 180-1, available at URL: http://www.nist.gov/cmvp.