Cryptographic Module Security Policy for the

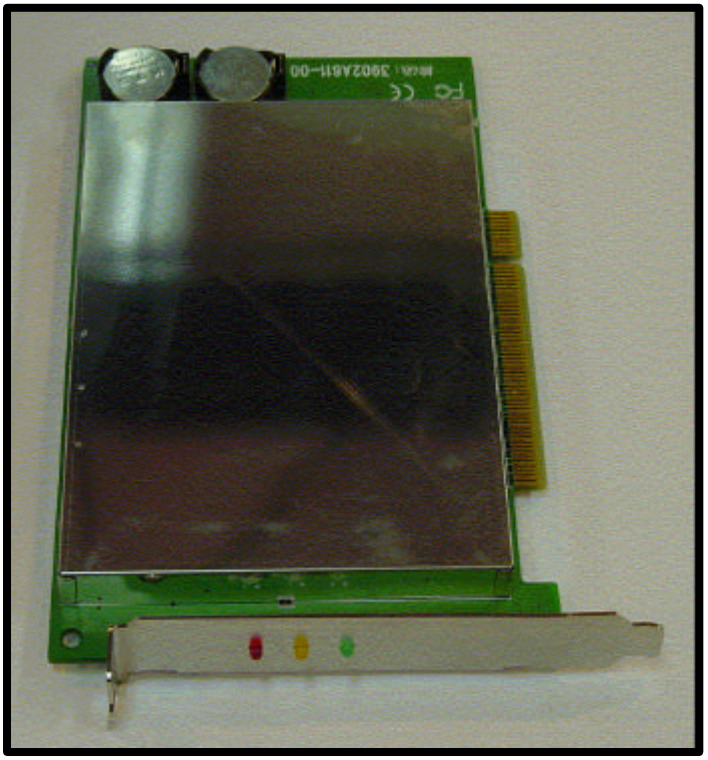
NST Security CryptoCard 2200(CC2200)

(Hardware Version 1.0; Firmware Version 1.0)

Version: 1.7

FIPS 140-1 Level 3 Validation

FIPS 140-1 Non-Proprietary Cryptographic Module Security Policy



***N**etwork **S**ecurity **T**echnology (**NST**) Co.*
5F, No.31, Sec. 1, Chung-Hsiao E. Rd., 100 Taipei Country Taiwan, ROC
TEL: 886-2-23938218 FAX: 886-2-2393-8659
E-MAIL: nst@nst.com.tw WEB: http://www.nst.com.tw

Table of Contents

1. Introduction

In FIPS 140-1 terminology the ***NST*** Security CryptoCard CC2200 is a "multi-chip embedded cryptographic module" that provides hardware cryptographic services to users, groups or processes. The ***NST*** Security CryptoCard is a 32-bit PCI adapter card that takes the PCI slot of a host server to provide hardware cryptographic services such as acceleration for bulk data encryption/decryption, digital signature generation/verification, secure key storage and key management to its clients.

This security policy specifies the security rules under which the ***NST*** Security CryptoCard shall operate, including an Identification and Authentication (I&A) policy, an access control policy, and a physical security policy. In the subsequent contents, the ***NST*** Security CryptoCard is referred to as the "CryptoCard", "CC2200", or simply "the module". Additionally, since there are two separate roles defined in the operation of the CryptoCard (Crypto-officer and User), the module defines that an operator is either a Crypto-officer or a User who is authorized to perform some specific cryptographic services.

2. Rules of Operation

All ***NST*** Security CryptoCards are delivered with a factory-set default ID/password pair for the Crypto-officer. This implies that the module uses factory-set default authentication and authorization information to determine whether the operator can assume the Crypto-officer role the first time an operator attempts to access the module. The module contains one and only one Crypto-officer account. A Crypto-officer account cannot be added or deleted. Once the module is received, it is recommended that the Crypto-officer follow the steps described below for secure operation before creating User accounts and performing parameter setups. The Crypto-officer can begin to configure the module only after the module has passed all power-on self-tests.

- Verify that the Crypto-officer has received the factory pre-set Crypto-officer's ID/password
- Crypto-officer should change the pre-set password after configuring the module
- Crypto-officer may optionally generate a Triple DES system key during configuring the module

It is the responsibility of the Crypto-officer to create or delete User accounts. The Crypto-officer assigns a default password when he creates a User account for an operator. The Crypto-officer should educate Users as to proper operation of accounts, this may include:

- Each User should securely and separately receive an ID/password
- Users should change passwords upon received them
- Users should not expose passwords to others
- Users should change passwords periodically

It is recommended that Users and the Crypto-officer should archive their own keys and security sensitive parameters periodically after the Crypto-officer has configured the module.

The Crypto-officer should educate the Users to archive their own keys periodically to ensure that they will operate in a safe manner. Since the module meets all FIPS 140-1 level 3 requirements, plain text keys and critical security parameters stored in the Secure Memory are zeroized when it detects any tampering attempted to the module. Therefore, the Crypto-officer should be aware that under no circumstances can he/she or the Users access the security sensitive parameters stored in the module by physically attacking the module.

2.1 Cryptographic Module

The ***NST*** Security CryptoCard CC2200 is a 32-bit PCI adapter card integrated with a computer with PCI slot. It could provide hardware cryptographic services such as acceleration for data encryption / decryption, digital signature generation / verification, message digest and message authentication to its clients. In addition, the CC2200 also provides a secure operation and management environment during the life cycle of

cryptographic keys in the module. The CC2200 possesses quite a few special physical security and logical security design features: for example, the tamper resistant circuitry, identity based authentication and service access control. The block diagram with major components of the CryptoCard is shown in Figure 1.

The ***NST*** Security CryptoCard, a "multi-chip embedded cryptographic module" in FIPS 140-1 terminology, is designed to meet Federal Information Processing Standard Publication (FIPS PUB) 140-1 level 3 cryptographic module requirements defined by the validation authorities of the Cryptographic Module Validation Program (CMVP): U.S Government's National Institute of Standards and Technology (NIST) and Communications Security Establishment (CSE) of the Government Canada. The FIPS140-1 cryptographic boundary is the entire Security CryptoCard CC2200 module, excluding the batteries.

2.2 Module Interface

Physical Interfaces

The ***NST*** Security CryptoCard CC2200 has two physical interfaces. The primary physical interface is a standard PCI bus interfacing to the PCI slot of a motherboard inside the host or server. Another physical interface is the power interface to the primary Lithium battery set outside the tamper resistant metal case.

There is no direct access interface to the internal Secure Memory and run time memory for storing temporary variables through PCI bus. The central processor of the module controls the access of the I/O buffer between the CC2200 and host. The access of the other internal memory access is protected and controlled by the processor. For each input command request to the module, the only physical entry point of the CryptoCard is PCI bus. Refer to Figure 1 for the block diagram of CC2200.

The input and output data interfaces of the CryptoCard share the same physical PCI interface for all applications. The proper interaction between the CryptoCard and the host side application by the control of I/O data buffer, control register, and status register ensures the correct data transmission. The contents passing the physical I/O interface include cipher text data, cryptographic keys, security sensitive parameters, key management data, authentication data, command return code, the other input and corresponding output data. The sending side sets the control register for data input ready signal, and the receiving side monitors the status register signal for detecting the sender's input data ready to be retrieved in the I/O buffer.

Besides the I/O interface, the Secure CryptoCard CC2200 has other two control input interfaces. One is the input signal pin for the zeroization of secure memory when the tamper circuit to the CryptoCard breaks, the other one is the hardware reset control signal pin of the CryptoCard.

Additionally, the module has two status output interfaces as well. One is the port to indicate low battery power status occurrence, the other one is the combination of two LED ports to indicate the errors occurring and the current state of the module.

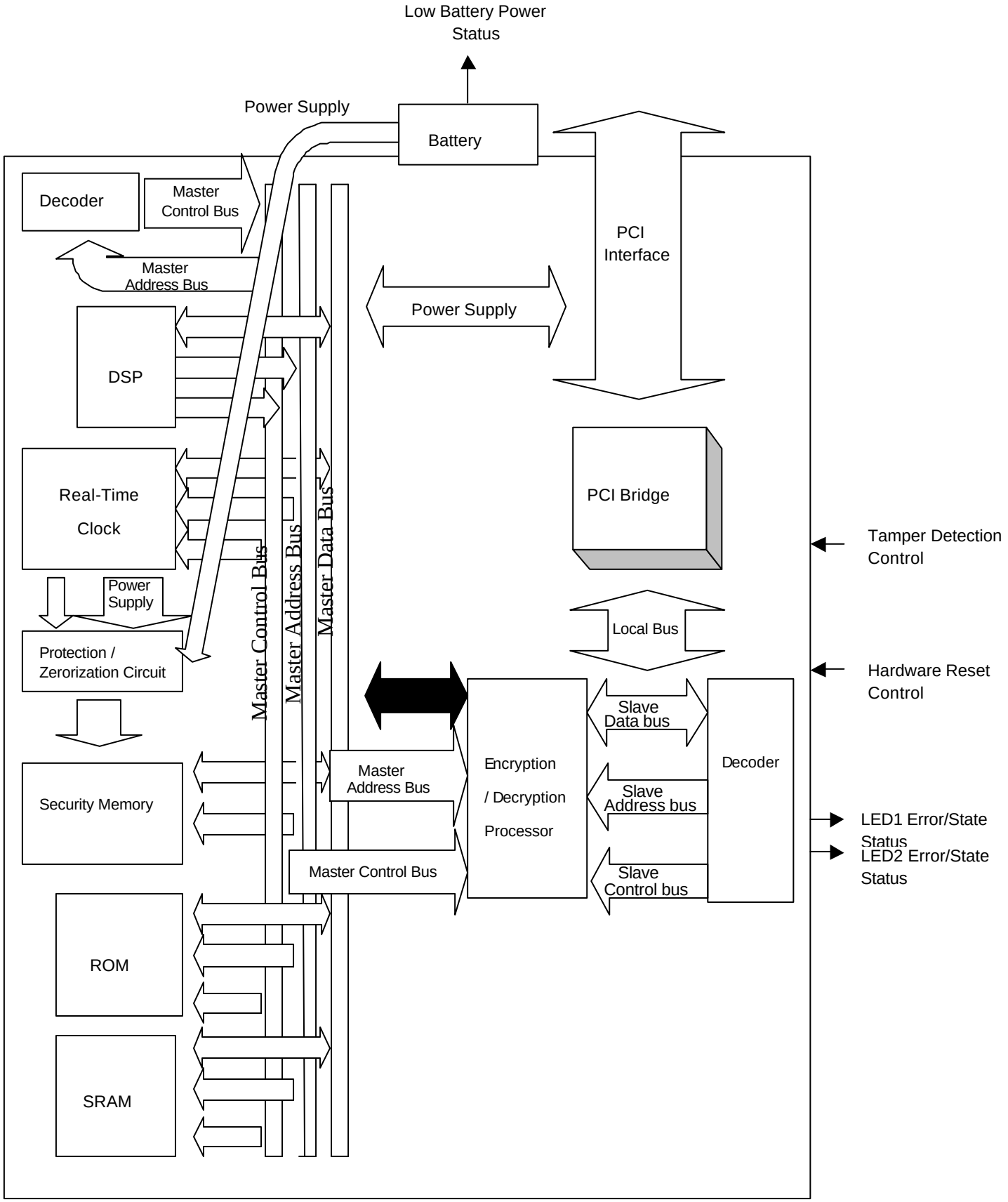


Figure 1 –Block Diagram of the Cryptographic Module CC2200

The relationship between logical interfaces and physical ports of CC2200 could be summarized in the table as follows:

Logical Interfaces	Physical Ports of CC2200
Data Input Interface	PCI bus
Data Output Interface	PCI bus
Control Input Interface	PCI bus, Tamper detection pin, hardware reset control pin
Status Output Interface	PCI bus, Low battery power status pin, Error/State indication pins (2)
Power Interface	PCI bus

Table 1 – Relationship between logical and physical interfaces of CC2200

The logical interfaces of the module that share the PCI physical port as kept separate by a combination of the PCI bus protocol and strict separation of the logical interfaces in the module firmware. The separate simultaneous user sessions are kept separate by splitting them into different logical sessions. The information from different logical sessions is kept logically separate, and is differentiated by distinct encryption session keys.

In our design, there are no cryptographic keys, authentication data, or critical security parameters passing through the I/O ports in plaintext format. This confidential data is encrypted by the session key, which is built between the CryptoCard and the software using the CryptoCard as the host side. The secure logical session is described in the next section.

Secure Logical Sessions

The data I/O security of the logical interface is based on the logical ciphering session built between CC2200 and the application of the interfacing host. The module interfaces are logically distinct from each other, since every distinct logical secure session is encrypted and maintained by a unique session key, the common secret, between CryptoCard and the host side application. The details to build the secure encryption channel after mutual authentication are depicted in the Section “Identification and Authentication (I&A) Policy”.

2.3 Identification and Authentication (I&A) Policy

The approach we adopt to authenticate an operator to the module is the “Identity-Based Authentication”, which satisfies FIPS 140-1 level 3 authentication requirements. Before operators can use the cryptographic module, they must perform the authentication action with their ID and password. After the authentication successfully completed, a secure communication session is established between the operator and module, thereafter kept alive until the operator logs out or the communication session is abnormally terminated. This is referred to as simply “the session” in this Security Policy.

In the CryptoCard, the strength of identification mechanism is based on two factors. One is the strength of the mutual authentication scheme based on challenge-response principles. The other is the strength of the password used in the authentication

procedures. When the CryptoCard receives a login request for a given user the CryptoCard derives a DES key (authentication key) from that user's log-in ID and stored password. The User's software derives a DES key from the log-in ID and password that the User provides. The module then uses the challenge-response protocol to make sure that both sides have derived the same secret key from the log-in ID and password. The challenge-response protocol is well known and has sufficient authentication strength; password security management is more dependent on the operators themselves, relatively. The references for password management are addressed in FIPS PUB 112 and U.S. Department of Defense password management guideline [1].

The Identity-Based Authentication is described as follows in terms of the authentication data and the authentication action:

Authentication Data Requirements

There is one and only one operator who can assume the Crypto-officer role. That is, there is only one operator account defined for the Crypto-officer role in the module. A Crypto-officer account cannot be added or deleted. A factory pre-set ID/password for the Crypto-officer role is assigned before the CryptoCard is delivered to the buyer. This ID/password is the same for every CryptoCard. Once buyers have received the CryptoCard and the factory pre-set ID/password, they should use it to log on to the module for the first time and change the password to their own.

Role	ID Content	Password Content	Restrictions and Requirements
Crypto-officer	Numeric, alpha or both	Numeric, alpha or both	Password is from eight to sixteen bytes in length One and only one Crypto-officer account exists Crypto-officer account can not be added and deleted Crypto-officer can modify his/her own password Crypto-officer can create and delete User accounts Crypto-officer can assign initial password to User Crypto-officer can not modify User's password
User	Numeric, alpha or both	Numeric, alpha or both	Password is from six to sixteen bytes in length One or more User account exists User can not create or delete Crypto-officer account User can not create or delete any User account User can only modify his/her own password

Table 2 – Authentication data material, restrictions and requirements

There are minimum password length requirements. For regular users, the password should be at least six-byte numeric or alpha characters. For the Crypto-officer, the minimum password requirement is at least eight bytes.

Identity-Based Authentication

The information required for an operator to authenticate himself to the module is the authentication data --- ID and password. These are not directly passed to the CryptoCard. The mutual authentication scheme is based on the challenge-response protocol. Since the CryptoCard intends to meet the security requirements of FIPS

140-1 at level 3, the password, being a security sensitive parameter, will not pass to the module through the cryptographic boundary directly. Both the host side software and the module's firmware shall perform the same ID and password based authentication procedures to generate a DES key (authentication key), for the mutual authentication between host side and the CryptoCard side. Once the authentication key is generated on the both sides, the challenge/response protocol proceeds to make sure both sides derived the same authentication key from the logon ID and password. The individual challenge of the host side and the CryptoCard is the nonce randomly generated by the distinct random number generators of both sides. At the same time, the session key is built for the data content encryption and decryption between the host side and the CryptoCard during this User session. The session keys are generated by the Diffie-Hellman key agreement algorithm between the Crypto Module and the software using the CryptoCard. The session keys are generated by the CryptoCard and the software of host side by the mutual exchange of Diffie-Hellman public keys calculated from the randomly generated Diffie-Hellman private keys of each side. The session key is generated during the mutual authentication procedures between the Crypto Module and its user.

Every User who is allowed to access the module must have a unique ID/password pair created and assigned by the Crypto-officer. Operators are required to enter their ID/password when they wish to use the cryptographic services of the module. All of the ID/passwords stored in the Secure Memory of the CryptoCard are in plain text since the tamper resistance mechanism is built into the module to prevent any possibility of externally probing data from the module's internal memory buses.

Only the Crypto-officer has the privileges to manage information on the User accounts, hence, the Crypto-officer can create or delete a User account for an operator. After the Crypto-officer has created a new User account for an operator, and assigned the unique ID/password pair, the account's authorization to access the services of the module is determined by the defined privileges of the User role of the module.

Since only the Crypto-officer has the privileges to create User accounts, he may create one for himself. Whenever the Crypto-officer wants to operate in a User role, the operator must logon under his regular user account. If the Crypto-officer has already logged in as the Crypto-officer role, he must first logout and later re-logon as his User, when he wishes to change roles from Crypto-officer to User.

2.4 Access Control Policy

Services and Critical Security Parameters of CryptoCard

The service category and functions provided by the CryptoCard are listed in Table 3. The related Critical Security Parameters (CSP) for these service functions include

- account passwords,
- global cryptographic key of the module (System Key),
- cryptographic keys of the legitimate accounts (Crypto-officer and User roles),
- cryptographic key attributes

The types of access to these CSPs, for example, reading or writing, and the accessible CSPs, are summarized in the following table.

Service	Functions	Accessible CSPs		Type of Access (C//W/R/U/D/A/E)
		Key	Password	
Key management	Key and parameter entry	✓		C
	Key generation	✓		C
	Key output	✓		R
	Key archiving	✓		A
	Key zeroization / Destruction	✓		D
	Key update	✓		U
	Key distribution	✓		R
	Key identifiers query	✓		R
	Key attributes query	✓		R
Cryptographic management	Initialization/Configuration			W
	Alarm handling and resetting			E
	Serial number query			R
	Local time setting			U
Show status	Version information			R
	Error code while in error state			R
Selectable Self-tests	Cryptographic algorithm tests			E
	Firmware tests			E
	Critical functions tests			E
	Statistical random number generator tests			E
Cryptographic operations	Encryption (Symmetric Key)	✓		E
	Decryption	✓		E
	Digital signature generation	✓		E
	Digital signature verification	✓		E
	Hash			E
	Random number generation			E
User management	Add User Account / Initiate Password		✓	C
	Delete User Account		✓	D
	Password Update		✓	U
	User Identifier Query			R

Table 3 – Summary of Services, functions, access type and CSPs

[Note] **Access Type**

"C" implies "Create" "W" implies "Write" "R" implies "Read" "U" implies "Update"
"D" implies "Delete" "A" implies "Archive" "E" implies "Execute"

Defined Roles and corresponding Services

Once an operator successfully logs on to the CryptoCard, the module will implicitly assume the role of the logged on user automatically since each operator's account can be only one specific role in the module.

In the CryptoCard, two roles are identified:

- Crypto-officer role, and
- User role

- **Crypto-officer Role**

The role assumed by an authorized Crypto-officer performs a set of cryptographic initialization or management functions (e.g., user management, initialization of CryptoCard, cryptographic management). There is one and only one operator account that can be the Crypto-officer role of the module.

- **User Role**

The role assumed by an authorized User obtains security services, performs cryptographic operations, or other authorized functions. All of the legitimate accounts in the CryptoCard are defined as a User role except the unique Crypto-officer.

The table below is the description of each distinct role, including its name, purpose and services that are performed in the role and the major services allowed for the corresponding role.

Role	Number of accounts	Purpose	Services	Functions	Permission
Crypto-officer	One	To perform a set of cryptographic initialization and management functions	• Key management	• Key and parameter entry	✓
				• Key generation	✓
				• Key output	✓
				• Key archiving	✓
				• Key zeroization/destruction	✓
				• Key update	✓
				• Key identifiers query	✓
				• Key attributes query	✓
			• Cryptographic management	• Initialization / Configuration	✓
				• Error handling and resetting	✓
				• Serial number query	✓
				• Local time setting	✓
			• Show Status	• Version information	✓
				• Error code while in error state	✓
			• Selectable self-tests	• Cryptographic algorithm tests	✓
				• Firmware tests	✓
				• Critical function tests	✓
				• SRNG tests	✓
			• Cryptographic operations	• Encryption	✓
				• Decryption	✓
				• Digital signature generation	✓
				• Digital signature verification	✓
				• Hash	✓
				• Random number generation	✓
			• User management	• Add user account / Initiate password	✓

				• Delete user account	✓
				• Password update	✓
				• User identifier query	✓
User	One or more than one	To perform cryptographic operations	• Key management	• Key and parameter entry	✓
				• Key generation	✓
				• Key output	✓
				• Key archiving	✓
				• Key zeroization/destruction	✓
				• key update	✓
				• Key identifiers query	✓
				• Key attributes query	✓
			• Cryptographic management	• Initialization / Configuration	X
				• Error handling and resetting	X
				• Serial number query	✓
				• Local time setting	X
			• Show Status	• Version information	✓
				• Error code while in Error state	✓
			• Selectable self-tests	• Cryptographic algorithm tests	✓
				• Firmware tests	✓
				• Critical function tests	✓
				• SRNG tests	✓
			• Cryptographic operations	• Encryption	✓
				• Decryption	✓
				• Digital signature generation	✓
				• Digital signature verification	✓
				• Hash	✓
				• Random number generation	✓
			• User management	• Add user account / Initiate password	X
				• Delete user account	X
				• Password update	✓
				• User identifier query	✓

Table 4 - Roles, services and corresponding functions

[Note] "✓" implies "allowable" "X" implies "unallowable"

Role/Service Access Control

After an operator (either a Crypto-officer or a User) has authenticated himself to the module, he can perform the cryptographic services of his corresponding role as authorized by the module. We define the detail Role/Service Access Control table by the following columns to construct the general principles of access control rules. These columns of the table are depicted as follows.

- Column "Un-authentication public"

  The column information indicates what kind of commands could be issued by anyone without passing the authentication procedures.

  For example: anyone can query the systems global and public information such as version, supporting algorithms and serial number of the CryptoCard, without authentication requirements since such information are not security-relevant. The information is basic, open and not confidential for any query.

- Column "Self Management" with Role "C" (Crypto-officer)

The column information indicates what kind of commands could be issued by a Crypto-officer after passing the authentication procedures.

For example, an operator in role of Crypto-officer can perform the User Management service, but he is not permitted to add or delete his own account as the Crypto-officer.

- Column "Self Management" with Role "U" (User)

  The column information indicates what kind of commands could be issued by a User after passing the authentication procedures.

  For example, an operator in the User role can perform the Key Management service but he is only allowed to manage his own key.

- Column "$User_1$ (U_1) manages $User_2$ (U_2)"

  The column information indicates what kind of commands could be issued by a $User_1$ on $User_2$'s relevant data.

  For example, $User_1$ can perform the Key Management service. He is authorized to manage his own keys, but he is not authorized to manage $User_2$'s keys. In other words, he cannot perform the key generation or key output for $User_2$, but he is allowed to perform digital signature verification by using the $User_2$'s RSA public key for digital signature application.

- Column "Crypto-officer (C) manages User (U)"

  The column information indicates what kind of commands could be issued by a Crypto-officer on another user's relevant data.

  For example, the Crypto-officer can perform the Key Management service. He or she is authorized to not only manage his own keys, but also to perform partial commands of the managing User's keys. That is, he can perform the key generation for User.

- Column "User (U) manages Crypto-officer (C)"

  The column information indicates what kind of commands could be issued by a user on a Crypto-officer's relevant data.

  For example, a User can perform the Key Management service. He is authorized to manage his own keys, but he is not authorized to manage Crypto-officer's keys. For example, he cannot perform the key generation or key update for the Crypto-officer.

The relation between role, services and the privilege control among distinct role entity is

summarized in Table 5, “Matrix of the service access control among distinct roles”.

Service	Functions	Role/ Service Access Control					
		Un-authe-ntication / Public	Self Management		User$_1$ manages User$_2$ / Crypto-officer manages User / User manages Crypto-officer		
		All	C	U	U_1? U_2	C? U	U? C
Key management	Key and parameter entry	x	✓	✓	x	✓	x
	Key generation	x	✓	✓	x	✓	x
	Key output	x	✓	✓	x	x	x
	Key archiving	x	✓	✓	x	x	x
	Key zeroization / Destruction	x	✓	✓	x	✓	x
	Key update	x	✓	✓	x	✓	x
	Key distribution	x	✓	✓	x	x	x
	Key identifiers query	x	✓	✓	✓	✓	✓
	Key attributes query	x	✓	✓	x	✓	x
Cryptographic management	Initialization/Configuration	x	✓	x	N/A	N/A	N/A
	Alarm handling and resetting	x	✓	x	N/A	N/A	N/A
	Serial number query	✓	✓	✓	N/A	N/A	N/A
	Local time setting	x	✓	x	N/A	N/A	N/A
Show status	Version information	✓	✓	✓	N/A	N/A	N/A
	Error code while in command execution fails	x	✓	✓	N/A	N/A	N/A
Selectable self-tests	Cryptographic algorithm tests	x	✓	✓	N/A	N/A	N/A
	Firmware tests	x	✓	✓	N/A	N/A	N/A
	Critical functions tests	x	✓	✓	N/A	N/A	N/A
	Statistical random number generator tests	x	✓	✓	N/A	N/A	N/A
Cryptographic operations	Encryption (Symmetric Key)	x	✓	✓	x	x	x
	Decryption	x	✓	✓	x	x	x
	Digital signature generation	x	✓	✓	x	x	x
	Digital signature verification	x	✓	✓	✓	✓	✓
	Hash	x	✓	✓	N/A	N/A	N/A
	Random number generation	x	✓	✓	N/A	N/A	N/A
User management	Add User account / Initiate password	x	x	x	x	✓	x
	Delete user account	x	x	x	x	✓	x
	Password update	x	✓	✓	x	x	x
	User identifier query	✓	✓	✓	✓	✓	✓

Table 5 Matrix of the service access control among distinct roles

[Note]

“C” is short for the Crypto-officer role
“U” is short for the User role
“All” is short for all persons
“✓” implies “allowable”
“x” implies “unallowable”
“N/A” implies “not applicable”

Key Attributes Permission Check

The design of cryptographic key attributes follows the definition of PKCS#11 to enhance the granularity level of the security of the module. To perform a given command, the CryptoCard will check that the designated key with the proper attribute is set related to this command, and then determine if the command is permitted to be

executed with the assigned key. For example, the key output command, the module will check if the designated cryptographic key identifier with the key attribute "Extractable" is "TRUE" or not before allowing the execution of key output. If it is true, output of the specified key from the CryptoCard is allowed; otherwise, the key output by the specified key is prohibited.

2.5 Physical Security

The CryptoCard demonstrates an incredible array of physical security safeguards with the sophisticated design of its tamper-resistant mechanism.

The cryptographic module of the CryptoCard is encapsulated within a strong metal case. An intruder, attempting to break into the module by brute force or breach of the enclosure of the module, will easily leave clear visual evidence of tampering. There are no ventilation holes in the CryptoCard.

In order to provide additional protection to the module, the components in the case are coated with epoxy resin so that any attempt to probe the module's interior will encounter difficulty. The metal case housing the whole security related circuitry of the CryptoCard is filled with opaque, tamper-evident, passivated and hard epoxy material.

When the case is pried open, the tamper resistant circuitry inside triggers an active zeroization of all keys and other critical security parameters stored in the Secure Memory. A specially designed tamper prevention circuit will trigger the zeroization of the Secure Memory when it detects a tamper attempt by drilling or milling on the top of the metal case as well. Although the design does not intend to meet the level 4 physical security requirements, it is helpful for the physical security of the level 3 CryptoCard. The tamper detection cannot meet level 4 physical security requirements because the tamper detection circuit does not protect all sides of the module, only the two largest sides of the module.

In short, the tamper resistant circuitry initiates an active zeroization when it detects the following tamper conditions:

- Separate the enclosure from the circuit board of the CryptoCard
- Drilling or milling on the top of the metal case
- Remove the CryptoCard from the PCI slot (optional feature)

As mentioned above, all keys and other critical security parameters are stored securely in the Secure Memory of CryptoCard. Therefore, if power is supplied by the host computer, the CryptoCard consumes that power to retain the information in the Secure Memory. A set of two three volts Lithium batteries attached to the CryptoCard will also provide an ordinary source of power to Secure Memory in order to keep all the keys and other critical security parameters fresh and alive when the host is in the power-off mode. The ordinary Lithium battery set is outside the metal case for easy access to change a new battery when its energy runs out. Another set of batteries is built-into the RTC (Real Time Clock) electronic component enveloped and protected by the exterior metal case. When the

electric power of the ordinary Lithium battery set runs out, the electric power shortage LED indicator will light up, and the module can use the backup RTC battery power to keep the security related parameters safely stored in the Secure Memory. This backup battery set allows the Crypto-officer an opportunity to change the power-drained battery without losing the contents stored in the module. The hardware self-test of the module also includes a RTC electric power shortage test.

2.6 Cryptographic Key Management

Cryptographic key management involves the entire life cycle of the cryptographic keys employed with the CryptoCard, including their generation, entry, output, usage, storage, destruction, distribution and archiving.

Since the CryptoCard is intended to meet FIPS 140-1 level 3 requirements, the secret keys and private keys in the module are protected from unauthorized disclosure, modification and substitution. Public keys must be protected against unauthorized modification and substitution. Therefore, when keys are stored in the secure memory of the CryptoCard, they are in plain text because the secure memory is protected in the tamper-resistant steel case. If keys are exported from the module for storage or usage, they are encrypted with the session key and sent through the cryptographic boundary of the module to the external target applications.

This section, describes how the module performs key management as follows.

Key Material

The module supports three types of keys that are generated both internally and externally. The types of keys are DES, Triple DES and RSA. The Crypto-Officer is the only operator authorized to use and manage the system key, a Triple DES key, of the module.

DES [Note 1] and Triple DES keys are used for encryption and decryption, since RSA is used for signature generation/verification and key distribution in FIPS mode. Table 6 describes the cryptographic functions of each key.

Cryptographic Functions	Types of keys used			
	DES Key	Triple DES key	RSA Public key	RSA Private key
Encryption	✓	✓	✓(Non-FIPS Mode only)	N/A
Decryption	✓	✓	N/A	✓(Non-FIPS Mode only)
DAC (Data Authentication Code)	✓	✓	N/A	N/A

Note 1 *NIST has instructed that all modules use Single DES for compatibility with legacy applications only.*

Digital Signature Generation	N/A	N/A	N/A	✓
Digital Signature Verification	N/A	N/A	✓	N/A
Key Distribution	✓	✓	✓	✓

Table 6 – Cryptographic functions of each key

The operational mode of CC2200 can only be set by the Crypto-Officer. The authenticated Crypto-Officer may change the operational mode of CC2200 to FIPS mode or Non-FIPS mode at any time by issuing the command to set the operational mode to the CryptoCard. Once the mode is successfully set to the Non-FIPS mode, the RSA encryption and decryption operation commands are enabled for use by all authenticated operators. Otherwise, the RSA encryption and decryption operation commands are disabled when the operation mode is under FIPS mode.

Keys entered into and output from the module are encrypted with the session key, a DES key generated during the mutual authentication procedures when an operator logs on. Since key protection is essential to the security level of the module and cryptographic operations/services, methods the module uses to protect the keys are introduced as follows:

Key Generation

- **FIPS-approved random number generation algorithms for key generation**
  - The module uses one of the FIPS-approved random number generation algorithms --- ANSI X9.31 Annex C for the generation of random number key.
  - The module provides random key generation for DES keys, Triple DES keys and RSA Keys.
- **Types of keys are generated**
  - System key (a Triple DES key used by Crypto-Officer only)
  - Authentication key (A DES key used by the challenge-response protocol)
  - General cryptographic keys of the operators (Crypto-Officer & Users)
    - DES key
    - Triple DES key (112 or 168 bits)
    - RSA public and private keys (512 ~ 2048 bits) [Note 2]

The values used during key generation are not accessible outside of the module in any format. The key generation procedures proceed continuously in the module until the result comes out. That is, no data is allowed to input or output from the module during the course of key generation.

Key Distribution

To better secure the key distribution operation, an operator is required to provide his or her ID and password to generate the authentication key and identify himself or herself to the module by mutual authentication procedures before the key distribution operations can begin.

The key distribution technique employed is the commercially available RSA public key-based key distribution technique. Since there is no FIPS-approved public key-based key distribution technique, the commercial RSA key transport method is used by the key wrapping command to encrypt the target key to be distributed. Hence, the module uses this technique to distribute DES, Triple DES and RSA public/private keys.

Note 2 *NIST recommends that RSA keys should be at least 1024 bits.*

In this module, the possible and allowable combination of wrapping keys and wrapped keys are listed as follows:

Wrapping Algorithm	Wrapping Key	Wrapped Key
DES/3DES CBC	DES/3DES CBC	RSA key
DES/3DES CBC	DES/3DES CBC	DES/3DES key
RSA	RSA public	DES/3DES key

Table 7 – Combination of wrapping keys and wrapped keys

It is assumed the RSA public keys used for the wrapping key have been previously loaded or generated in the module so that the target key can be wrapped for later distribution. Since the RSA public key used as the wrapping key is the key encryption key, it should be taken from the remote receiver with the corresponding RSA private key to decrypt the wrapped target key. The public key could also be retrieved from the receiver's electronic certificate issued and distributed by PKI (Public Key Infrastructure) systems.

Wrapping keys using DES/3DES as the wrapping algorithm is reserved for key archiving and not used for key distribution.

Key Entry and Output

The module only supports the electronic key entry and output. To ensure that each key is entered/outputted with the correct entity, an operator is required to implicitly authenticate himself to the module with the issued command encrypted and decrypted by the session key, a DES key, generated during the successful mutual authentication procedures. In addition the design of key attributes follow the definition of PKCS#11 to enhance the level of security of the module. The keys allowed to be extracted from the module are exported outside of the module and are encrypted by the session key to ensure there is no secret leakage through the cryptographic boundary.

As described earlier, passwords and security sensitive parameters are securely protected by encryption with the session key between the operator and the module because only the legitimate operator and module can generate the same shared secret – the session key. Thereafter only the legitimate operator can have access to the module. The authentication mechanism assures that the key entry and output of the target key can only be executed by the legitimate operators.

DES, Triple DES and RSA keys can be entered into the module and output from the module if they have extractable characteristics of the key attributes. As for the authorization of key entry and output, the Crypto-Officer can perform the key entry for himself and other users of the module. An operator, including the Crypto-Officer and the users of the module, can deal with his or her own keys for entry and output.

Key Storage

The key types stored in the module include DES, Triple DES and RSA key. These keys are stored in the Secure Memory, which is an SRAM chip in the module. Since the SRAM is protected by the tamper resistance mechanism (refer to Section "Physical Security"), the keys stored in these memories have no risk of exposing the contents due to any external breach. Therefore these keys are stored in plain text form in the Secure Memory.

To protect the unauthorized disclosure, modification, and substitution of the secret key and private key stored in the module, the module implements the mechanism of mutual authentication and session key encryption for the requested command, which ensures the command issuer is the correct and legitimate identity. In addition, the ACT (Access Control Table) is implemented to check the authorization of the command issuer (refer to Section 2.4, "Mutual Authentication (MA) Scheme" and "Role / Service Access Control"). These mechanisms assure that the unauthorized disclosure, modification, and substitution of the secret key and private key are never stored in the module by an unauthorized operator.

These mechanisms also provide the means to ensure that all keys are associated with the correct entity (the command issuer) to which the keys are assigned. The association of the key and the correct entity is by the key identifier and the operator identifier. The shared secret between the operator and the CryptoCard is the operator's password which provides the basis of the pairwise unique component to identify the command issuer's identity for the module. The password will not be directly passed through the cryptographic boundary. A secret authentication key generated from the password is the common secret between the operator and the module, which makes the further mutual authentication protocol able to proceed (refer to Section "Identification and Authentication (I&A) Policy").

The unauthorized attempt to swap or use the secret or private keys that belong to two different entities is impossible since the authentication and authorization scheme prevent the situation from happening.

Key Destruction

The CryptoCard provides the capability to zeroize all plain text cryptographic keys within the module. An operator in the User role can only zeroize his own keys. But if he is in the Crypto-Officer role, he can zeroize all keys of the module. In the module, keys are subject to zeroization when the following two situations occur:

- **Detection of Tamper Intrusion Attempt by the CryptoCard**
  - The sensor circuit inside the enclosure of the CryptoCard will detect physical tampering and the module will begin to zeroize the secure memory by grounding. Meanwhile, all operators' passwords will also be zeroized, because their disclosure

to the outsider would also compromise the security of the module.

- **Demand to Destruct the Keys by Operators**
  - The Crypto-Officer issues a command to zeroize a User's key when he discovers a User is suspect.
  - The Crypto-Officer implicitly zeroizes a User's keys when he deletes the corresponding User account.
  - The Crypto-Officer or User can zeroize his own keys when he suspects they might be compromised.
  - The Crypto-Officer or User can zeroize his own keys when they are no longer needed and used.

Key Update

Key update involves updating the cryptographic key attributes or key values of the legitimate operator accounts of the CryptoCard. The cryptographic keys including DES, T-DES and RSA keys are owned by the legitimate accounts of the CryptoCard.

A key update is accomplished by an authorized operator who inputs the new key attribute values or new key values to the CryptoCard to replace the old values of the target key in the Secure Memory. Similar to the other authentication-required commands, the key update commands are issued only after successfully passing the authentication procedures, and the new key value and attribute parameters are updated and encrypted by the session key.

Key Archiving

Generally speaking, an operator, including Crypto-Officer and a User, of the module, can archive his or her own keys from the module to the memory or hard disk of the external host or server machine plugging the CryptoCard. They archive or backup their own keys by encrypting their keys, along with the PKCS #11 key attributes, with an externally provided DES or 3DES key back-up key. The encrypted key information is then output from the module for archival storage.

In order to ensure each key is archived with the correct entity before the key archiving operation, an operator is required to authenticate himself to the module by passing the mutual authentication procedures as the described in Section "Identification and Authentication (I&A) Policy". To restore the archived keys, an operator's issued restore command request must pass the implicit authentication of the module by session key ciphering, and then the module must use the same back-up key to decrypt the archival packs and restore the plain text key to the Secure Memory of the module.

2.7 Cryptographic Algorithms

The Algorithm implementation of the CryptoCard follows the related FIPS Publication documentation. The CryptoCard supports SHA-1 for message digest generation, DES

and Triple DES for bulk data encryption/decryption and RSA for digital signature generation / verification. It also provides the DES DAC (Data Authentication Code) and Triple DES DAC algorithms. The module uses FIPS 186-2 Appendix 3 and ANSI X9.31 Annex C random number generator for RSA Key generation. The table below is a list of each cryptographic algorithm implemented in the module, including its name, key length supported and the implementation in compliance with standards.

Cryptographic Algorithm	Key length (bits)	Standard
DES (ECB & CBC) [Note 1]	56	FIPS 46-3 (ANSI X9.52), FIPS 81
Triple DES (ECB & CBC)	112/168	FIPS 46-3, FIPS 81
SHA-1	N/A	FIPS 180-1
RSA [Note 2]	512~ 2048	FIPS 186-2 (ANSI X9.31)
DAC (or MAC)	56/112/168	FIPS 113

Table 8 – Algorithm implementation of the Cryptographic Module

2.8 EMI/EMC

To meet FIPS 140-1 level 3 security requirements, *the **NST*** Security CryptoCard passes the FCC radio certification by PEP Testing Laboratory. The module also conforms to the EMI/EMC requirements and passes the FCC Part 15, Class B certification. It also passes the local EMC standards, CNS 13438, of Taiwan, as well.

2.9 Self-Tests

The CryptoCard is capable of performing self-tests in order to ensure that the module is functioning properly. The Self-tests include two kinds of tests; the Power-up self-tests and Conditional tests. Certain self-tests are performed when the module is powered up to ensure the module is operating normally and ready to accept external request commands after these tests. Conditional tests are performed under various conditions, typically when a particular function or operation is performed (i.e., key pairwise consistency test executed right after RSA key generation operation).

The two parts of self-tests Power-up self-tests and Conditional tests provided in the module are depicted as follows.

Power-up Self-tests

Power-up self-test items are required to be executed when the module powers up. They consists of the following tests:

Note 1 *NIST has instructed that all modules use Single DES for compatibility with legacy applications only.*

Note 2 *NIST recommends that RSA keys should be at least 1024 bits.*

Self-Test Items	Contents
Firmware Integrity Test	• DAC (FIPS 113)
Statistical Random Number Generator (SRNG) Test	• Monobit Test • Poker Test • Runs Test • Long Run Test
Continuous RNG Test	• FIPS approved ANSI X9.31 PRNG algorithm
Cryptographic Algorithm Known Answer Test (KAT)	• Digital signature generation and verification : RSA (ANSI X9.31) • Symmetric encryption and decryption : DES (FIPS 46-3) • Symmetric encryption and decryption : Triple DES (FIPS 46-3) • Message digest : SHA-1 (FIPS 180-1)
Critical Functions Test	• Major hardware components functional tests

Table 9 – Self-test items and contents

Conditional Tests

Self-tests except Power-on self-tests, shall be performed under certain conditions, typically when a particular function or operation is performed. It consists of the following tests:

Conditional Test Items	Contents
Pairwise Consistency Test	• Performed immediately a RSA key pair is generated.
Statistical Random Number Generator (SRNG) Test	• The test can be performed on demand. • Test items include ➢ Monobit Test ➢ Poker Test ➢ Runs Test ➢ Long Run Test
Continuous RNG Test	• FIPS approved ANSI X9.31 PRNG algorithm • The module performs this test whenever a random number is generated.

Table 10 – Conditional test items and contents

3. Summary

- **Physical Security Protection**

The passwords and keys stored in the module's Secure Memory are securely protected. When the tamper trial triggers the tamper resistance circuitry of the module, it will cause the zeroization circuit to zeroize all the contents stored in the Secure Memory so that no secret of the keys and passwords are revealed. The key zeroization is based on grounding the power supply to the secure memory, and will make the SRAM unable to keep the original contents in the memory cells because there is no power supplying it. Therefore, keys are stored in the Secure Memory in plain text format. If keys are not stored in the module's Secure Memory or are transited through the cryptographic boundary of the hardware module, they will exist in cipher text format.

- **Logical Security Protection**

A. Identity-Based Authentication

Since the CryptoCard meets FIPS 140-1 level 3 requirements, the module provides identity-based authentication. The operator requests to gain access to the module must pass the Challenge-Response mutual authentication between the host side application and the CryptoCard. The symmetric authentication key used for the mutual authentication is generated from the logon account's unique ID/password pair, and the session key used to cipher the command and response is generated using Diffie-Hellman key agreement during the authentication procedures between the two sides.

B. Service Access Control

Once an operator has passed the authentication procedures, the module will check the account information, implicitly assume the role for the operator, and grant the access rights of the corresponding authorized service list to the role. The requested command would be checked against the authorized service list of the logon role to determine if it is to be executed by the module. The permission check of PKCS#11 key attributes enhances the security granularity of cryptographic key usage.

4. Reference

[1] U.S. Department of Defense, ***"Department of Defense Password Management Guideline"***, CSC-STD-002-85, Department of Defense Computer Security Center, Fort Meade, MD, April 1985