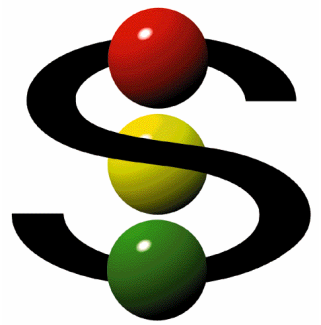

3S Group Incorporated

Type 2 Cryptographic Support Server (T2CSS)

T2CSS Cryptographic Module Security Policy

Jnne 2008

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 SCOPE

The purpose of this document is to define the security policy of the Type 2 Cryptographic Support Server (T2CSS) Board. This security policy is presented in accordance with the documentation requirements of Federal Information Processing Standard (FIPS) 140-1, Security Requirements for Cryptographic Modules. This policy document describes how the T2CSS board satisfies the level 2 requirements of FIPS140-1 to protect sensitive information in U.S. Government as well as non-Government information systems.

1.1 Applicable Board Versions

This security policy applies to the following board versions:

1. Hardware: 1.0, 1,1, 1.2, and 2.0
2. Firmware: 1.0, 1,1, and 1.2

2 APPLICABLE DOCUMENTS

The following documents are referenced in this document:

- FIPS PUB 46-3, Data Encryption Standard (DES), NIST, 25 October 1999.
- FIPS PUB 81, DES Modes of Operation for DES and SKIPJACK, 2 December 1980.
- FIPS PUB 140-1, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST), 11 January 1994.
- FIPS PUB 180-1, Secure Hash Algorithm (SHA-1) Standard, NIST, 17 April 1995.
- FIPS PUB 185, Escrowed Encryption Standard (EES), NIST, 9 February 1994.
- FIPS PUB 186-2, Digital Signature Algorithm (DSA) Standard, NIST, 27 January 2000.
- Derived Test Requirements for FIPS 140-1, Security Requirements for Cryptographic Modules, NIST, March 1995.
- FORTEZZA Application Implementers Guide, NIST, Document # MD4002101-1.52, 5 March 1996
- Interface Control Document for the FORTEZZA Crypto Card (Production Version) (DRAFT), Revision P1.5, National Security Agency (NSA) X21, December 2 1994
- Public Key Cryptographic Standard (PKCS) #11, v2.10, Cryptographic Token Interface Standard, RSA Laboratories, December 1999.

3 TYPE 2 CRYPTOGRAPHIC SUPPORT SERVER (T2CSS)

Both Government and private industry are increasingly utilizing public key cryptography to secure information, and this places greater demands on the processing capacity of the information systems. The Government as well as the business community is becoming more aware of the

need for higher security assurance. A reliable public key infrastructure (PKI) is vital to achieving interoperability among the users in these communities, in order to conduct electronic commerce and exchange sensitive information over unprotected public networks.

The U. S. Department of Defense, through its Multi-Level Information Security System Initiative (MISSI), developed the FORTEZZA technology to support writer-to-reader security in their messaging systems. Individuals and organizational end-entities are registered and provided a PCMCIA (or PC) card, hereinafter referred to as the FORTEZZA PC card, which contains symmetric and asymmetric keys and certificates. These keys are used to achieve data confidentiality, data integrity, user authentication and non-repudiation.

Irrespective of the form factor, FORTEZZA PC cards and smart cards as hardware tokens are gaining wider acceptance to provide higher assurance security. These PC or smart cards, however, cannot provide the throughput needed to secure information on the server side, even when several cards are used in parallel.

The Type 2 Cryptographic Support Server (T2CSS) is a hardware FORTEZZA device with a Peripheral Component Inteconnect (PCI) or Peripheral Component Interconnect Express (PCIe) interface. Figure 1 shows the T2CSS PCI board and Figure 2 shows the T2CSS PCIe board. The T2CSS is used in server-class machines required to handle multiple requests for security services from multiple users. T2CSS is the perfect solution for server applications that have demanding security assurance and performance requirements..

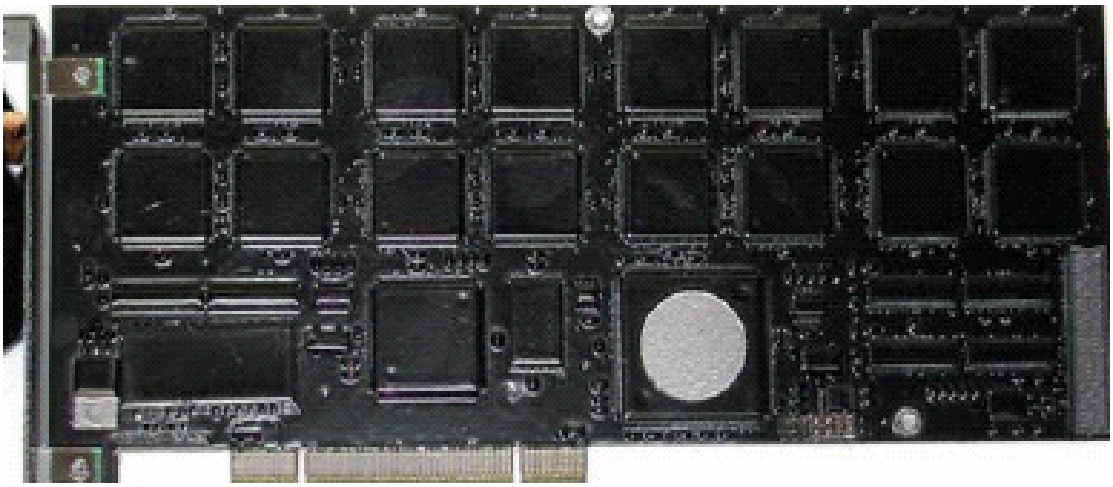

Figure 1 T2CSS PCI Board

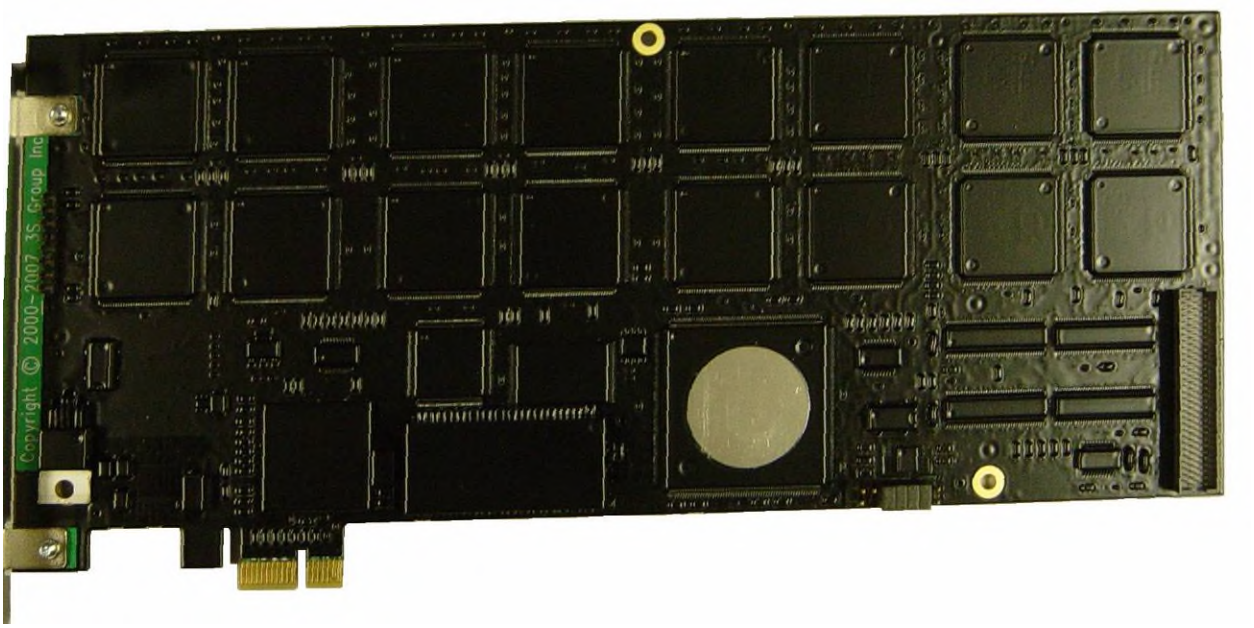

Figure 2 T2CSS PCIe Board

The T2CSS supports both the Government and the private industry security requirements. It complies with the FORTEZZA requirements for symmetric and asymmetric processing, and interfaces with the MISSI PKI. It also complies with non-FORTEZZA standards and PKIs. The same concepts, security criteria, design rules and practices are employed to satisfy both FORTEZZA as well as non-FORTEZZA requirements.

The T2CSS system contains two major components shown in Figure 2; a multi-chip (multiple

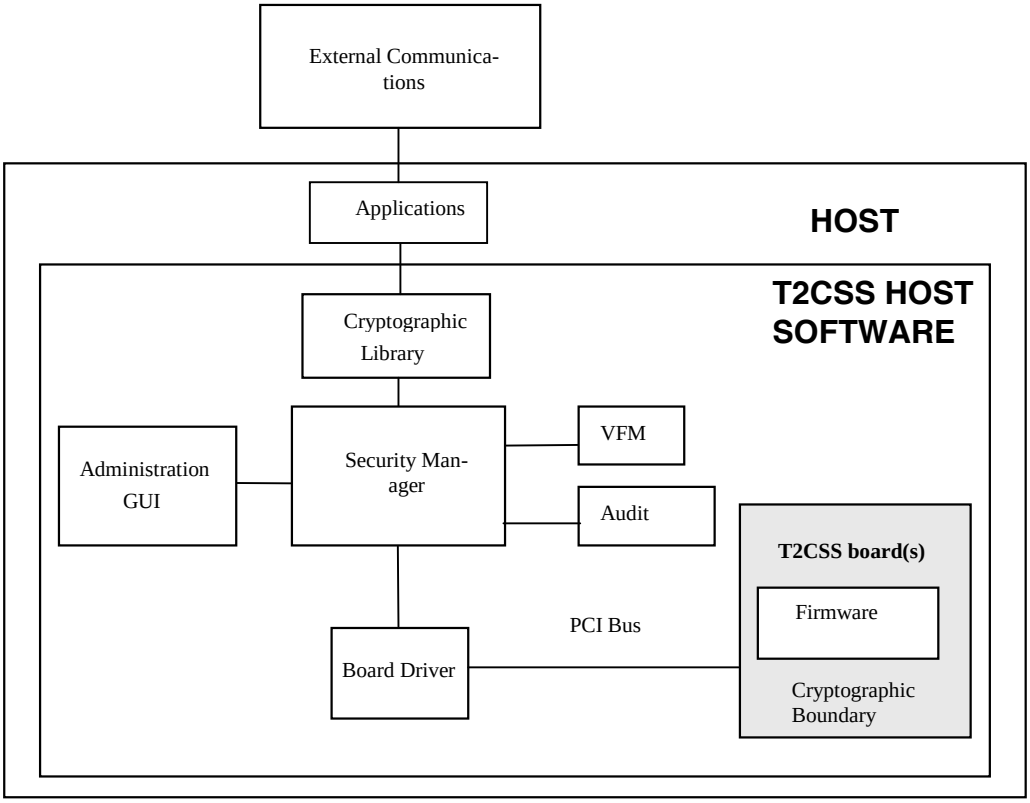

Figure 3 The T2CSS System

cryptographic processors) embedded module with a PCI or PCIe interface and a suite of host software that performs management, administrative and maintenance functions.

3.1 Cryptographic Module Overview

The T2CSS board contains multiple cryptographic processors; each supports multiple concurrent operators and can switch between them efficiently. The board also contains a control processor that implements load balancing to ensure efficient and effective utilization of the cryptoprocessing resources. Multiple boards can be operated in the host server to boost performance and improve reliability.

Cryptographic services are provided to Virtual Tokens (VTs); a VT is a collection of keys, certificates and authentication data that is unique to an individual operator of the T2CSS. Each token contains multiple keys and certificates issued to or created by the operator. In the FORTEZZA domain, these virtual tokens are called Virtual FORTEZZA Cards (VFCs). Keys supporting FIPS approved and non-FIPS approved algorithms (listed below) for both FORTEZZA and commercial operators can be loaded into these tokens.

References are made to FORTEZZA throughout this document, but the same considerations apply to non-FORTEZZA operation. For example, a T2CSS VFC contains FORTEZZA Skipjack

keys for encryption and DSA keys for digital signature. In the same manner, a non-FORTEZZA version of this token, called simply a Virtual Token (VT), may contain DES, triple-DES and RSA keys.

Multiple VFCs are stored in a host database called the Virtual FORTEZZA Manager (VFM) or Virtual Token Manager (VTM). Each VFC is encrypted using 80-bit Skipjack in CBC mode when stored in the VFM, and is decrypted on the board before use. The owner of a VFC can only use that VFC after successfully logging in with a PIN phrase.

The VFC is loaded onto the T2CSS board and allocated to a cryptoprocessor when the VFC owner requires security services. From an operational standpoint, the VFC owner can view this process as a temporary "leasing" of the cryptoprocessor hardware. The T2CSS host software loads VFC(s) on the board to perform cryptographic operations.

The T2CSS board also contains credentials and keying material stored in persistent memory. This Board Token can be accessed by some of the operators defined for the T2CSS system (see Section 5 for description of these operators). This Board Token is never offloaded from the T2CSS board.

3.1.1 Cryptographic Boundary

The FIPS cryptographic boundary (the boundary of the cryptographic module) is the perimeter of the T2CSS board. The jumper block and the expansion connector are excluded from the FIPS 140-1 validation, as they are not security relevant.

3.1.2 Interfaces

The PCI or PCIe bus is the only physical interface used by applications connecting to the module. The four logical interfaces (command, input, output and status) all use this single physical interface. Hardware versions 1.0, 1.1, and 1.2 have the PCI interface, and hardware version 2.0 has the PCIe interface.

3.2 Host Software Overview

The host software consists of a device driver, security management software and Application Programming Interfaces (API) and libraries. Server or end-user applications can access the T2CSS board through well-defined APIs such as the FORTEZZA Cryptologic Interface (CI) and Public Key Cryptographic Standard (PKCS) #11.

The T2CSS system is easy to use relative to management and administration. For application developers high-level APIs are provided to hide low-level security concepts and details.

- The T2CSS system is easy to install. A utility program is provided which installs the host software and sets up the system with minimal effort.

- The support software also includes a Graphical User Interface (GUI) tool that eases administration and management of the entire T2CSS system.
- Applications that are already FORTEZZA enabled need not make any modifications to work with the T2CSS. Other APIs, such as Microsoft Cryptographic API (CAPI), are available to application developers to interface with the T2CSS.

The T2CSS system software includes a device driver, which is needed for host applications (including the rest of the T2CSS system) to communicate with the T2CSS board. The driver can manage concurrent access to multiple boards.

The Security Manager handles all functions related to session management, token management, and access control. It serves as a single point of management between multiple applications that use multiple VFCs, and maps these VFC onto multiple T2CSS boards.

The Administration GUI (Graphical User Interface) provides the T2CSS Administrator with the means to manage and administer the T2CSS system. Some of the functions it provides are: starting and stopping the T2CSS system; installing, removing and assigning VFCs; archiving and restoring the VFM database and its database key; and, setting audit levels, view audit logs.

The T2CSS supports the following operating environments:

- Windows NT
- Windows2000
- Solaris
- Linux.

4 SECURITY FEATURES

4.1 Security Services

The T2CSS provides security services such as data confidentiality, data integrity, key management, digital signatures, time stamping, and non-deterministic random number generation. Security mechanisms for authentication, access control and certificate management are implemented.

4.2 Algorithms

The T2CSS system implements Government and commercial cryptographic algorithms in hardware, making it capable of satisfying the requirements of both Government and non-Government information systems.

The following FIPS approved algorithms are implemented:

1. Skipjack encryption and decryption: ECB, CBC, OFB64, CFB64, CFB8 modes

2. DES encryption and decryption: ECB, CBC, OFB64, CFB64, CFB8 modes
3. Two-key Triple-DES encryption and decryption: ECB and CBC modes
4. Three-key Triple-DES encryption and decryption: ECB and CBC modes
5. NIST Secure Hash Algorithm (SHA-1)
6. NIST Digital Signature Algorithm with variable size moduli (512-1024 bits) and 160-bit private key
7. RSA signature algorithm with variable size moduli (512-1024 bits)
8. Pseudo-random number generation (per Appendix 3.3 of FIPS 186-2)

The following non-FIPS approved algorithms are also implemented:

1. Key Exchange Algorithm (KEA) with 1024-bit moduli and 160-bit private key
2. Secure timestamping and timekeeping

4.3 Virtual Tokens

As stated earlier, virtual tokens contain keys and certificates supporting the algorithms listed above. An 80-bit Skipjack database key cryptographically protects each VFC when stored in the VFM. This database key never leaves the hardware in unencrypted form and is generated using the board's pseudo-random number generator. The T2CSS host software provides management functions such as saving and restoring database keys, as well as saving and restoring the VFM database.

4.4 Power-On Self Tests

The T2CSS board design includes an automatic cryptographic self-test, performed at system startup. This self-test is also available when the T2CSS board is reset. Tests include known-answer tests for the Skipjack, DES, TDES, SHA-1 and RSA functional block of each cryptoprocessor, pairwise consistency test for DSA, verification of all firmware images in nonvolatile memory, and system-level processor and memory tests. A pairwise consistency test is performed whenever a DSA, KEA or RSA key pair is generated or loaded onto a cryptoprocessor.

4.5 Random Number Generation

Each cryptoprocessor contains a nondeterministic noise generator; the output of this generator is subjected to a monobit test at bootup and continuous tests for all-ones and all-zeros. This generator provides seed data to the random number generator, which complies with Appendix 3.3 of FIPS 186-2.

4.6 Physical Security

Physical security measures include an opaque tamper-evident conformal coating.

4.7 Key Management

The T2CSS supports the following functions performed on keys: generation, distribution, entry and output, storage, destruction and archival. Keys, to include symmetric and asymmetric keys, are handled for the various algorithms enumerated above.

The T2CSS provides storage and retrieval for certificates issued by Government (NSA's MISSI) as well as commercial PKIs.

4.8 Performance

Each T2CSS board is optimized for simultaneous cryptographic processing to multiple users for enhanced performance. The PCI or PCIe bus allows much higher data bandwidth to and from the board than other conventional solutions such as SCSI. Multiple boards can be used within a single host system to enhance performance and reliability.

5 ROLES AND IDENTITIES

Roles in the T2CSS system are based on the FORTEZZA concept of tokens. The T2CSS supports two types of tokens, a single T2CSS Board token, and multiple users' tokens. Table 1 defines these tokens.

The T2CSS defines two types of roles for authorized access, supporting identity-based authentication conforming to FIPS level 2 requirements. These roles and identities for each token type are presented in Table 1.

Table 1 Roles, Identities, and Tokens

Token Type	Identity	FIPS Role
Board Token	1. Board Site Security Officer (SSO) 2. Board User (Administrator)	Crypto-Officer User
User VFC	3. VFC SSO 4. VFC Operator	Crypto-Officer User

An individual may assume more than one of these identities at different times. All operators must present a valid PIN to be authenticated successfully.

5.1 Board SSO Identity

The Board SSO identity is responsible for initialization and management of the Board Token. Services include setting of PIN phrases (SSO or User); archiving private keys on the Board To-

ken; setting the Real-Time Clock (RTC) on the board; and loading cryptographic keys, security parameters and trusted certificates (e.g., MISSI PKI certificate hierarchy).

5.2 Board Administrator Identity

The Board Administrator identity is responsible for managing the day-to-day operation of the T2CSS system and the contents of the VFM database. The Board Administrator may transition the T2CSS from power-up state to an operational state, load VFCs into the VFM database, monitor and reset the board, select audit levels, archive and restore the VFM database and database key. The Board Administrator can update the board firmware image.

The Board Administrator uses the Board Token to perform these functions. The next two identities (VFC Operator and VFC SSO) cannot request security services from the T2CSS board until the Board Administrator has logged into the Board Token.

5.3 VFC SSO Identity

Each User VFC supports its own SSO operator. The VFC SSO identity provides initialization services similar to those of the Board SSO identity, except that the scope of these services is limited strictly to the User VFC. Cryptographic keys, security parameters and trusted certificates may be loaded into a User VFC by this identity in the same way that the Board SSO identity may load the Board Token.

5.4 VFC Operator Identity

Each User VFC supports an identity that can request cryptographic services from the T2CSS board; this is the VFC Operator identity. All of the algorithms listed previously in section 4.2 are available to the VFC Operator. Applications that require FORTEZZA services will authenticate themselves as the VFC Operator for every T2CSS virtual token to be used.

6 SERVICES AND RULES

The services provided by the T2CSS system can be broken down into two broad categories: Cryptographic Services and Management/Administration Services

6.1 T2CSS Cryptographic Services

Cryptographic services involve operations on security-relevant data. The security design of the T2CSS will ensure that only authorized personnel and applications access T2CSS services and that only they have access to the specific services corresponding to the roles.

The data items affected by these operations are listed in Table 2 below.

Table 2 : Security Relevant Data Items (SRDI)

SRDI	Description
Board Key (Database Key)	The Key that is used to protect the T2CSS VFC database
Manufacturer Default PIN	The PIN phrase that must be entered to log in to a Virtual Token before it has been initialized
Message Encryption Key (MEK)	A bulk encryption key used for encrypting and decrypting message data. MEKs can exist for the Skipjack, DES or Triple-DES algorithms
VFC SSO PIN	The PIN phrase that must be input to assume the VFC SSO identity
Board SSO PIN	The PIN phrase that must be input to assume the Board SSO identity
Status	The current module state, mode and personality status (i.e. identity of loaded private keys)
Token Encryption Key (TEK)	A value derived by the KEA. Used to encrypt other symmetric keys
Board Administrator PIN	The PIN phrase that must be input to assume the Board Administrator identity
VFC Operator PIN	The PIN phrase that must be input to assume the VFC Operator identity
Storage Key Variable (Ks)	A Skipjack key stored permanently in its own key register and used for encrypting other quantities before they are stored or offloaded
Key File Encryption Key (KFEK)	A Skipjack key used to encrypt the Ks of the Board Token (Board SSO or Board User Identity) or User VFC (for VFC User or VFC SSO Identity).
Private Key (X)	This is the private part of a Public/Private key pair used in KEA, DSA, or RSA algorithm
Public Key (Y)	The public part of a Public/Private key pair used in KEA, DSA, or RSA algorithm
Board Token Zeroize Default PIN	The Board SSO PIN phrase that must be entered to log on to the Board Token once it has been zeroized.
User VFC Zeroize Default PIN	The VFC SSO PIN phrase that must be entered

SRDI	Description
	to log on to the User VFC once it has been zeroized.

Table 3 below lists all of the T2CSS Cryptographic Services available to all identities. Unless indicated otherwise, successful authentication for a particular identity is required before being allowed to perform the services listed in Table 3. See section 5 for an explanation of the identities supported by the T2CSS.

All services listed in Table 3 below are described in the FORTEZZA Application Implementers Guide (AIG) listed in section 2.

Table 3 : Services and Rules for Cryptographic Operations

Service	Board Administrator and VFC Operator	Board SSO and VFC SSO	Rules
Generating Keys			
Storage Key (Ks)		X	Only loaded during initialization
Generate/Load/Delete MEK	X		
Generate/Delete TEK	X		TEKs may not be offloaded
Generate/Load Signature key pairs (DSA or RSA)	X	X	RSA key pairs may only be loaded
Generate/Load Key Exchange key pairs (KEA)	X	X	
Certificates			
Load Trusted Certificate		X	
Load All other Certificates	X	X	
Delete Certificates	X	X	Key pairs are only deleted when the corresponding certificate is deleted
Retrieve Certificates	X	X	
Protecting Data			
Encrypt	X		
Decrypt	X		
Authenticating Data			
Hash	X		
Generate / Verify Digital Signature	X		

Service	Board Administrator and VFC Operator	Board SSO and VFC SSO	Rules
Generate / Verify Timestamp	X		
Key Management			
Extract Private Keys (export service)		X	Only keys generated by SSO may be extracted
Relay/Install Private Keys (import service)	X	X	
Encrypt Symmetric Keys	X		
Save/Restore Crypto State	X		
General			
View Time	X	X	No authentication needed
Set Time		X	Only Board SSO may modify the board-level real-time clock
View Status/ Configuration	X	X	No authentication needed
Generate Random Numbers	X	X	No authentication needed
Zeroize VFC		X	No authentication needed
Access Control			
Check Pin	X	X	VFC Operator/Board Administrator locked out after 10 unsuccessful PIN check attempts; for VFC SSO and Board SSO, token is zeroized after 10 unsuccessful PIN check attempts
Change Pin		X	

6.2 T2CSS Management/Administration Services

Table 4 below lists all the T2CSS Management/Administration Services available on the T2CSS board to the operators. These services are not available to the VFC Operator or VFC SSO identities.

Table 4 T2CSS Management Services

Service	Board Administrator Identity	Board SSO Identity
Board Token Initialization		X
Update Board Firmware	X	X
Management of User VFCs	X	
Management of Database Key	X	
System Monitoring	X	

Brief details on the T2CSS Management/Administration Services follow.

6.2.1 Board Token Initialization

Initializing the Board Token is primarily the responsibility of the Board SSO identity. The initialization process closely mirrors that of the FORTEZZA PC card, and is described in the FORTEZZA Application Implementers Guide.

6.2.2 Management of User VFCs

The T2CSS can only be available for applications to use once the board has been transitioned to an operational state; only then can the VFC Operator access his/her token. The T2CSS Administrator must log in to the Board Token with the Board Administrator PIN to transition the board(s) from an initialized to an operational state.

The steps required to initialize a User VFC match those of initializing the Board Token with the exception that the VFC SSO (not the Board SSO) performs the initialization process. The T2CSS host software and board firmware implement measures to securely import an encrypted User VFC image into the T2CSS system. This VFC image is encrypted in 80-bit CBC Skipjack by a Certificate Authority to protect the keys and certificates contained within the VFC image. Only the T2CSS Administrator can perform this initialization service following a successful Board Token login.

6.2.3 Management of Database Key

Only the T2CSS Administrator has means to manage the VFC database and to create, save and restore the board key that encrypts the database. The T2CSS Administrator also has the means to re-encrypt, archive and load a VFC database. The T2CSS Administrator can perform this service following a successful Board Token login.

6.2.4 System Monitoring

The T2CSS Administrator, through host software, can view T2CSS system information such as system status, board status, etc. The T2CSS Administrator can also view the audit information generated by the T2CSS system.

7 STATES

The T2CSS implements a finite state machine model identical to that of the FORTEZZA PC card. Both the Board Token and all User VFCs adhere to the states of a FORTEZZA PC card, as defined in the FORTEZZA Crypto Card Interface Control Document (ICD). The state transitions and the events are as outlined in this ICD. The board firmware will check for mode type, PIN type, and valid state and then permit the cryptographic functions to be performed in accordance with the ICD.

8 GLOSSARY

Administrator	The onsite person or persons responsible for the setup, operation, and maintenance of the T2CSS security system. The Board Administrator is the person who manages user tokens in the T2CSS, to include loading, assignment, archival and restoral.
Board Key	The T2CSS Database Key that encrypts User VFC data
Board, T2CSS	A cryptographic processing hardware device designed to securely load multiple users' cryptographic tokens and perform requested security services. A Peripheral Computer Interconnect (PCI) or Peripheral Computer Interconnect Express (PCIe) bus based board resides in the host server.
Board Token	A collection of cryptographic keys and certificates that is permanently resident on the T2CSS board. It uses algorithms and procedures to provide security services to the Board Administrator and Board SSO.
CI Library	The T2CSS cryptologic interface library.
Cryptographic Boundary	An explicitly defined, contiguous perimeter that establishes the physical bounds of the T2CSS
Factory Default PIN	Default PIN for FORTEZZA token, used when that token has not been otherwise initialized.
Initialization, T2CSS Board	Each T2CSS board is loaded with a virtual FORTEZZA image that is not offloaded at any time. This image must be initialized before other users may be imported into a T2CSS system.
Initialization, VFC or VT	A process that creates virtual FORTEZZA cards, or virtual tokens, by programming and loading the board's or user's keying materials and identity. A PIN is created and delivered to the owner of the VFC or VT.
FORTEZZA card	A PCMCIA (or PC) card performs cryptologic processes on given data. The hardware token along with supporting software provides security services including data confidentiality, integrity, user authentication and non-repudiation. The card uses SKIPJACK encryption and decryption algorithm, SHA-1 hashing algorithm, DSA digital signature algorithm and Key Exchange Algorithm (KEA) for key exchange. The FORTEZZA technology was developed by the U. S. Department of Defense under MISSI to secure writer-to-reader messaging
Ks	The user's storage key.

KFEK	A Skipjack key used to encrypt the Ks of the Board Token or User VFC.
MEK	Message encryption key. Value generated by the cryptographic processor and used for encryption and decryption.
MISSI	Multi-Level Information System Security Initiative taken by National Security Agency to secure writer-to-reader messaging
PIN	Personal identification number. Phrase used to log onto the virtual FORTEZZA card (VFC) or Virtual Token (VT). This is an alphanumerical value to be held in private by a user. Each User VFC has a VFC Operator PIN and a VFC SSO PIN. The Board Token has a Board Administrator PIN and a Board SSO PIN
PIN, Board (also Administrator PIN)	Refers to the one of the two PINs that permits access to the Board Token. The board transfers from the standby state to the operational state when a successful board User PIN is entered.
PIN, SSO	Each VFC has an SSO PIN. Successful entry of the board SSO PIN transitions the T2CSS system into the SSO-enabled mode. The SSO PIN allows the SSO to change information in the User's VFC.
PIN, User	Successful entry of the board User PIN transfers the T2CSS system into the operational mode state. Successful entry of the application's VFC Operator PIN allows the application/user access to the T2CSS services.
T2CSS Host Resident Software	T2CSS software that resides on, and is executed by, the host platform's central processing unit (CPU). This software consists of the board driver, VFM or VTM, cryptographic library, and Security Manager.
TEK	Token encryption key.
Virtual FORTEZZA card (VFC) or Virtual Token (VT)	A virtual form of the FORTEZZA PC card (VFC) with the same characteristics and functionality as the FORTEZZA PC card and providing the same security services. It is used in the T2CSS. A VT is a non-FORTEZZA token providing the same security services as the VFC. See FORTEZZA Card above.
VFM or VTM Repository	A database on the host server where encrypted VFCs or VTs are stored while not in use. VFCs are encrypted by the board and stored in the host repository. The Board Administrator assigns the VFC to the intended user/owner ID and access privileges in the repository.
Zeroize	A process that clears a storage location or device and removes any residual traces of the data.

Zeroize Default PIN	For the Board Token, the SSO PIN phrase required to assume the Board SSO identity for a zeroized Board Token. For a User VFC, the SSO PIN phrase required to assume the VFC SSO identity for a zeroized User VFC