MYKOTRONX INC
A Rainbow Technologies Company

357 VAN NESS WAY — SUITE 200
TORRANCE, CALIFORNIA 90501
CAGE CODE 6S598

Pages: 24

TITLE:

Security Policy for 82A FORTEZZA Crypto Card

DATE: December 17, 2002 DOC NO. D1014

CIIN: CE100 REV.: E

Superseding: D
Dated: 7/27/99

Originator: **K. Reid**

Approvals:

Engineering	**Date**	**Manufacturing**	**Date**
Quality Assurance	**Date**	**Configuration Management**	**Date**

REVISION/CHANGE RECORD

REV	DATE	AUTHORIZATION	REVISION / CHANGE DESCRIPTION	PAGES AFFECTED
IR	11/19/96	See cover sheet	Initial Release	All
A	1/15/97	See Cover Sheet	Changes directed by InfoGuard Co. Matrix of Services: description of relay access mode, added footnote to LoadX and LoadCertificate, changed GetHash to user role, Firmware Update access mode. Security Rules: added 25 through 28, added text to 4, 7, & 14; Added Crypto Boundary to section 4. Added dates to section 2.	Pg 18 - 21 Pg 13 - 15 Pg 9 Pg 2
B	2/19/97	See Cover Sheet	Added Pairwise Consistency Test Removed Private Information page	Pg 14
C	6/18/99	See Cover Sheet	Updated to incorporate: • ICD Waiver 4.1. Firmware Update • ICD Waiver 4.3,Load IV for Encrypt • Leaf Supression	 Pg 5, 11, 13, 15, 19 Pg 5, 15 Pg 4, 13
D	7/27/99	See Cover Sheet	Updated EMI to FIPS Correct Typographical Errors	Pg 9 Pg 7, 8, 10, 11, 13, 14, 15, 20, 21
E	3/8/02	See Cover Sheet	Updated version dates of applicable docs. Added 3 commands to Table 2, Operator Services Command Set Added 1 SRDI item to section 7 Added 3 entries to table 3. Changed nomenclature to 82A Fortezza	Pg 5, 11, 16, 19 Various
	12/17/02	B. Yamamoto	Updated FIPS 186 reference to 186-2. Reference in section 3, first paragraph to section 2.1 is a typo. Should be “1.1”. Added command descriptions to 4.2. Removed rule 26 from section 5.	Pg 5 Pg 9 Pg 11 Pg 15

1. **MYKO RCR 1-16-96**

TABLE OF CONTENTS

Scope of Document

This document describes the Security Policy for the 82A FORTEZZA Crypto Card. The Security Policy specifies the security rules under which the 82A FORTEZZA card operates. This document covers the security related services of the card and is not intended to address non-security related 82A FORTEZZA card services or functions.

The 82A FORTEZZA Crypto Card is a cryptographic module which implements the Digital Signature Algorithm Standard - Section 2.1, 5; Secure Hash Algorithm Standard - see Section 2.1, 3; Key Exchange Algorithm Standard - see Section 2.1, 4; and the Skipjack Encryption Algorithm Standard - see Section 2.1, 4. The card complies with PCMCIA specification Standard Release 2.1 - see Section 2.2, 1. The card provides 41 individual commands which can be used to support cryptographic based authentication and encryption applications.

1. APPLICABLE DOCUMENTS

1.1. Government Documents

1. Interface Control Document for the FORTEZZA Crypto Card (Production Version) (DRAFT), Revision P1.5, National Security Agency (NSA) X21, December 2 1994

2. Federal Information Processing Standards (FIPS) Publication (PUB) 140-1, Security Requirements For Cryptographic Modules, National Institute of Standards and Technology (NIST), 11 January 1994

3. FIPS PUB 180-1, Secure Hash Algorithm Standard (SHA-1), NIST, 17 April 1995

4. FIPS PUB 185, Escrowed Encryption Standard (ESS), NIST, 9 February 1994

5. FIPS PUB 186-2, Digital Signature Algorithm Standard (DSA), NIST, 27 Jan 2000

6. Derived Test Requirements for FIPS 140-1, Security Requirements for Cryptographic Modules, NIST, March 1995

7. FORTEZZA Application Implementors Guide, NIST, Document # MD4002101-1.52, 5 March 1996
8. FORTEZZA ICD Waivers, Version 1.0, 5 June, 1998

1.2. Non-Government Documents

1. Personal Computer Memory Card International Association (PCMCIA) PC Card Standard, Release 2.1, July 1993, Personal Computer Memory Card International Association, Sunnyvale, CA. 94086

2. PCMCIA Services Specification, Release 2.1, July 1993, Personal Computer Memory Card International Association, Sunnyvale, CA. 94086

2. Terms and Abbreviations

CAW	Certification Authority Workstation. The workstation the SSO uses to initialize the Card, and generate and sign user certificates.
CBC	Cipher Block Chaining
Certificate	A 2048-byte packet of information containing KEA and/or DSA information about a user or a generic data field.
Certificate Index	The ordinal value used to access certificates on the card. The Certificate Index is used to bind a Certificate Label, Certificate and a set of Private Components together. The Certificate Index zero (0) is used for the Root Registry Certificate.
Certificate Label	The ASCII/ANSI string that is a human readable alias for a certificate. The Certificate Label is always 64 bytes long for FORTEZZA. The Certificate Label must be formatted in accordance with the "Certificate Labeling Format Specification".
CFB	8/16/32/64 Cipher Feedback
CIS	Card Information Structure.
COTS	Commercial-Off-The-Shelf components
DSA	Digital Signature Algorithm.
DSA-Yb	Digital Signature Algorithm Public Component of Recipient (128 bytes).
Even Word	A value or address where the 2 Least Significant Bits (LSB) are 00. Examples of 32-bit even word boundary addresses are: 0000 0000h, 0000 0004h, 0000 0008h, etc. All pointers on the card require 32-bit even word boundary addresses.
G	A DSA parameter (between 64-128 bytes) defined by the SSO. For FORTEZZA, G is a 128 byte parameter.
Gsize	Size of the G parameter.
Hash	An algorithm to digest any amount of data to a fixed size.
IV	Initialization Vector used in the encryption/decryption process.
Ks	The Storage Key Variable (80 bits). Stored in Register 0 after a successful Check PIN Phrase.
KEA	Key Exchange Algorithm for Electronic Public/Private Key Exchange.
KEA-Yb	Recipient's Public Component used in key exchanges (128 bytes).
Key Register Index	Index parameter to specify use of a temporary key storage register valid values are 0 - 31.
Key Registers	A set of temporary storage registers for storage of encryption keys.

LA	Local Authority (the SSO).
Long	32-bit big endian value
MEK	Message Encryption Key generated by the Card's random number generator.
OFB	64-bit Output Feedback
P	The prime modulus (64 - 128 bytes) used in the key exchange and DSA. For FORTEZZA, the prime modulus, P, is always 128 bytes.
PCMCIA	Personal Computer Memory Card International Association.
Personality	A certificate assigned to an individual (e.g. SSO, Self and Department). An individual may have more than one certificate for a person's different uses.
PIN Phrase	Personal Identification Number Phrase used to log onto the card.
Psize	The size of P, the prime modulus
Q	The prime divisor. For FORTEZZA, Q is always set to a 160 bit value.
Qsize	Denotes the size of the prime divisor Q, in bits.
R	One of the two parameters defining the digital signature (S is the other). For FORTEZZA, R is always 160 bits.
Ra	A 1024-bit random number generated for the public/private key exchange.
Rb	A 1024-bit random number received from the other party involved in the key exchange.
Root	The Root generates and signs all CAW certificates.
Root Certificate	The certificate used to validate certificates from the CAW and other users. Certificate Index 0 is where the Root certificate is located.
RTC	Real-Time Clock.
S	One of the two parameters defining the digital signature (R is the other). For FORTEZZA, S is always 160 bits.
Signature	A value used to authenticate that the data came from a specific author and has not been modified. The signature is composed of two parts: R and S. The R and S are always 160 bits each, making the Signature 320 bits for FORTEZZA.
SSO	Site Security Officer.
SSO Default PIN	The PIN (or PIN Phrase) that must be entered by a SSO to logon to the Card when it is being initialized, after receipt from the manufacturer. The SSO changes the default PIN to create a SSO unique PIN.
TEK	Token Encryption Key used with the KEA for the public/private key exchange.
Tuple	An information format defined by the PCMCIA specification. . A variable length chain of data blocks.

User Personality	Same as Personality.
User PIN	The PIN Phrase that must be entered by a User to logon to the Card. The SSO installs and changes the User PIN. The User is not allowed to change the User PIN for FORTEZZA.
Wrap	Encrypt one key with a different key.
X	User's secret component in the DSA or KEA exchange. For FORTEZZA, X is always 192 bits in length.
Y	User's public component in the DSA or KEA exchange.
Yb	Recipient's public component in the DSA or KEA exchange. For FORTEZZA, Yb is always 128 bytes.
Zeroize	A process that clears the User and SSO PIN Phrases, certificates, and key material stored on the Card.
Zeroize PIN	The default SSO PIN Phrase defined for all Card implementations. This PIN Phrase must be entered by the SSO to logon to the Card once it has been zeroized. Unlike other PINs, this PIN cannot be changed.

3. Cryptographic Boundary and Security Level

The 82A Fortezza Crypto Card is a cryptographic module designed to meet the overall security requirements of FIPS 140-1 security level 2 - see Section 1.1, reference 2. The cryptographic boundary (the boundary of the cryptographic module) is the edge of the card. Table 1 lists the security levels corresponding to each of the eleven security requirement sections of FIPS 140-1. The module does not contain an operating system, hence the requirements of that section do not apply.

Table 1: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module	2
Module Interfaces	2
Roles and Services	2
Finite State Machine	2
Physical Security	2
Software	2
Operating System Security	N/A
Key Management	2
Cryptographic Algorithms	2
EMI/EMC	3
Self Tests	2

4. Roles and Services

The 82A FORTEZZA cryptographic module supports two distinct operator roles. These operator roles are:

- User Role
- Site Security Officer (Cryptographic Officer) Role

The cryptographic module enforces the separation of operator roles using role-based operator authentication. An operator must select a role and then log-on using the appropriate access code (PIN phrase) for that role. At the end of each session the operator must log-out. The defined roles supported by the module are described in the following sections.

1. The Site Security Officer (SSO) Role

   This role is equivalent to the Crypto Officer Role defined in FIPS 140-1. An authorized operator acting in the SSO role has access to a set of cryptographic initialization or management functions which include setting of PIN phrases (SSO or User), archiving private keys and setting the Real-Time Clock (RTC), cryptographic key and parameter entry and cryptographic key cataloging. Most of these services are not available to the User Role

2. The User Role

   This role is equivalent to the User Role defined in FIPS 140-1. An authorized operator acting in the User role has access to all services provided by the module except those restricted to the SSO role only. See Table 3 for a definition of those services available for each role.

   Certain non-cryptographic card services (commands) may be called without the card being initialized. The services that may be performed prior to SSO or User log-on are marked with a (2) in Table 2.

4.1. List of Commands

The commands (services) executed by the 82A FORTEZZA Crypto Card are listed in Table 2.

Table 2, Operator Services Command Set

Change PIN (1)	Get Certificate	Restore (3)
Check PIN (2)	Get Hash (3)	Save(3)
Decrypt (3)	Get Personality List-	Set Key (3)
Delete Certificate	Get Status (2)	Set Mode (3)
Delete Key (3)	Get Time (2)	Set Personality
Encrypt (3)	Hash (3)	Set Time (1)
Extract X (1)	Initialize Hash (3)	Sign (3)
Firmware Update	Install X	Timestamp (3)
Generate IV (3)	Load Certificate	Unwrap Key (3)
Generate MEK (3)	Load DSA Parameters (3)	Verify Signature (3)
Generate Ra (3)	Load Initialization Values (1)	Verify Timestamp (3)
Generate Random No. (2)	Load IV (3)	Wrap Key (3)
Generate TEK (3)	Load X	Zeroize (2)
Generate X	Relay	Load BRAM (2)
Get Self Test Status (2)	Chip Self Test (2)	

Notes: (1) Commands available only to the SSO
(2) Commands may be called without the card being initialized
(3) Commands available only to the User

4.2. Command Descriptions

Please refer to the FORTEZZA Crypto Card Interface Control Document for a detailed description of each command.

Check PIN implements an SSO or User log-on to a card.

Change PIN is used by an SSO to change an old or default PIN to a new PIN.

Decrypt is a User command that will decrypt a block of encrypted data.

Delete Certificate deletes a specified certificate.

Delete Key deletes a specified key in a key register.

Encrypt is a User command that will encrypt a block of unencrypted data.

Extract X is used by an SSO to extract a TEK wrapped X-value for distribution or local storage purposes. The SSO may only extract an X that was loaded, installed, or generated by an SSO.

Firmware Update updates the firmware image stored in nonvolatile memory.

Generate IV generates an Initialization Vector (IV).

Generate MEK generates a random Message Encryption Key (MEK).

Generate Ra generates an R_a.

Generate Random generates a random number.

Generate TEK generates a Token Encryption Key (TEK) for public/private key exchange.

Generate X generates a public key pair, the private X and public Y keys.

Get Self Test Status returns the result status of the most recently executed selftest.

Get Certificate returns the specified certificate.

Get Hash hashes the last block of data and returns the final Hash value.

Get Personality List returns the list of personalities installed on this card.

Get Status returns the status code for the Card.

Get Time returns the current time from the Card's onboard real-time clock.

Hash hashes the specified block of data. Used repeatedly between *Initialize Hash* and *Get Hash*.

Initialize Hash initializes the hash value.

Install X is the reverse of Extract X.

Load Certificate loads the provided certificate into nonvolatile memory.

Load DSA Parameters allows a User to load externally supplied p, q and g parameters to use for signature verification outside of the domain of the currently selected personality. Note: an application will normally obtain the KEA and DSA p's, q's and g's from a reference file to build a FORTEZZA certificate.

Load Initialization Values enables an SSO to load a card's initialization parameters. These parameters include:

1. Random Seed Value
2. Storage Key Variable (Ks) - a plaintext value

Load IV loads an IV into the Card.

Load X loads the private key X into nonvolatile memory.

Relay transfers a TEK wrapped X from one workstation to another that is *not* the end destination of X.

Chip Self Test executes the SELFTEST ROM primitive that executes a full hardware self-test.

Restore restarts an interrupted process (see Save, below.) One (1) encryption/ decryption process plus one (1) hash process may be saved and restored at a time.

Save optionally may be used to interrupt encryption, decryption, and hashing.

Set Key is used by an application to select a Key Register, the contents of which will be used in following commands. Set Key is used like Set Personality.

Set Mode will initialize the cryptologic to the specified mode.

Set Personality selects a Certificate Register, the contents of which will be used in following commands.

Set Time enables an SSO to advance or stop the card's RTC (date and time). For security reasons, there is no way to reverse the card's RTC.

Sign computes a DSA digital signature over a provided Hash Value.

Timestamp computes a DSA digital signature over a provided hash value and the current time as provided by the Card's onboard real-time clock.

Unwrap Key unwraps the wrapped key into the specified key register using the unwrapping key in the specified key register.

Verify Signature validates a digital signature using the provided Hash Value and the signer's public key Y.

Verify Timestamp validates a digitally signed timestamp using the provided Hash Value and the provided date/time components.

Wrap Key wraps a plaintext key.

Zeroize will erase (or 'zeroize') all data buffers, internal buffers, key registers, certificates, and public/private key pairs. The PIN's will also be reset to the Zeroize Default PIN.

Load BRAM updates the data stored in the BRAM memory area using the provided binary image.

5. Security Rules

The security rules enforced by the 82A FORTEZZA Crypto Card are enumerated below.

1. There is only one SSO and one User per card.
2. After 10 consecutive unsuccessful SSO log-on attempts the SSO's PIN and all keying material are zeroized. After zeroization the PIN is set to a known ZEROIZED PIN value.
3. After 10 consecutive unsuccessful User log-on attempts the User's PIN value is zeroized requiring the user to return the card to the SSO.
4. Only an SSO may, load initialization value, set the date/time of the RTC, change the SSO and User PINs, and Extract an X-value
5. The only valid Cryptologic Commands that may be performed on a card prior to SSO or User log-on are Get Status, Get Time, Generate Random Number, Check Pin, and Zeroize.
6. Either a logged on User or SSO may load, generate, or install X-values. Only the SSO may load X-values and/or a certificate in Certificate Index 0.
7. The SSO can only extract X-values that the SSO created/loaded.
8. The cryptographic module implements the FIPS PUB 185 Escrowed Encryption Standard - see Section 2.1.4 - for encryption and decryption of message traffic. This standard specifies use of a symmetric-key algorithm (SKIPJACK). The module supports the following SKIPJACK modes: Electronic Codebook (ECB), 64 bit Output Feedback (OFB), Cipher Block Chaining (CBC) and 8/16/32/64 bit Cipher Feedback (CFB).
9. The cryptographic module implements an NSA designed asymmetric encryption algorithm called the Key Encryption Algorithm (KEA). KEA is used to generate a Token Encryption Key (TEK) which is used to wrap Message Encryption Keys (MEK) and Private keys (X).
10. The cryptographic module implements the FIPS PUB 180-1 Secure Hash Standard Secure Hash Algorithm (SHA-1).
11. The cryptographic module implements the FIPS PUB 186 Digital Signature Standard Digital Signature Algorithm (DSA).
12. Upon the application of power or upon receipt of a Reset command, the cryptographic module performs the power-up self-tests described below:
    a) Cryptographic Algorithm Test: Known answer tests are performed on all cryptographic algorithms implemented in hardware including SKIPJACK encrypt, Digital Signature Algorithm and Secure Hash Algorithm.
    b) Software/Firmware Test: ROM and non-volatile on-chip and off-chip memory tests are performed using a FIPS approved authentication technique.
    c) Random Number Generator Test: Functional testing of ring oscillators and LFSR is performed.
    d) Critical Functions Test: Known answer test on chip multiplier, Capstone BRAM test.

e) RAM Test: Functional test of RAM memory.

13. Conditional Tests.

a) Pairwise Consistency Tests: Test is performed.

b) Software/Firmware Load Test: A load test is performed.

c) Continuous Random Number Generator Test: A random number generator test is performed once upon every functional access of the random number generator (once regardless of the length of the random number needed).

14. The following initialization of the 82A FORTEZZA card must be accomplished by the SSO before the card will support User cryptographic services.

a) Install the card's Ks value (this is done in the Load Initialization Value service).

b) Change the SSO default PIN phrase (this is done in the Change PIN service when executed by the SSO).

c) Load a certificate into certificate index 0 (this is done in the Load Certificate service when executed by the SSO).

d) Set the User PIN Phrase (this is done in the Change PIN service).

15. Before the card can be used for cryptographic services the User must successfully log on and select a personality (certificate). Prior to selecting a personality, card services that do not require a user's private key may be selected.

16. When the card is in a Zeroized state, as the result of a Zeroize command or of 10 consecutive unsuccessful log on attempts by the SSO, the SSO must use the Zeroize PIN phrase to log on. All card parameters must then be reinitialized.

17. After 4096 failed attempts, total, not consecutive, to load an IV the User PIN value is zeroized and the User is logged out.

18. The card can be used to store at least 32 wrapped TEKSs or MEKs. Keys are accessed using a key or register index of 0 to 31.

19. Key register 0 is reserved for storing the wrapped storage Key (Ks).

20. The wrapped Ks cannot be extracted from the card (i.e., you cannot use WrapKey to extract Ks).

21. The card can be used to store at least 27 certificates. The certificates are accessed using a certificate index.

22. Certificate index 0 is reserved for the Policy Approval Authority certificate.

23. The Generate X command may not specify certificate PIN index 0.

24. The Load X command may not specify certificate index 0.

25. The User cannot use InstallX to restore an X to certificate index 0.

26. Public components for key exchange are not stored on the card.

27. A known IV value may be loaded prior to an encrypt operation.

6. Security Relevant Data Items

The Security Relevant Data Items (SRDIs) are defined below.

Certificate: An internal data structure containing a public X.509 certificate plus a private KEA and DSA information about a User. The structure of the FORTEZZA version of the X.509 certificate is defined in the FORTEZZA Application Implementors Guide - Section 2.1, 9.

Cipher mode: The selected cipher mode, either ECB, CBC, OFB, or CFB.

Data: Plain text or Cipher text data.

g parameter: One of the parameters used with the KEA and DSA.

Hash: The value produced by "digesting of a message" using the Secure Hash Algorithm.

Manufacturer Default PIN: The SSO PIN phrase that must be entered to log-on to the card when it is first received from the manufacturer.

Message Encryption Key (MEK): The Key generated by the card's random number generator, used for encrypting/decrypting message data.

Message Initialization Vector (IV): This is a 64 bit random number used to initialize the SKIPJACK encryption algorithm - see Section 2.1, 4. The algorithm is initialized with a unique IV for each message encrypted.

BRAM Public Key: A DSA key used to verify a BRAM image prior to actually loading into BRAM.

p parameter: A prime number used in the KEA and DSA.

q parameter: A prime divisor used in the KEA and DSA.

r value: One of two parameters used in DSS to define a digital signature (s is the other).

Ra: A random number generated by the message originator in a KEA key exchange.

Rb: A random number received from the message recipient in a direct-connection key exchange.

Time: The date and time maintained by the on-board RTC. Only the SSO can set (advance or stop) the RTC.

s value: One of two parameters used in DSS to define a digital signature (r is the other).

SSO Role PIN: The PIN phrase that must be input to enter the SSO role.

Status: The current module state, mode & personality status.

Token Encryption Key (TEK): A value generated by the KEA. Used to wrap keys.

User Role PIN: The PIN phrase that must be input to enter the User role.

Storage Key Variable (Ks): This Key is stored in Register 0 after a successful Check PIN phrase.

User's Private Key (X): This is the private part of the Public/Private key pair used in the Key Encryption Algorithm (KEA) and the DSA.

User's Public Key (Y): This is the public part of the Public/Private key pair used in the Key Encryption Algorithm and the DSA.

Zeroize Default PIN: The SSO PIN phrase that must be entered to log-on to the card once it has been zeroized.

7. Modes of Access

Terms used in the Modes of Access column of Table 3 are described below:

Clear (index#): Clear SRDI at register index # n.

Generate: The SRDI is generated by the card.

Initialize: Hash function command.

Initiate/Continue: Hash function commands

Input: Data input to the card via the Data In Block.

Input (index#): Input SRDI into register index # n.

Output: Data output from the card via the Data Out Block.

Output (index#): Output of SRDI from register index # n.

Retrieve: The SRDI is retrieved from card storage.

Select: Selection of parameters or mode.

Select (index#): Selection of a key or certificate from index # n.

Store: The SDRI is stored in the Crypto Card

Unwrap: Decrypt one key with a different key.

Verify: DSA Signature Verification.

Wrap: Encrypt one key with a different key.

Zeroize: A process that clears User and SSO PIN phrases, and other memory on the card, as required.

The host application program and the 82A FORTEZZA Crypto Card communicate by means of a shared memory interface consisting of a Command Block, a Data-In Block and a Data-Out Block. The application places a Command Block at the start address of the card's shared memory. The Command Block is made up of six fields: Command, Pointer to Next Command Block, Pointer to Data-In, Pointer to Data-Out, Response, and Channel Specifier. The Data-In Block is used to provide input data to commands executed on the card. The Data-Out Block is used to provide output data to the application program. Keys are stored in Key Registers which the host selects based upon their Key Register Index Identifier. The card contains storage for 32 keys identified by Key Register Index 0 through 31. Register 0 is used for storing wrapped Ks. The card contains storage for certificates including one SSO certificate and multiple User certificates. These are stored according to a certificate index.

8. Matrix of User & SSO Services, SRDIs and Modes of Access

The relationships between User and SSO Services, SRDIs and Modes of Access to SRDIs are shown in Table 3.

Table 3: Matrix of Services, SRDIs and Modes of Access

Service	SRDI	Modes of Access	SSO Role	User Role
Change PIN phrase	PIN (current) PIN (new) SSO/User type Ks	Input Input Input Unwrap, wrap	X	
Check PIN phrase	PIN Ks p, q & g parameters, same values always used	Input Unwrap, wrap, move to register 0 Retrieve	X	X
Chip Self Test			X	
Decrypt	Data - cipher text Data - plain text	Input Output		X
Delete Certificate	Certificate	Clear (index#)	X	X
Delete Key	MEK / TEK	Clear (index#)		X
Encrypt	Data - plain text Data - cipher text	Input Output		X
Extract X	Selected X-value	Output (TEK wrapped X value)	X	
Firmware Update	DSA Public Key	Verify	X	X
Generate IV	IV data	Generate, output		X
Generate MEK	MEK	Generate, wrap, store (index #)		X
Generate Ra (Ra is used in generation of TEK)	Ra	Generate, output		X
Generate Random No.	Random number	Generate, output	X	X
Generate TEK (TEK used in Encrypt, Decrypt, Wrap)	Ra or Rb Yb or Ya TEK, X p, q and g	Input Input Generate, wrap, store (index #) Select Select		X

Service	SRDI	Modes of Access	SSO Role	User Role
Generate X	X-value Y-value p, q, & g parameters certificate	Generate, wrap, store Generate, output Input, store Select(index#)	X	X
Get Certificate	Certificate	Output (index#)	X	X
Get Hash	Hash (value)	Output (hash value)		X
Get Personality List	Certificates	Output (all certificate names in memory)	X	X
Get Self Test Status			X	X
Get Status	Status (state, mode, personality)	Output (status)	X	X
Get Time	RTC	Output (date/time)	X	X
Hash	Hash (function)	Initiate/continue		X
Initialize Hash	Hash (function)	Initialize (per SHA-1)		X
Install X (used to restore an archived X-value	X-value Yb p, q, & g parameters	Input, unwrap, wrap (index#) Input Input, store	X	X
Load BRAM	BRAM Public Key	Verify	X	
Load Certificate[1]	Certificate	Input (index#)	X	X
Load DSA Parameters	p, q & g parameters	Input		X
Load Initialization Value	Random seed value Ks (user key)	Input Input, wrap	X	
Load IV	IV data	Input		X
Load X[2]	X p, q, & g parameters Y generated value	Input, wrap (index#) Input (index#) Generate Output	X	X

[1] Only the SSO may load a Certificate into certificate index 0.
[2] Only the SSO may load an X-value into index 0.

Service	SRDI	Modes of Access	SSO Role	User Role
Relay	X-value Ra Ya (extractor) Yb (installer) TEK	Input, unwrap, wrap Input, generate, output Input Input Generate (for unwrap, Generate (for wrap)	X	X
Restore	Crypto state (hash, encrypt, or decrypt)	Input (hash-value, or encrypt /decrypt state)		X
Save	Crypto state (hash, encrypt, or decrypt)	Output, store (hash-value, or encrypt or decrypt state)		X
Set Key	MEK / TEK	Select (index#), unwrap		X
Set Mode	Cipher mode (ECB /CBC/OFB/CFB)	Select (cipher mode)		X
Set Personality	Certificate	Select (index#)	X	X
Set Time	RTC	Input (date/time)	X	
Sign	Hash (value) X p, q & g r value s value	Input Select, unwrap Select Output Output		X
Timestamp	Hash value X p, q, & g, same values always used r value s value time (signed)	Input Select, unwrap Retrieve Generate, output Generate output Output		X
Unwrap Key	TEK MEK	Select(index#),unwrap Select(index#),unwrap		X
Verify Signature	Hash value p, q & g r value s value Y value (originator)	Input Select Input Input Input		X

Service	SRDI	Modes of Access	SSO Role	User Role
Verify Timestamp	p, q, & g, same values always used. Y, same value always used Hash Value r value s value time (signed)	Retrieve Retrieve Input Input Input Input		X
Wrap Key	TEK MEK	Select (index#), unwrap Select (index#), unwrap, wrap		X
Zeroize	Card data & internal buffers	Zeroize	X	X