kasten chase

HIGH-ASSURANCE DATA SECURITY

Enterprise RASP

Security Policy
For
RASP Secure Modem

Synopsis:

This document describes the Security Policy for the RASP Secure Modem. The Security Policy specifies the security rules under which the RASP Secure Modem operates. This document covers the security-related services of the RASP Secure Modem and is not intended to address non-security related RASP Secure Modem services and functions.

Author(s):	Kathir (Nathan) Nadarajah	
Contributors:	Patrice St. Louis	
Reviewer(s):	Kasten Chase:	Patrice St. Louis, Garry McCracken, Serge Rioux, Bill Colvin, Steve Demmery, Peter Andruski
	Mykotronix:	Blane Yamamoto
	CEAL:	Miles Smid

Filename:	SecurityPolicyRASP_15.doc
Status:	Version 1.5 FINAL
Revision Date:	August 13, 2001
Print Date:	August 13, 2001

Approvals

Serge Rioux, Data Security Market Manager, Kasten Chase Applied Research	Date
Bill Colvin, Chief Technology Officer, Kasten Chase Applied Research	Date
Garry McCracken, Vice President of Operations, Kasten Chase Applied Research	Date

Revision History Table

Revision	Changes Since Previous Revision
Version 1.0 DRAFT A	This is the initial release of the document.
Version 1.0 DRAFT B	Updated with comments from Kasten Chase reviewers.
Version 1.0 FINAL	Updated with comments from customer.
Version 1.1 DRAFT A	Updated with comments from customer.
Version 1.1 FINAL	Draft A Released.
Version 1.2 DRAFT A	Updated with comments from Miles Smid.
Version 1.2 FINAL	Draft A Released.
Version 1.3 FINAL	Updated section 6.1.3 to better define the term Mode of Access
Version 1.4 FINAL	Updated section 6.0 to clarify the FIPS approval mode and card's operation. Updated section 7.0, security rule # 3 to clarify what becomes of the "user" parameters after the 10^{th} unsuccessful user logon attempt; security rule # 12d is corrected to refer SHA-1. Updated section 5.0 to define SRDI term KFEK
Version 1.5 FINAL	Updated Section 3 to define the term LAW.

TABLE OF CONTENTS

1. Introduction

1.1 Purpose

This document describes the Security Policy for the RASP Secure Modem. The Security Policy specifies the security rules under which the RASP Secure Modem operates.

The RASP Secure Modem is a Type II PC Card with an external adapter that houses the Data Access Arrangement (DAA) and the Real-Time Clock circuitry. It consists of a cryptographic module and a Micro Control Unit/Modem Data Pump (MCU/MDP) component to achieve V.34 modem operation. The cryptographic module 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 Algorithm Standard – see Section 2.1, 4. The RASP Secure Modem uses a communication protocol in conjunction with a dual asynchronous FIFO between the MCU and the Crypto Engine. This communication protocol is used by the MCU to request security functions from the Crypto Engine. The RASP Secure Modem complies with PCMCIA specification Standard Release 2.1 – see Section 2.2, 1.

The RASP Secure Modem has two operating modes: Secure Modem and FORTEZZA. The dots on the case indicate the current switch setting and the operating mode. The yellow dot indicates that the modem is operating in "Secure Modem" mode, whereas the blue dot indicates that the modem is operating in "FORTEZZA®" mode.

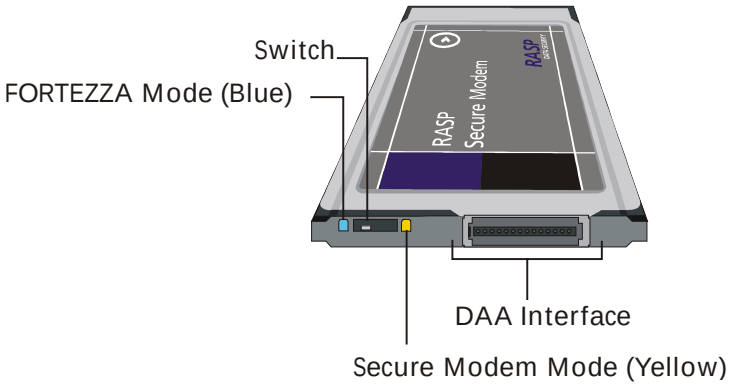

Figure 1: RASP Secure Modem - Dual Mode Functionality

1.2 Scope

This document covers the security-related services of the RASP Secure Modem and is not intended to address non-security related RASP Secure Modem services and functions.

2. Applicable Documents

2.1 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, Digital Signature Algorithm Standard (DSA), NIST, 19 May 1994

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

7. FORTEZZA® Application Implementers Guide, National Security Agency (NSA), Workstation Security Products, Document #MD4002101-1.52, 5 March 1996

8. FORTEZZA® Skipjack and KEA Algorithm Specifications, 13 February 1998

2.2 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

3. Security Policy for Palladium Secure Modem, Rev A, Nov. 20, 1998.

3. Terms and Abbreviations

CA	Certificate Authority. A Certificate Authority registers end-users, issues their certificates, and can also create CAs below them. The CA also periodically issues a CRL that lists the certificates of revoked users who were created by the CA.
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 RASP Secure Modem. 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 the RASP Secure Modem. 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.
CRL	Certificate Revocation List. A list of FORTEZZA® card certificates that, although they are still within their validity intervals, they can no longer represent valid bindings between user public keys and distinguished names.
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 RASP Secure Modem require 32-bit even-word boundary addresses.
g Parameter	A DSA parameter (between 64 - 128 bytes) defined by the SSO. For the RASP Secure Modem, g is a 128-byte parameter.
Gsize	The size of the g parameter.
Hash	An algorithm to reduce any amount of data to a fixed size.
ICRL	Indirect Certificate Revocation List. A list of FORTEZZA® keys that the Policy Creation Authority (PCA) believes to be compromised and that are no longer trustable.
ICRLA	Indirect Certificate Revocation List Authority. The ICRLA is a special purpose authority for issuing a single ICRL file for the entire PAA domain. An ICRLA is a subject and asset to the PAA. The sole responsibility of the ICRLA is to manage the ICRL that lists every certificate within the PAA domain (and, optionally, cross-certified domains) that has been revoked due to a key compromise.

IV	Initialization Vector used in the encryption/decryption process.
Ks	The RASP Secure Modem's Card 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 the use of a temporary key storage register. Valid values are 0 - 9.
Key Registers	A set of temporary storage registers for storage of encryption keys.
KFEK	A value generated by the MYK-82 cryptographic processor chip during initialization. It is used for encrypting the storage key for protection when it is stored in non-volatile memory.
KRL	Key material Revocation List. Alternately, the Compromised Key List (CKL). Lists the KMIDs of users who have lost control of their Cards and PINs or who are a threat to the security of the system. All certificates on a KRL (or CKL) are also placed on a CRL.
LA	Local Authority (the SSO).
LAW	Local Authority Workstation. The physical workstation used by the Local Authority and Root. A major part of the system infrastructure, it is used to perform certificate, CRL and KRL management and Card initialization functions.
Long	32-bit big endian value.
MCU	Micro Control Unit.
MDB	Modem Data Pump.
MEK	Message Encryption Key generated by the RASP Secure Modem's random number generator.
OFB	64-bit Output Feedback.
p Parameter	The prime modulus (64 - 128 bytes) used in the key exchange and DSA. For the RASP Secure Modem, the prime modulus, p is always 128 bytes.
PAA	Policy Approval Authority. It is the top level authority in a certificate hierarchy tree. A PAA creates ICRLAs, register PCAs, and signs their certificates. A PAA can also issue a CRL file.
PCA	Policy Creation Authority. It is an administrative root of a security policy domain of end-users and other subsidiary authorities. A PCA registers the CAs in its domain, defines their configurations, and issues their certificates. A PCA has the capability to issue certificates to end-users and other end-entities, but is not expected to do this. The PCA will periodically issue a CRL for its domain. The CRL file lists the certificates of revoked CAs in the PCA's domain (this also includes any users who the PCA created).
PCMCIA	Personal Computer Memory Card International Association.
Personality	A certificate assigned to an individual (for example, 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 logon to the RASP Secure Modem.
Psize	The size of p, the prime modulus.

q Parameter	The prime divisor. For the RASP Secure Modem, q is always set to a 160-bit value.
Qsize	The size of the prime divisor q, in bits.
R Parameter	One of the two parameters defining the digital signature (s is the other). For the RASP Secure Modem, r is always 160 bits.
Ra	A 1024-bit random number generated for the 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 Parameter	One of the two parameters defining the digital signature (r is the other). For the RASP Secure Modem, 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 the RASP Secure Modem.
SRDI	Security Relevant Data Item. SRDIs are the sensitive data elements owned by the cryptographic application that requires protection. Examples include cryptographic keys and access control profiles.
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 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 the RASP Secure Modem.
Wrap	Encrypt one key with a different key.
x	The x value is wrapped with Ks and is stored in non-volatile memory in their associated certificate index location. It is the User's secret component. For the RASP Secure Modem, x is always 160 bits in length and the stored wrapped value is 192 bits.
y	User's public component in the DSA or KEA exchange (1024 bits or 128 bytes).
Yb	Recipient's public component in the DSA or KEA exchange. For the RASP Secure Modem, Yb is always 1024 bits or 128 bytes.
Zeroize	A process that clears the User and SSO PIN Phrases, certificates, and key material stored on the RASP Secure Modem.

Zeroize PIN	The default SSO PIN Phrase defined for all RASP Secure Modem implementation. This PIN Phrase must be entered by the SSO to logon to the RASP Secure Modem once it has been zeroized. Unlike other PINs, this PIN cannot be changed.

4. Cryptographic Boundary and Security Level

The RASP Secure Modem is a multi-chip standalone cryptographic module designed to meet the overall security requirements of FIPS 140-1 security level-1 - see Section 2.1, 2. The cryptographic boundary (the boundary of the cryptographic module) is the edge of the RASP Secure Modem. Table 1 lists the security levels corresponding to each of the eleven security requirement sections of FIPS 140-1. The module does not execute untrusted software, which is the FIPS condition.

Table 1: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module	1
Module Interfaces	1
Roles and Services	1
Finite State Machine	1
Physical Security	1
Software	1
Operating System Security	N/A
Key Management	1
Cryptographic Algorithms	1
EMI/EMC	3
Self Tests	1

5. Security Relevant Data Items

Security Relevant Data Items (SRDIs) are defined below:

Certificate: An internal data structure containing a public V 3.0 X.509 DSA/KEA certificate and private KEA and DSA information about a User. The structure of the RASP Secure Modem version of the V3 X.509 certificate is defined in the SDN.706 X.509 Certificate and Certificate Revocation List Profiles and Certificate Path Processing Rules for MISSI documents.

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.

Key File Encryption Key (KFEK): A value generated by the MYK-82 cryptographic processor chip during initialization. It is used for encrypting the storage key for protection when it is stored in non-volatile memory.

Manufacturer Default PIN: The SSO PIN phrase that must be entered to logon to the RASP Secure Modem when it is first received from the manufacturer.

Message Encryption Key (MEK): The Key generated by the RASP Secure Modem's random number generator that is 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 encrypted session.

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, and personality status.

Token Encryption Key (TEK): A value generated by the KEA. It is 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 Exchange Algorithm (KEA) and the Digital Signature Algorithm (DSA).

User's Public Key (y): This is the public part of the Public/Private key pair used in the Key Exchange Algorithm (KEA) and the Digital Signature Algorithm (DSA).

Zeroize Default PIN: The SSO PIN phrase that must be entered to logon to the RASP Secure Modem once it has been zeroized.

6. Roles and Services

The cryptographic module is designed to be fully compliant with FIPS 140-1 security level-1 with two supported modes – FORTEZZA and Modem. One user at a time can operate the card in either one of these supported modes.

6.1 FORTEZZA Mode

The RASP Secure Modem cryptographic module in FORTEZZA mode supports two distinct operator roles:

- Site Security Officer (Cryptographic Officer)
- User

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

6.1.1 Site Security Officer (SSO) Role

This role is equivalent to the Cryptographic 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 that include setting 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.

Note: The SSO does not have access to all User commands.

6.1.2 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 2 for a definition of those services available for each role.

Certain non-cryptographic card services (commands) may be called without logging into the RASP Secure Modem. The services that may be performed prior to SSO or User logon are marked with a (2).

6.1.3 Matrix of Commands, User & SSO Services and SRDIs

The services (commands) supported by the MYK-82 FORTEZZA Crypto Engine and the relationships between User and SSO Services, SRDIs and SRDI Modes of Access are shown in Table 2. For a detail description of each command, refer to the FORTEZZZA Crypto Card Interface Control Document. SRDI Modes of Access indicates how the SRDIs are used and affected by commands. Terms used in the SRDI Modes of Access column of Table 2 are described below:

Clear (index#):	Clears SRDI at register index # n.
Generate:	The SRDI is generated by the RASP Secure Modem.
Initialize:	Hash function command.
Initiate/Continue:	Hash function command.
Input:	Data input to the RASP Secure Modem via the Data-In Block.
Input (index#):	Input SRDI into register index # n.
Output:	Data output from the RASP Secure Modem via the Data-Out Block.
Output (index#):	Output of SRDI from register index # n.
Retrieve:	The SRDI is retrieved from RASP Secure Modem storage
Select:	Selection of parameters or mode.
Select (index#):	Selection of a key or certificate from index # n.
Store:	The SRDI is stored in the Crypto Card.
Unwrap:	Decrypt one key with a different key.
Wrap:	Encrypt one key with a different key.
Zeroize:	A process that clears User and SSO PIN phrases, and other memory on the RASP Secure Modem, as required.

The host application program and the RASP Secure Modem in “FORTEZZA” mode, communicate by means of a shared memory interface that consists 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 RASP Secure Modem’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 provides input data to commands that are executed on the RASP Secure Modem. The Data-Out Block provides

output data to the application program. Keys are stored in Key Registers that the host selects based upon their Key Register Index Identifier. The RASP Secure Modem contains storage for 10 keys identified by Key Register Index 0 through 9. Register 0 is used for storing wrapped Ks. The RASP Secure Modem contains storage for certificates including one SSO certificate and multiple User certificates. These are stored according to a certificate index.

Table 2: Matrix of Services, SRDIs and Modes of Access

Service/Command	Description	SRDI	SRDI Modes of Access	SSO Role	User Role
Change PIN	Used by an SSO to change an old or default PIN to a new PIN.	PIN (current) PIN (new) SSO/User type Ks	Input Input Input Unwrap, wrap	X	
Check PIN (2)	Implements an SSO or User logon to a RASP Secure Modem.	PIN Ks p, q & g parameters, same values always used	Input Unwrap, wrap, move to register 0 Retrieve	X	X
Decrypt	Decrypts user data.	Data - cipher text Data - plain text	Input Output		X
Delete Certificate	Zeroizes the certificate and certificate label, the private component (x), public component (y), and public key parameters (p, q, and g) associated with the certificate specified by the certificate index	Certificate	Clear (index#)	X	X
Delete Key	Deletes the Key.	MEK / TEK	Clear (index#)		X
Encrypt	Encrypts user data.	Data - plain text Data - cipher text	Input Output		X
Extract x	Used by an SSO to extract a TEK wrapped x-value for distribution or local storage purposes. The SSO may only extract a x that was loaded, installed, or generated by an SSO.	Selected x-value	Output (TEK wrapped x value)	X	

Service/Command	Description	SRDI	SRDI Modes of Access	SSO Role	User Role
Firmware Update	Loads new firmware to the RASP Secure Modem. This command supports a secure firmware update that allows the user or SSO to download Crypto Engine Firmware with a DSA signature as the last 60 bytes. Crypto Engine firmware code stores public component (y) and public key parameters (p, q, and g) that corresponds to Kasten Chase's private component (x) that is used to sign the firmware. These parameters are used to verify the signature during a code download process. If the signature verification succeeds, the downloaded code is written to the Crypto Engine code space. If the signature verification fails, the downloaded code is rejected.	RASP Secure Modem F/W	Store	X	X
Generate IV	Generates an initialization vector.	IV data	Generate, output		X
Generate MEK	Generates a random Message Encryption Key.	MEK	Generate, wrap, store (index #)		X
Generate Ra	Generates a Ra. Ra is used in generation of TEK.	Ra	Generate, output		X
Generate Random Number	Generates a Random Number.	Random number	Generate, output	X	X
Generate TEK	Generates a Token Encryption Key (TEK) for a key exchange. TEK used in Encrypt, Decrypt, and Wrap.	Ra or Rb Yb or Ya TEK, x p, q, and g parameters	Input Input Generate, wrap, store (index #) Select Select		X

Service/Command	Description	SRDI	SRDI Modes of Access	SSO Role	User Role
Generate x	Generates a public key pair, private component (x), and public component (y) of the type specified by the algorithm type.	x-value y-value p, q, and g parameters certificate	Generate, wrap, store Generate, output Input, store Select(index#)	X	X
Get Certificate	Returns the certificate associated with the certificate index.	Certificate	Output (index#)	X	X
Get Hash	Hashes the last block of data and returns the final hash value	Hash (value)	Output (hash value)		X
Get Personality List	Returns the list of structures containing a certificate index and a certificate label.	Certificates	Output (all certificate names in memory)	X	X
Get Status	Returns the status of the RASP Secure Modem.	Status (state, mode, personality)	Output (status)	X	X
Get Time	Retrieves and returns the current time from the real time clock of the DAA attached to the RASP Secure Modem.	RTC	Output (date/time)	X	X
Hash	Hashes the user data.	Hash (function)	Initiate/continue		X
Initialize Hash	Initializes the Hash	Hash (function)	Initialize (per SHA-1)		X
Install x	Installs a previously extracted (x). See Extract x. (used to restore an archived x-value).	x-value Yb p, q, and g parameters	Input, unwrap, wrap (index#) Input Input, store	X	X
Load Certificate	Loads a certificate into the non-volatile memory of the RASP Secure Modem.	Certificate	Input (index#)	X	X[1]

[1] Only the SSO may load a Certificate into certificate index 0.

Service/Command	Description	SRDI	SRDI Modes of Access	SSO Role	User Role
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, q, and g parameters from a reference file to build a RASP Secure Modem certificate.	p, q, and g parameters	Input		X
Load Initialization Value	Enables an SSO to load a RASP Secure Modem's initialization parameters. These parameters include: • Random Seed Value • Storage Key Variable (Ks) - a Plain text value	Random seed value Ks (user key) KFEK	Input Input, wrap Input, wrap	X	
Load IV	Loads an initialization vector (IV) to the RASP Secure Modem for decryption operations.	IV data	Input		X
Load X	Loads a user specified value (x) and generates the public component (y).	x p, q, and g parameters y generated value	Input, wrap (index#) Input (index#) Generate Output	X	X[2]
Relay	Transfers a TEK wrapped x from one workstation to another that is **not** the end destination of x.	x-value Ra Ya (extractor) Yb (installer) TEK	Input, unwrap, wrap Input, generate, output Input Input Generate (for unwrap, Generate (for wrap)	X	X

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

Service/Command	Description	SRDI	SRDI Modes of Access	SSO Role	User Role
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.	Crypto state (hash, encrypt, or decrypt)	Input (hash-value, or encrypt /decrypt state)		X
Save	May be used to interrupt encryption, decryption, and hashing. This is optional.	Crypto state (hash, encrypt, or decrypt)	Output, store (hash-value, or encrypt or decrypt state)		X
Set Key	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.	MEK / TEK	Select (index#), unwrap		X
Set Mode	Used to set the cryptologic mode to the specified mode for the specified cryptologic operation.	Cipher mode (ECB /CBC/OFB/CFB)	Select (cipher mode)		X
Set Personality	Selects a Certificate Register, the contents of which will be used in following commands.	Certificate	Select (index#)	X	X
Set Time	Enables an SSO to advance or stop the modem's RTC (date and time). For security reasons, there is no way to reverse the RASP Secure Modem's RTC.	RTC	Input (date/time)	X	
Sign	Computes a digital signature using the Digital Signature Algorithm (DSA).	Hash (value) x p, q, and g parameters r value s value	Input Select, unwrap Select Output Output		X

Service/Command	Description	SRDI	SRDI Modes of Access	SSO Role	User Role
Timestamp	Generates a digital signature over the provided hash value and the current time from the Real-Time Clock of the DAA that is attached to the modem.	Hash value x p, q, and g parameters, same values always used r value s value time (signed)	Input Retrieve Generate, output Generate output Output		X
Unwrap Key[3]	Unwraps the wrapped key using the key in the key register that is indicated by unwrap index.	TEK MEK	Select(index#),unwrap Select(index#),unwrap		X
Verify Signature	Validates a digital signature and signer's public component (y).	Hash value p, q, and g parameters r value s value y value (originator)	Input Select Input Input Input		X
Verify Timestamp	Validates the hash value and time stamp with the supplied public component (y).	p, q, and g parameters, same values always used y, same value always used Hash Value r value s value time (signed)	Retrieve Retrieve Input Input Input Input		X

[3] Key index 0 can not be used as the unwrapped key destination.

Service/Command	Description	SRDI	SRDI Modes of Access	SSO Role	User Role
Wrap Key	Wraps the plain text key in the key register indicated by the key index with the key in the key register indicated by the wrap index.	TEK MEK	Select (index#), unwrap Select (index#), unwrap, wrap		X
Zeroize	Zeroizes the RASP Secure Modem's data buffers, internal buffers, key management information, personalities, all public key pairs (x and y), all key registers and disallows user access.	RASP Secure Modem data and internal buffers	Zeroize	X	X

6.2 Modem Mode

When the RASP Secure Modem in this mode, it only supports the user role and the following extended AT commands are available via a PCMCIA RS-232 serial interface. For a complete list of supported commands, refer to the *RASP Secure Modem/RASP Client User Guide*.

Table 3: Extended AT Command List

Command	Description
ATI3	Displays the Version String: Reports the base firmware version, basic model, application code, interface type code, MCU firmware version and MYK-82 Crypto Engine firmware version
ATI4	Displays the modem's identifier string.
ATX	Disables / Enables Extended Connect Message: This command disables / enables the extended connect message. The default is enabled.
ATZ	MCU / MYK-82 Crypto Engine Reset: Performs a soft reset and restores the configuration profile according to the parameter supplied. If no parameter is specified, zero is assumed. The command structure is as follows: ATZ<cr> Soft reset and restore stored profile 0 ATZ0<cr> Soft reset and restore stored profile 0 ATZ1<cr> Soft reset and restore stored profile 1
AT!C	PIN Entry: The PIN command accepts case-sensitive, alphanumeric Personal Identification Number's (PIN's). The PIN size is between four and 12 characters and is delimited using the left and right bracket symbol, [ ]. The command structure is as follows: AT!C[xxxxxxxxxxxx]<cr> where x is the PIN The PIN is transferred to the Crypto Engine for verification.
AT!E	Gets the Local Status Message: This command retrieves the local status message (LSM). The command structure is as follows: AT!E<cr>
AT!L	Lists the Personalities: The List Personalities command allows the host user to retrieve all KEA K type personalities that are available on the RASP Secure Modem. The command structure is as follows: AT!L<cr>
AT!S	Sets the Personality: The Set Personality command allows the host user to select one of the personalities returned in the List Personalities command. The command structure is as follows: AT!Sxx<cr> where xx is a decimal number between 1 and 26

Command	Description
AT**0	Secure Code Download: The Secure Code Download command allows code that has a DSA signature to be loaded into the modem's MCU code space. The code image is sent from the DTE as 128K bytes of binary data with the DSA signature as the last 60 bytes of the 128K bytes. The modem's MCU executes the "Verify MCU Code DSA" command, passing the code to the Crypto Engine to verify the signature using Digital Signature Algorithm (DSA). All cryptographic functions are disabled until a signature is verified. When the signature is successfully verified, the loaded code is written to the MCU code space. If signature verification fails, the code is rejected. The command structure is as follows: Step 1: AT**<cr> or AT**0<cr>
AT**1	ICRL Download: The ICRL download command allows the host system to update the ICRL. Prior to the ICRL download, the user must login and set a personality. The command structure is as follows: Step 1: AT**1<cr> Step 2: Send ICRL file (in binary format with length of the file in the first two bytes in big endian format)

In this mode, the internal MYK-82 FORTEZZA Crypto Engine provides services (commands) to the Modem Control Unit to perform cryptographic operations. Table 4 lists these internal services.

Table 4: MYK-82 FORTEZZA Crypto Engine Internal commands used by MCU

Command (Value)	MYK-82 Action
Soft Reset (0x00)	Initialize Crypto Engine.
Encrypt Data (0x01)	Encrypts one byte of user data using SKIPJACK 8-bit CFB mode.
Decrypt Data (0x02)	Decrypts one byte of user data using SKIPJACK 8-bit CFB mode.
Get KEA Packet (0x03)	Sends a KEA packet containing Ra and IV parameters to the MCU.
Load KEA Packet (0x04)	Receives a KEA packet containing Ra and IV parameters from the MCU.
Check PIN (0x05)	Accepts a PIN that consists of four (4) to twelve (12), case-sensitive, alphanumeric characters and validates it.
Get Software Version (0x06)	Sends four (4) ASCII characters to the MCU that represent the firmware version.
Get ICRL (0x07)	Sends an ICRL to the MCU.
Load ICRL (0x08)	Accepts and validates an ICRL from the MCU.
Get X.509 V3 Certificate Chain (0x09)	Sends a X.509 V3 Certificate Chain or a ICRLA V3 certificate to the MCU.
Load X.509 V3 Certificate Chain (0x0A)	Accepts a X.509 V3 Certificate chain from the MCU or a ICRLA V3 certificate.
Verify MCU Code DSA (0x0B)	Modem MCU uses this command to verify the signature of the MCU code during code download and to verify the integrity of

Command (Value)	MYK-82 Action
	the code during power up or upon reset. Crypto Engine uses the Digital Signature Algorithm (DSA) to verify the signature attached to the end of the MCU code block. Crypto Engine verifies the intergrity of the code by computing the hash over the code using SHA-1 and verifying that against the stored hash value.
Get Status Message (0x0C)	Sends the local status message or the extended connect message data structure to the MCU.
Get Personality List (0x0D)	Returns a list of KEA K type personalities stored on the RASP Secure Modem.
Set Personality (0x0E)	Allows the user to select a personality to use for the KEA exchange.
Get ICRL Information (0x0F)	Sends ICRL information (ICRLA Distinguished Name or ICRL serial number) to the MCU.
Load ICRL Information (0x10)	Receives ICRL information from the MCU and compares it to the ICRL information stored in the Crypto Engine address space.

7. Security Rules

The security rules enforced by the RASP Secure Modem's Crypto Engine are enumerated below:

1. There is only one SSO and one User per modem.
2. After 10 consecutive unsuccessful SSO logon attempts, all data in the card including the SSO's PIN, all keying material are lost and the card will transition into the Zeroized State. After zeroization of security parameters, the SSO PIN is set to a known ZEROIZED PIN value
3. After 10 consecutive unsuccessful User logon attempts, the card zeroizes the User PIN and transitions to the LAW Initialized State. However other User data in the card is not lost. The user **must** return the card back to the SSO.
4. Only an SSO may load initialization values, set the date/time of the RTC, change the SSO and User PINs, and extract a wrapped x-value.
5. The only valid Cryptologic Commands that may be performed on a modem prior to an SSO or User logging on to the modem are: Get Status, Get Time, Generate Random Number, Check PIN, and Zeroize.
6. Either a logged-on User or SSO may update firmware, load, generate, or install wrapped x-values. Only the SSO may load wrapped x-values and/or a certificate in Certificate Index 0.
7. Only the SSO can extract wrapped x-values and only those x-values generated, loaded, or installed by the SSO may be extracted.
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 a NSA designed asymmetric encryption algorithm called the Key Encryption Algorithm (KEA). KEA is used to generate a Token Encryption Key (TEK) that 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) **MYK-82 Chip Self-Test**: Performs hardware self test on the MYK-82.

    b) **RAM Test**: Performs a non-destructive self-test on the RAM memory to test the data-bus, address-bus and cell integrity.

    c) **DSA Test**: Performs DSA testing by generating a Public and Private Key pair, signing a random value and, then verifying the signature.

    d) **Firmware Test**: ROM and non-volatile on-chip and off-chip memory tests are performed using a FIPS approved authentication technique. Integrity of the MCU firmware and MYK-82 firmware are verified by computing the hash value of the firmware using SHA-1 and comparing that against the hash value stored in the flash.

    e) **Cryptographic Algorithm Test**: Known answer tests are performed, on all cryptographic algorithms implemented in the hardware including SKIPJACK encrypt and Secure Hash Algorithm.

    f) **Random Number Generator Test**: Functional testing of ring oscillators and Linear Feedback Shift Register (LFSR) is performed.

    g) **RTC Time Test**: Tests that the Real Time Clock has not been backdated by checking that the current time as reported by the Real Time Clock, is greater than the time last stored in the flash. Stored time in the flash is updated when this test is successfully completed. This test is only performed when the card is in “Secure Modem’ mode.

13. Conditional Tests.

    a) **Pairwise Consistency Tests**: Tests given X and Y for pairwise consistency.

    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 (regardless of the length of the random number needed).

14. The following initialization of the RASP Secure Modem must be accomplished by the SSO before the RASP Secure Modem will support User cryptographic services.

    a) Install the RASP Secure Modem’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 RASP Secure Modem can be used for cryptographic services, the User must successfully configure the modem to operate in a specific country, logon, and select a personality (certificate).

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

17. When RASP Secure Modem is in "FORTEZZA" mode, 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 RASP Secure Modem can be used to generate/store at least 10 wrapped TEKs or MEKs in registers. Keys are accessed using a key or register index of 0 to 9.

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

20. The wrapped Ks cannot be extracted from the RASP Secure Modem (that is, you cannot use WrapKey to extract Ks).

21. The modem can be used to store a maximum of 26 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 index 0.

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

25. The User cannot use Install x to restore a x to certificate index 0.

26. Only the SSO/User can update the RASP Secure Modem firmware, which is signed with DSA.

27. An SSO or a User can generate a Random Number. You do not have to logon; PIN access is not required.

28. Public components for key exchange are stored on the RASP Secure Modem.