Cryptek Common Security Module (CSM)
Cryptographic Module Security Policy

Version 1.6
Revision Date: June 23, 2005

Cryptek Inc.
1501 Moran Road
Sterling, VA. 20166-9309

Table of Contents

1 INTRODUCTION 3

1.1 PURPOSE 3
1.2 REFERENCES 3
1.3 PRODUCT LINE NAME CHANGE 3

2 SECURITY LEVEL 4

3 MODULE OVERVIEW 4

4 MODES OF OPERATION 5

4.1 FIPS APPROVED OPERATION 5
4.2 NON-FIPS APPROVED ALGORITHMS 6
4.3 SETTING FIPS MODE 6

5 PORTS AND INTERFACES 6

6 ROLES, SERVICES, AND AUTHENTICATION 7

6.1 ASSUMPTION OF ROLES 7
6.2 USER ROLE 7
6.3 CRYPTO-OFFICER ROLE 7
6.4 ADMINISTRATOR ROLE 7
6.5 SERVICES 8

7 DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS) 8

7.1 CSP/SRDI TO SERVICES RELATIONSHIP 9

8 SERVICE TO CSPS/SRDI ACCESS OPERATION RELATIONSHIP 11

9 OPERATIONAL ENVIRONMENT 11

10 SECURITY RULES 11

11 PHYSICAL SECURITY 13

12 MITIGATION OF OTHER ATTACKS POLICY 13

13 ACRONYM LIST 14

1 Introduction

1.1 *Purpose*

This is a non-proprietary cryptographic module security policy for the Cryptek Common Security Module (CSM) covering hardware revisions 5110N0017-1, 5110N0017-2, 5110N0017-3, 5110N0017-4, and firmware versions 2.1.9 and 2.4.0.3 The security policy describes how the CSM meets the security requirements of FIPS 140-2 level 1 and how to operate the module securely, in FIPS mode. The information contained in this document is provided to fulfill the Security Policy requirements of FIPS 140-2.

1.2 *References*

The following NIST Federal Information Processing Standards (FIPS) publications are referenced throughout this document.

- FIPS 140-2 Security Requirements for Cryptographic Modules
- FIPS 180-2 Secure Hash Standard
- FIPS 198 The Keyed-Hash Message Authentication Code (HMAC)
- FIPS 46-3 Data Encryption Standard (DES)
- FIPS 186-2 Digital Signature Standard (DSS)

For more information on Cryptek and the Cryptek product line visit the Cryptek website at http://www.cryptek.com. For information on validated Cryptek products visit the Common Criteria Evaluation and Validation Scheme (CCEVS) website at http://niap.nist.gov/cc-scheme/ValidatedProducts.html, and the NIST validated Modules List website at http://csrc.nist.gov/cryptval/140-1/140val-all.htm.

1.3 *Product Line Name Change*

The Cryptek network security product line has recently undergone a branding change that affects the product names. The new product names are not yet reflected in all documents. Please refer to Table 1-1 below to map the old nomenclature to the new nomenclature. Note: the Cryptek Secure Facsimile product line is not affected by this name change.

Table 1-1. Summary of Product Name Changes

Previous Nomenclature	New Nomenclature	Description
Diamond*Central*™, cCentral	CC200	Central manager for Cryptek network security products.
Diamond*PAK*™, PAK, cPAK	CP102, 104, 106	Hardware-based, rack-mounted, server-side security device that protects up to 6 network devices.
Diamond*Link*™, Link, cLink, cPoint	CL100, 150	Hardware-based, client-side security device that protects a single host.
Diamond*UTC*™, UTC, SUTC, cTerm	CT100	Sun Ray-based, ultra thin client integrated security solution.
Diamond*VPN*™, cVPN	CV100	Hardware-based, network edge or workgroup security device.
Diamond*SAT*™, cSAT	CS100, 101, 102	Hardware-based device for handling security and acceleration for long-haul networks.
Diamond*Agent*™, cAgent	CA100	Software-based, client-side security application.
cVDL	CVDL100	Database firewall network appliance that uses Virtual Data Labeling (VDL) technology.
Diamond*NIC*, NIC, cNIC, NSD-Prime	CN100	Hardware-based, client-side security device that protects a single host. PCI form factor (found only in the CC200)

2 Security Level

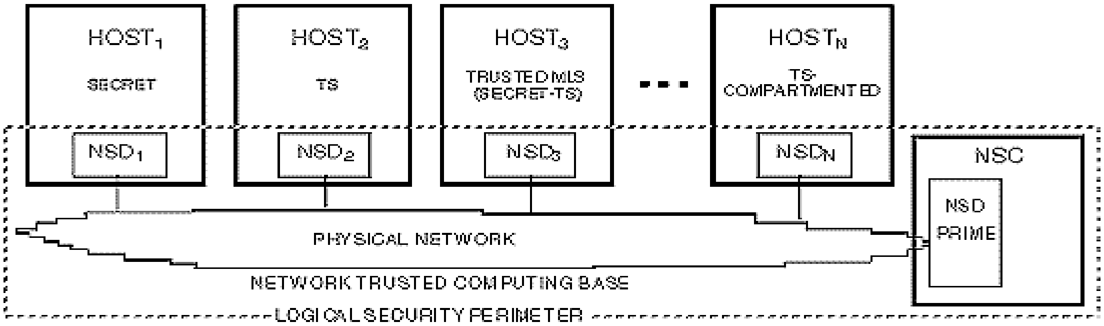
All hardware revisions of the CSM specified within this security policy are classified as a multi-chip embedded cryptographic module and meet the overall requirements applicable to FIPS 140-2 Level 1 security.

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	2
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 2 - Module Security Level Specification

3 Module Overview

The CSM is a centrally managed secure network product designed to control the flow of information to and from nodes and access to nodes on a network. Information flow is controlled on the basis of: security labels associated with network nodes and information packets on the network; explicit assignment of allowed information flow paths on the network; and, addresses, protocols, and services associated with network traffic.



The CSM is designed to operate at layer 3 of the protocol stack, using Internet Protocol Version 4 (IPv4) networking. The CSM hardware and firmware constitutes the core technologies used in all Cryptek Diamond*TEK* products.

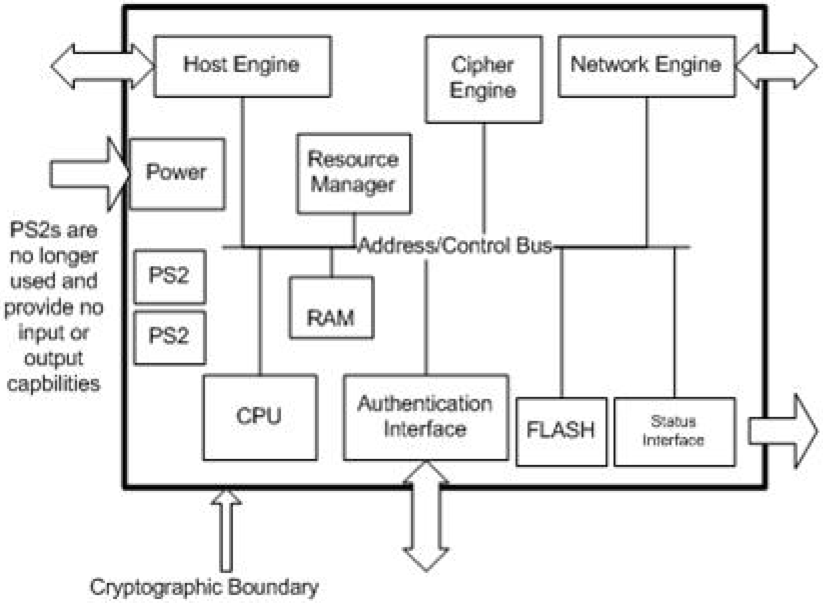


Diagram 1 – Diagram of the Cryptographic Module

4 Modes of Operation

The CSM supports the following three modes of operation, ONLINE, ONLINE-SECURE, and BYPASS. The modes supported by the CSM are determined by the Administrator during configuration setup and by the User, during authentication. The ONLINE mode signifies the CSM is configured to communicate with CSMs, Other IPSec (OIPs) nodes, or Clear Text Nodes (CTNs). CSMs will always talk encrypted to CSMs and OIPs nodes and enforce the information flow controls set by the Administrator. CSMs will talk to assigned CTNs in the clear (unencrypted) and enforce the information flow controls set by the Administrator. The ONLINE-SECURE mode signifies the CSM is configured to only communicate with other CSMs or OIPs nodes. All communication between these nodes will employ encryption and enforce the information flow controls set by the Administrator. The BYPASS mode signifies the CSM is configured to communicate with any CTN. While the CSM is in the BYPASS mode no encryption or information flow controls are supported. To configure a CSM to operate in the BYPASS mode requires two separate actions. The Administrator must configure the CSM to allow the bypass condition and the User must present bypass credentials to the CSM to activate the bypass mode.

4.1 FIPS Approved Operation

In FIPS mode, the CSM cryptographic module only supports FIPS Approved algorithms as follows:

- Triple-DES (three key) for encryption
- DES (one key) for encryption (for use with interfacing with legacy systems only)
- DES-MAC for firmware authentication
- SHA-1 for hashing and signature generation
- HMAC-SHA-1 for message authentication
- RSA PKCS#1 version 1.5 for digital signature
- ANSI x9.31 A.2.4 RNG

The CSM cryptographic module also provides the following cryptographic support in all modes of operation;

- The CSM cryptographic module supports the deterministic random number generator (DRNG), ANSI X9.31-1998. The DRNG is seeded by the Crypto Officer during the installation process.
- The CSM cryptographic module supports PKI using X.509 certificates wrapped in PKCS 7 format (1024 bits) for CSM to CSM authentication. **Note:** This is an option specified by the Administrator at the Diamond*Central* during configuration setup and installed by the Crypto Officer.

- Diffie-Hellman (DH) key exchange.

4.2 Non-FIPS Approved Algorithms

When not in FIPS mode the CSM supports the MD5, HMAC-MD5 algorithms for signature generation and hashing.

4.3 Setting FIPS Mode

The CSM can be configured to operate in FIPS mode during initial setup by the Administrator at the Diamond*Centra*[1]*l*. The Diamond*Central* is a centralized GUI security configuration and management workstation. Setup of the CSM is accomplished by traversing the various menu screens and entering the appropriate values. Initial setup instructions are provided below;

1. At the **Action Bar** select the "ADD NSD" icon.
2. Enter the ID number and name of the CSM. Click *Next>* to advance to the "Addressing" window.
3. Enter all the appropriate addressing information (e.g. Ethernet address, proxy Ethernet address, IP address, subnet mask, default router, CSM type). Click *Next>* to advance to the "key Type" window.
4. Within the "Key Type" window make the following selections;

• DES Key Length[2]	(Min = 168)	(Max = 168)
• Authentication Type	HMAC SHA-1	
• MODP Groups	1024	

5. Click *Next>* to advance to the "Audit Threshold" window. Default values will remain unchanged.
6. Click *Next>* to advance to the "Profiles" window. Select the appropriate communication policy for the CSM by scrolling through the "Security Profiles:" window.
7. Click the *Finish* button and the setting of the FIPS mode is complete for the CSM.

To view the FIPS settings of a CSM the Administrator must go to the Diamond*Central* and select the "View NSD" icon. This will allow the Administrator to confirm the security values set for the CSM without making any changes to it.

5 Ports and Interfaces

The CSM supports seven physical interfaces, Network port, Host port, Authentication Interface, Status Interface, PS/2 in port, PS/2 out port, and the Power port. The Network port and Host port for all hardware revision are 10/100 sensing Ethernet ports providing a RJ45 connection with the exception of revision 5110N0017-2, which supports 10/100 SC fiber optic interfaces. Status information is provided to the operator through a single LCD screen, multiple LEDs, audible signals or any of these in combination.

Physical ports	Logical Interface(s)
Network port	Data input, data output, status output, control input
Host port	Data input, data output, status output, control input
Authentication port	Data input, control input
Status port	Status output
PS/2 in port	Unused
PS/2 out port	Unused
Power port	Power interface

[1] *Note: The DiamondCentral is also known as the Network Security Center (NSC).*

[2] *Note: Setting the minimum and maximum key size to 168 disables single DES use with IPSec.*

6 Roles, Services, and Authentication

6.1 Assumption of Roles

All CSM revisions support three distinct operator roles (Administrator Role, Crypto Officer Role, and User Role) and provide Role Base authentication. The authentication mechanisms employed by all CSM revisions is determined by the Administrator during configuration setup and by the distinct operator role being assumed. The chart below maps the CSM revision to the authentication mechanism and authentication type, supported by firmware version 2.1.9.

Authentication Type	CSM Hardware Revision				Authentication Strength of Mechanism
	5110N0017-1	5110N0017-2	5110N0017-3	5110N0017- 4	
PIN	X	X			The probability that a random attempt will succeed or a false acceptance will occur is between 1/10^{7} and 1/10^{17} which is less than 1/1,000,000. **Note** to meet the FIPS requirement a PIN should be at least 7digits.
Shared Secret	X	X	X	X	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^{112} which is less than 1/1,000,000
PKI Certificate	X	X	X		The probability that a random attempt will succeed or a false acceptance will occur is 1/2^{80} which is less than 1/1,000,000

6.2 User Role

The CSM, regardless of hardware revision provides User role access through the authentication interface. The possession of the User authentication credentials provides access to the CSM (not necessarily to the network) for the User role. The User role is supported by two methods of authentication, a unique ID number (8 -32 bytes) with shared secret or a unique ID number (8 – 32 bytes) and PIN (to operate in FIPS mode, PIN must contain seven or more digits) combination with shared secret. The selection of which combination of authentication mechanisms are activated, is determined by the Administrator during configuration setup. The User presents the authentication credentials to the CSM for validation. Once the CSM has validated the authentication credential they are sent to the Diamond*Central* using a trusted channel for policy download. If the validation fails or the policy request is denied an error message will be displayed by the status output (LED or LCD). A successful validation and policy request will result in authorized services being provided to the User in accordance with the security policy download. Three consecutive failed authentication attempts will disable the CSM, and requires Administrator action.

6.3 Crypto-Officer Role

The CSM provides the Crypto Officer Role access through the authentication interface (Note: PKI certificates are loaded using the Host port) using the credentials provided by the Administrator. The credentials provided by the Administrator include all the configuration settings for the CSM, shared secret, and a checksum for integrity (Note: When the Administrator assigns the CSM to support PKI certificates for node to node authentication the Crypto officer is provided additional authentication credentials in the form of a X.509 certificate in a PKCS 7 format.). The Crypto Officer presents the credential to the CSM for validation. A failed validation results in a failed installation and an error message being displayed by the status output (LED or LCD). A successful validation results in authorized services being provided to the Crypto officer. If during the configuration setup the Administrator assigns the CSM to a *Static user* then the credentials will also contain the *Static users'* unique ID number (8 – 32 bytes) for authentication. The *Static user*s' unique ID number and shared secret are presented to the CSM for validation. Once the CSM has validated the authentication credentials for the *Static user* they are sent to the Diamond*Central* using a trusted channel for policy download. If the validation fails or the policy request is denied an error message will be displayed by the status output (LED or LCD). A successful validation will result in authorized services being provided to the *Static user*.

6.4 Administrator Role

The possession of the shared secret (Diamond*Central* 14 bytes) provides authentication for the Administrator role to the CSM. The Administrator presents the authentication credentials to the CSM using a trusted channel. A failed validation by the CSM will require the CSM be re-installed by the Crypto officer. A successful validation will allow the Administrator access to the CSM to provide authorized services.

6.5 Services

The following table provides information about the Services to Security functions and Roles availability to services within the CSM.

Services	Security Functions	User Role	Crypto-Officer Role	Administrator Role
Transmit Packets Process	DES, 3DES, SHA-1, HMAC-SHA-1	X		
Receive Packets Process	DES, 3DES, SHA-1 HMAC-SHA-1	X		
Initiate Bypass	N/A	X		
Initiate State change of CSM	DES, 3DES, SHA-1 HMAC-SHA-1[3]	X	X	X
Initiate Self-test of CSM	N/A	X	X	
Load Diamond*Central* shared secret	SHA-1		X	
Configure the CSM per predefined policy	DES, 3DES, SHA-1 HMAC-SHA-1			X
Zeroize CSM	DES, 3DES, SHA-1 HMAC-SHA-1			X
Update CSM Firmware	DES, 3DES, SHA-1 HMAC-SHA-1, DES-MAC			X

7 Definition of Critical Security Parameters (CSPs)

The following table contains the description of the Critical Security Parameters (CSP) in the CSM.

CSP	Description
Diamond*Central* shared secret (**DCSS**)	Used to provide encrypted communication between the CSM and the Diamond*Central* for the Administrator interface.
Traffic encryption keys (**TEK**s)	Used to encrypt the traffic between the CSM and another CSM or other IPSec device. These are generated as part of the IKE key generation process (3DES).
Traffic authentication keys (**TAK**s)	Used to authenticate traffic between the CSM and another CSM or other IPSec device. These are generated as part of the IKE key generation process.
Diffie-Hellman private keys (**DHPK**)	Generated by the CSM for each used level of classification and used as part of the IKE key generation process.
Firmware update key (**FWUK**)	Sent to the CSM by the Diamond*Central* as part of the firmware update sequence. The firmware is stored in RAM and a DES_MAC is calculated on the firmware using the update key. If the computed value is the same as the value sent from the Diamond*Central* then the firmware in the flash is replaced by the new firmware.
Node authentication values (**NAV)**	A shared secret or the PK certificate value is used as the authentication mechanism for the IKE key generation process.
Unique Identification number (**ID**)	A number between 8-32 bytes long used in authenticating the user to a network security device.
Personal Identification Number (**PIN**)	An optional number, between 1-17 bytes, long used in conjunction with the unique identification number to authenticate the user to the network security system.
Deterministic Random Number Generator (RNG)	A RNG is used to generate random numbers. The CSM supports a deterministic random number generator (DRNG), in accordance with ANSI X9.31.

[3] The Administrator can initiate a state change on a CSM at any time using the trusted channel. The User and Crypto officer can initiate a state change by cycling power or by removing and re-inserting their authentication credentials.

The following table contains a description of a Security Relevant Data Item (SRDI) not considered CSPs. The SRDI is protected within the cryptographic boundary against unauthorized modification and substitution.

SRDI	Description
Discretionary Access Control List (**DAT**)	The list of approved source and destination addresses (IP address, TCP/UDP port numbers, and protocols).
DH Public Key (**DHLK**)	Generated by the CSM for each used level of classification and used as part of the IKE key generation process.
Node authentication value (public key)	Used as part of the authentication mechanism for the IKE key generation process.

7.1 CSP/SRDI to Services Relationship

Transmit Packet Processing: The operation to transmit a packet shall first access the current state of the CSM. If the CSM is off-line, then the packet is not processed until the state changes to on-line. If the CSM is on-line, then the discretionary access control list (**DAT**) is checked to determine if communication is allowable. If the destination is not allowable (because of IP address, TCP/UDP port number, or protocol) then the packet is destroyed and an audit event is generated.

If the **DAT** signifies that the destination is allowable and is clear text (CTN), then the transmit security window (**TSW)** is accessed to determine if the CSM can transmit that particular label. If the label cannot be transmitted then the packet is destroyed and an audit event is generated. If the label is within the bounds of the transmit security window (**TSW)** of the CSM, then the **DAT** is checked to determine if the receiving address is allowed to receive the label associated with the address. If the packet label cannot be received by the destination address, then the packet is destroyed and an audit event is generated. If the label can be received by the destination address, then the packet is transmitted to the network.
If the **DAT** signifies that the destination is allowable and communication is to be encrypted (CSM or OIPs), then the keys associated with the destination (**TEK** and **TAK**) are accessed to determine if there is a key for the label associated with the packet.
If a key exists, then it is used to encrypt the packet and the key associated with the authentication mechanism (**TAK**) is used to perform the authentication of the packet. If the useful life of the key has been exhausted, then the keys (**TEK** and **TAK**) associated with the destination address are destroyed. After the encryption and authentication is complete, the packet is transmitted to the network.
If no key exists for the destination/label pair, then the CSM shall check the label of the packet against the transmit security window (**TSW)** of the CSM. If the label cannot be transmitted, then the packet is destroyed and an audit event is generated. If the packet is within the bounds of the transmit security window (**TSW)** and the destination address may not be a CSM, then the label of the packet is checked against the label defined for the destination address in the **DAT**. If the label of the packet is not a subset of the label of the destination address, then the packet is destroyed and an audit event is generated. If the destination address is a CSM or the label of the packet is a subset of the label associated with the destination address, then the packet is destroyed and an IKE process is instigated.
The IKE process will utilize the list of approved encryption algorithms (**ACAL**) and the list of approved authentication algorithms (**AAAL**) to negotiate an acceptable combination to secure the information between the new nodes. If the CSM does not have a Diffie-Hellman private value generated for the classification level, then a Diffie-Hellman public (**DHLK**) and private (**DHPK**) keys are generated. The Diffie-Hellman data, the shared secret or PKI certificate (**NAV**) associated with the destination address and random data generated as part of the IKE protocol are used to generate the keying material (**TEK** and **TAK**) to secure the communications between the CSM and the destination address.
Receive Packet Processing: The operation to receive a packet shall first access the current state of the CSM. If the CSM is not on-line and the packet is not from the Diamond*Central*, then the packet is thrown away and the network buffer is returned to the network coprocessor. If the CSM is on-line, then the discretionary access control list (**DAT**) is checked to determine if communication is allowable. If the source is not allowable (because of IP address and SPI number) then the packet is destroyed and an audit event is generated.

If the **DAT** signifies that the destination is allowable and is clear text (CTN), then the receive security window (**RSW)** is accessed to determine if the CSM can receive that particular label. If the label cannot be received then the packet is destroyed and an audit event is generated. If the label is within the bounds of the receive security window (**RSW)** of the CSM, then the **DAT** is checked to determine if the sending address is allowed to send the label associated with the address. If the packet label can not be sent by the source address, then the packet is destroyed and an audit event is generated. If the label can be sent by the source address, then the packet is passed to the host system.
If the **DAT** signifies that the source is allowable and communication is supposed to be encrypted (CSM or OIPs), then the keys associated with the destination (**TEK** and **TAK**) are accessed to determine if there is a key for the label associated with the packet.
If a key exists, then it is used to decrypt the packet and the key associated with the authentication mechanism (**TAK**) is used to perform the authentication of the packet. After the decryption and the authentication are complete, the packet is checked for allowable protocols and TCP/UDP port numbers. If the **DAT** signifies that the protocol and TCP/UDP port number is acceptable, then the packet is given to the host system.

If no key exists for the source/label pair, then the CSM shall check the label of the packet against the receive security window (**RSW)** of the CSM. If the label can not be received, then the packet is destroyed and an audit event is generated. If the packet is within the bounds of the receive security window (**RSW)** and the source address may not be a CSM, then the label of the packet is checked against the label defined for the source address in the **DAT**. If the label of the packet is not a subset of the label of the source address, then the packet is destroyed and an audit event is generated. If the source address is a CSM or the label of the packet is a subset of the label associated with the source address, then the packet is destroyed and an IKE process is instigated.
The IKE process will utilize the list of approved encryption algorithms (**ACAL**) and the list of approved authentication algorithms (**AAAL**) to negotiate an acceptable combination to secure the information between the new nodes. If the CSM does not have a Diffie-Hellman private value generated for the classification level, then a Diffie-Hellman public (**DHLK**) and private (**DHPK**) key is generated. The Diffie-Hellman data, the shared secret or PKI certificate (**NAV**) associated with the source address and random data generated as part of the IKE protocol are used to generate the keying material (**TEK** and **TAK**) to secure the communications between the CSM and the source address. If key material exists for the communications channel, then the old keying material (**TEK** and **TAK**) are zeroized and replaced with the new values.
Load Diamond*Central* shared secret: The load Diamond*Central* shared secret function requires the use of the Crypto officer authentication credentials. The credentials identify its user as a Crypto officer and contain the shared secret used by the CSM for communication with the Diamond*Central*. The CSM will copy the information from the credentials and store it in its on-board FLASH memory (**DCSS**).

Configure the CSM per a predefined policy: The Administrator (via the Diamond*Central*) shall download (under protection of the encrypted communication between the CSM and the Diamond*Central* using the **DCSS**) the defined discretionary access control list (**DAT**), the transmit security window (**TSW**), the receive security window (**RSW**) and node authentication values (**NAV**) each time a user successfully logs into the CSM. The change could be an addition or a removal of the ability to send/receive packets to other host systems. In the case of a removal, any traffic encryption keys (**TEK**) or traffic authentication keys (**TAK**) used for communication between the node and the removed destination node are zeroized.

Zeroize CSM: The Administrator can zeroize the all the CSPs (DCSS, TEKs, TAKs, DHPK, FWUK, NAV, RNG) and SRDIs stored and in use by the CSM. The command is sent via the encrypted communication channel setup by the **DCSS**. The command will zeroize the **DCSS**, traffic keys (**TEK** and **TAK**), the Diffie-Hellman keys (**DHPK** and **DHLK**), the discretionary access control list (**DAT**), the security window (**DSW**), the node authentication values (**NAV**), approved crypto algorithm list (**ACAL**) and the approved authentication algorithm list (**AAAL**).

Update CSM firmware: The Administrator (via the Diamond*Central*) can send a new version of the firmware of the CSM via the encrypted channel setup by the **DCSS**. The Diamond*Central* will first send an authentication key (**FWUK**) and the firmware. The CSM shall verify the signature of the firmware and only update the firmware if the signature is verified. Once the firmware is updated, the CSM will zeroize the **FWUK** and reset its self.

Initiate Bypass: To configure a CSM to operate in the BYPASS mode requires two separate actions. The Administrator must configure the CSM to allow the bypass condition and the User must present bypass credentials to the CSM to activate the bypass mode. The BYPASS mode signifies the CSM is configured to communicate with any CTN. While the CSM is in the BYPASS mode no encryption or information flow controls are supported.

Initiate State change of CSM: The Administrator (Diamond*Central*) can initiate a state change (e.g. suspend, shutdown, and online) using the encrypted channel setup by the **DCSS**. The User and Crypto officer can initiate a state change by cycling the power of the CSM or by removing and re-inserting their authentication credentials. **Note:** Upon User/Crypto officer initiated state changes, authentication credentials must be submitted. There are two supported methods of authentication, a unique **ID** number (8 -32 bytes) with shared secret or a unique **ID** number (8 – 32 bytes) and **PIN** (to operate in FIPS mode, **PIN** must contain seven or more digits) combination with shared secret. Further information can be found in Section 6.2.

Initiate Self-test of CSM: The User and Crypto officer can initiate the CSM to perform self-tests by cycling the power or by removing and re-inserting their authentication credentials.

8 Service to CSPs/SRDI Access Operation Relationship

The table on this page has been devised to show the Services vs. CSPs/SRDI and Role access.

Services vs. CSPs/SRDI	DCSS	TEK	TAK	DHPK	FWUK	DAT	NAV	RNG	ID	PIN	U	C	A
Transmit Packet Processing		WAZ	WAZ	WA		AZ	AZ	AZ			X		
Receive Packet Processing		WAZ	WAZ	WA		AZ	AZ	AZ			X		
Initiate Bypass											X		
Initiate Self-test of CSM											X	X	
Initiate State change of CSM[4]	A	WAZ	WAZ	WA		AZ	AZ	AZ	AZ	WAZ	X	X	X
Load Diamond*Central* shared secret	W							W				X	
Configure the CSM per a predefined policy	A	Z	Z			W	W						X
Zeroize CSM	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z			X
Update CSM Firmware					WAZ								X

In the above table, access to the CSPs/SRDI via the service utilizes the following abbreviations:

A = Access (note that the actual value is never seen outside the security perimeter so it is not technically a read)
W = Write
Z = Zeroize

In the table above, access to services by individuals is shown by placing an X in the appropriate column at the right of the table. The following abbreviations apply:

U = User
C = Crypto officer
A = Administrator.

9 Operational Environment

The FIPS 140-2 Operational Environment requirements are not applicable because all CSM revisions do not contain a modifiable operational environment.

10 Security Rules

This section documents the security rules enforced by the CSM to implement the security requirements of this FIPS 140-2 Level 1 module[5].

1. The CSM shall provide three distinct operator roles. These are the User role, the Crypto Officer role, and the Administrator role.
2. The CSM shall provide Role-Based authentication.
    - Possession of the User authentication credentials provides access to the CSM (not necessarily the network) for the User role. Possession of the Crypto officer credentials provides authentication for the Crypto officer. Possession of the shared secret provides authentication for the Administrator role.
3. When the CSM has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. The cryptographic module shall encrypt message traffic using the TDES algorithm.
5. The cryptographic module shall perform the following tests:

    A. Power up Self-Tests:

    1. Cryptographic algorithm tests:

        a. TDES Known Answer Test

[4] The User and Crypto officer can initiate a state change by cycling power or by removing and re-inserting their authentication credentials then submitting. Note: The Administrator (Diamond*Central*) can initiate a state change (e.g. suspend, shutdown, and online) using the encrypted channel. Additionally, only the User is able to write to the PIN.

[5] Security rules are contained in the numbered paragraphs. Additional information is provided for background purpose only.

b. DES Known Answer Test

c. DES_MAC Known Answer Test

d. SHA-1 Known Answer Test

e. HMAC-SHA-1 Known Answer Test

f. MD-5 Known Answer Test

g. HMAC-MD-5 Known Answer Test

h. DRNG Know Answer Test

i. RSA Known Answer Test

2. Software Integrity Test (CRC32)

3. Critical Functions Tests

a. RAM Walking Ones Test

B. Conditional Self-Tests:

1. Continuous Random Number Generator (RNG) test – performed on DRNG

2. RSA pair-wise consistency test. This is performed when the CSM is configured to support PKI.

3. Policy Integrity Test (Bypass test)

4. Firmware load Test (DES-MAC)

5. Exclusive Bypass Test

6. At any time the CSM is in an idle state, the operator shall be capable of commanding the module to perform the power-up self-test.
7. Prior to each use, the internal DRNG shall be tested. Testing is accomplished using the continuous Random number generator test.
8. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
9. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. The CSM shall not support concurrent operators.
11. The User shall be capable of commanding the module to perform the power-up self-tests by removing and re-inserting the authentication credentials, pressing the **Reboot** button or cycling the power.
12. The CSM shall not communicate with the Diamond*Central* (Administrator role) to allow a User to login to the device until after it has been initialized by the Crypto officer credentials and User authentication credentials haves been presented. After reading the configuration information from the Crypto officer credentials and updating the Diamond*Central* shared secret and communication data, the CSM will transition to the offline state and await the insertion of User credentials. CSMs configured to use a *Static user* assignment await the pressing of the **Reboot** button or power cycle to transition to the online state.
13. The User is disallowed after one invalid attempt to initialize with the Diamond*Central* (Administrator role).
14. The CSM shall generate audits for all attempted Mandatory and Discretionary Access Control (MAC and DAC) violations.
15. The CSM shall generate audits for all received encrypted packets that do not pass the message authentication code test.
16. The User shall not have access to any cryptographic services unless the CSM has been commanded to transition to the ONLINE state by the Diamond*Central* (Administrator role).
17. The CSM shall recognize a Users credentials and attempt to initialize with the Diamond*Central* (Administrator role) using data on the Diamond*Central* shared secret, User credentials and the profile selected by the User.
18. The CSM shall have a bypass mode that is enable by requiring two separate actions. The Administrator must configure the CSM to allow the bypass condition and the User must present bypass credentials too the CSM to activate the bypass mode. While the CSM is in the bypass mode no encryption or information flow controls are supported.
19. The Diamond*Central* (Administrator role) shall download a non-security auditing policy to include statistical, broadcast and TCP Open/Close events. These audit events shall be sent to the Diamond*Central* (Administrator role) for logging.
20. The CSM and the Diamond*Central* (Administrator role) shall use ISAKMP to negotiate keys during each initialization.
21. The CSM shall determine the encryption and authentication algorithms and keys based on the shared secret or PKI method of the IKE standard.
22. The CSM shall support a different key for each host/ label of data combination.
23. The CSM shall accept a firmware update from the Diamond*Central* (Administrator role) if the update passes a DES Message Authentication Code (DES-MAC) check using the firmware update key sent to the CSM from the Diamond*Central* (Administrator role) via the trusted channel.
24. The CSM shall accept state control commands (suspend, online, and shutdown) commands from the Diamond*Central* (Administrator role) via the trusted channel.

25. The Diamond*Central* shall be capable of zeroizing the Diamond*Central* (Administrator role) shared secret stored in the CSM.
26. If the User credentials are removed from the CSM or in the case of a *Static user* when the reboot button is pressed or power cycled, the CSM shall notify the Diamond*Central* (Administrator role) and change its state to offline via the trusted channel.
27. The data communication keys (TEK and TAK) shall be zeroized when the User credentials are removed or in the case of a *Static user* when the reboot button is pressed or the CSM power is cycled.
28. The Administrator shall verify the authentication type reads SHA-1, when operating in FIPS mode.
29. The Diamond*Central* (Administrator role) shall, before allowing the CSM to transition to the online state, download a transmit and receive mandatory access control policy to the CSM. This policy shall include a maximum and minimum transmit window as well as an allowable and mandatory transmit and receive category set.
    - All outgoing packets shall have a security level between the maximum and minimum transmit level and a category set that is a superset of the mandatory and a subset of the allowable category values.
    - All incoming packets shall have a security level between the maximum and minimum transmit classification level and a category set that is a superset of the mandatory and a subset of the allowable category values.
30. The CSM shall only support or accept SHA-1 based signatures for the PKI node authentication value.
31. The CSM shall send all auditable events to the Diamond*Central* for logging.
32. The Diamond*Central* (Administrator role) shall download communication rules (DAC policy) to the CSM. The policy shall be re-configurable by the Diamond*Central* (Administrator role) at any time. These rules define the communication paths as follows:
    - Valid destination addresses for packets sent from the attached host to the network.
    - Valid source addresses for packets being sent to the attached host from the network.
    - Allowable/prohibited TCP and UDP port values for transmission and reception by the host.
    - Allowable/prohibited protocols for transmission and reception by the host.
    - The encryption algorithm used to secure the IPSec packet (DES or 3DES).
    - The authentication mechanism used to secure the IPSec packet (MD5 or SHA-1).

11 Physical Security

The CSM is classified as a Multi-chip Embedded module designed to be placed into a commercial grade enclosure for operations. The CSM consists of a single integrated circuit board module of commercial grade components. The zeroization of critical security parameters (CSPs) is accomplished by the Administrator role at the Diamond*Central*. The CSM(s) FCC validation was performed using Diamond*TEK* products.

12 Mitigation of Other Attacks Policy

The CSM cryptographic module makes no additional claims to mitigating other attacks.

13 Acronym List

AAAL	Approved Authentication Algorithms
ACAL	Approved Encryption Algorithms
CCEVS	Common Criteria Evaluation and Validation Scheme
CSM	Common Security Module
CSP	Critical Security Parameters
CTN	Clear Text Node
DAC	Discretionary Access Control
DAT	Discretionary Access Control List
DCSS	Diamond*Central* Shared Secret
DES	Data Encryption Standard
DES-MAC	Date Encryption Standard – Message Authentication Code
DHLK	Diffie-Hellman Public Key
DHPK	Diffie-Hellman Private Key
DRNG	Deterministic Random Number Generator
DSS	Digital Signature Standard
FIPS	Federal Information Processing Standards
FWUK	Firmware Update Key
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MAC	Mandatory Access Control
MD5	Message Digest v.5
MODP	Modular Exponential
NAV	Node Authentication Value
NSC	Network Security Center
NSD	Network Security Device
OIPS	Other IPSec
PIN	Personal Identification Number
PKCS#7	Public Key Cryptographic Standard #7 (Cryptographic Message Syntax Standard)
PKI	Public Key Infrastructure
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman
RSW	Receive Security Window
SC	Secure Channel
TAK	Traffic Authentication Key
TCP	Transmission Control Protocol
TEK	Traffic Encryption Key
TSW	Transmit Security Window
UDP	User Datagram Protocol
X.509	Authentication Framework for Directory Services