Diamond*Pak* and CP106
Security Policy

Version 1.1
Revision Date: January 6, 2006

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

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary cryptographic device security policy for the Cryptek Diamond*Pak* (H/W Ver. 5010D27630 Rev. C) and CP106[1] (H/W Ver. 5010D27630 Rev. D) with firmware version 2.1.9 or 2.4.0.3. The security policy describes how the Diamond*Pak* and CP106 meet the security requirements of FIPS 140-2 level 2 and how to operate the devices 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, CP104, CP106	Hardware-based, rack-mounted, server-side security device that protects up to 6 network devices.
Diamond*Link*™, Link, cLink, cPoint	CL100, CL150, CL100F	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, CS101, CS102	Hardware-based device for handling security and acceleration for long-haul networks.

[1] Cryptek has recently undergone a branding change that affects the entire product line. The Diamond*Pak* is also being sold under the product name CP106. Only the Diamond*Pak* (DP-600) or CP106 with 6 CSMs has been FIPS 140-2 validated. The DiamondPak/CP106 both use CSM hardware version 5110N0017-3. This security policy only covers the Diamond*Pak* (DP600) and CP106 with 6 CSMs. Cryptek also makes a CP102 and CP104 with 2 and 4 CSMs encased in rack-mounted commercial grade metal cases.

Previous Nomenclature	New Nomenclature	Description
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

The Diamond*Pak*/CP106[2] specified within this security policy is classified as a standalone cryptographic device with six CSMs encased in a rack-mount commercial grade metal case. Each CSM, or "channel", within the Diamond*Pak* acts as its own cryptographic device. All revisions within this security policy, where the device is sealed with tamper-evident stickers, meet the overall requirements applicable to FIPS 140-2 Level 2 security.

Security Requirements Section	FIPS 140-2 Level
Cryptographic Module	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 2 - Diamond*Pak* Security Level Specification with the tamper-evident seals.

3 Diamond*Pak*/CP106 Overview

Diamond*Pak*/CP106 is a rack-mounted network appliance designed for protecting multiple network based servers. With six channels, each having Diamond*TEK*'s self-protecting computer with a single security profile, Diamond*Pak* can protect multiple servers or split-band lines within a single server. With advanced access control for protecting critical back-end systems, Diamond*Pak* provides the same security protection that is used for our government's sensitive information. The design provides individual host and network interfaces for each channel, an authentication interface, status output interfaces, and a power switch. The authentication interface consists of a single card reader; a channel selector button to assign control of a CSM; and a reboot button. Status output is provided for each channel through a series of LEDs and audible signals.

Diamond*TEK* is the family name of a group of products designed and developed by Cryptek to provide the highest level of protection for information assets inside your enterprise network. Flexible in design, Diamond*TEK*: Will not impact application or user performance; Is complementary to other security components and non-intrusive to your business process; Integrated with other IPSec products and provides a mechanism for including them in a secure managed network; Features an operating system and platform-independent design that is: Unaffected by security leaks or flaws in the operating system or applications; Compatible with your legacy systems and applications; Adaptable to virtually any network configuration; Easily upgradeable and extremely flexible.

[2] This security policy only covers the Diamond*Pak* (DP600) and CP106 with 6 CSMs.

Photograph of a Diamond*Pak-6*

Photograph of a CP106

4 Modes of Operation

The Diamond*Pak*/CP106 supports the following three modes of operation, ONLINE, ONLINE-SECURE, and BYPASS. The modes supported by the Diamond*Pak* are determined by the Administrator during configuration. Each channel within the Diamond*Pak* maintains its own mode of operation.

The ONLINE mode signifies the active channel in the Diamond*Pak* is configured to communicate with other Diamond*TEK* secure nodes and/or Other IPSec (OIPs) nodes, and Clear Text Nodes (CTNs). The Diamond*Pak* will always talk encrypted to other Diamond*TEK* secure nodes and OIPs nodes and enforce the information flow controls set by the Administrator. The Diamond*Pak* will talk to assigned[3] CTNs in the clear (unencrypted) and enforce the information flow controls set by the Administrator. The ONLINE-SECURE mode signifies the active channel in the Diamond*Pak* is configured to only communicate with other Diamond*TEK* secure nodes and/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 active channel in the Diamond*Pak* is configured to communicate with any CTN. While the active channel in the Diamond*Pak* is in the Bypass mode, no encryption or information flow controls are supported. To configure a channel in a Diamond*Pak* to operate in the Bypass mode requires two separate actions. The Administrator must configure the CSM in the Diamond*Pak* to allow the bypass condition. The Crypto officer must present bypass credentials, in the form of a bypass card, to the active channel in Diamond*Pak* and press the reboot button.

[3] The devices ability to communicate with CTNs is established by the Administrator through the "Configure the Diamond*Pak* per predefined policy" service.

4.1 FIPS Approved Operation

In FIPS mode, the Diamond*Pak*/CP106 cryptographic device only supports FIPS Approved algorithms as follows:

- Triple-DES (three key) for encryption
- DES (one key) for encryption (Transitional phase only – valid until May 19, 2007)[4]
- DES-MAC for firmware authentication (Transitional phase only – valid until May 19, 2007)
- 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 Diamond*Pak*/CP106 cryptographic device also provides the following cryptographic support in all modes of operation;

- The Diamond*Pak* supports a deterministic random number generator (DRNG), ANSI X9.31-1998. The DRNG is seeded by the Crypto Officer during the installation process.
- The Diamond*Pak* supports PKI using X.509 certificates wrapped in PKCS 7 format (1024 bits) for Diamond*TEK* secure node to Diamond*TEK* secure node authentication. **Note:** This is an option specified by the Administrator at the Diamond*Central* during configuration setup and installed by the Crypto Officer for each channel.
- Diffie-Hellman (DH) key exchange (Key establishment methodology provides 80 bits of strength).

4.2 Non-FIPS Approved Algorithms

When not in FIPS mode the Diamond*Pak*/CP106 supports the MD5, HMAC-MD5 algorithms for signature generation and hashing.

4.3 Setting FIPS Mode

The Diamond*Pak*/CP106 can be configured to operate in FIPS mode during initial setup by the Administrator at the Diamond*Central*. The Diamond*Central* is a centralized GUI security configuration and management workstation. Setup of the Diamond*Pak* is accomplished by traversing the various menu screens and entering the appropriate values for each channel supported. 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 Diamond*Pak*. 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, link type). Click *Next*> to advance to the "Key Types" window.
4. Within the "Key Type" window make the following selections;

➤ DES Key Length	(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.

[4] DES is for use with interfacing with legacy systems only.

6. Click *Next>* to advance to the “Profiles” window. Select the appropriate communication policy for the Diamond*Pak* by scrolling through the “Security Profiles:” window.
7. Click the *Finish* button and the setting of the FIPS mode is complete for the Diamond*Pak*.

To view the FIPS settings of the Diamond*Pak* channel 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 Diamond*Pak* without making any changes to it. This step would be repeated for each channel supported by the Diamond*Pak*.

5 Ports and Interfaces

The Diamond*Pak*/CP106 supports the following physical interfaces, Network ports, Host ports, an Authentication Interface, Status Interfaces and the Power port. The Network port and Host port for the Diamond*Pak* are 10/100 sensing Ethernet ports providing a RJ45 connection. Status information is provided to the operator through a series of LEDs, audible signals or a combination of the two. For the Diamond*Pak* (DP600) there are six of the following[5], network ports, host ports and status interfaces; one for each channel. There is only one authentication interface which includes a card reader, a channel selector button, and a reboot button. The power port is controlled through a switch.

Physical ports	Logical Interface(s)
Network port (6)	Data input, data output, status output, control input
Host port (6)	Data input, data output, status output, control input
Authentication port (1)	Data input, control input
Status port (6)	Status output
Power port (1)	Power interface
Reboot Button	Power interface

6 Roles, Services, and Authentication

6.1 Assumption of Roles

The Diamond*Pak*/CP106 supports three distinct operator roles (Administrator Role, Crypto Officer Role and User Role) and provides Role Base authentication. The chart below maps the Diamond*Pak* to the authentication mechanism and authentication type, supported by firmware version 2.1.9 and 2.4.0.3.

Authentication Type	Authentication Strength of Mechanism
Shared Secret	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	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
ID	The ID is 8 – 32 bytes long. The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{64}$.

[5] The number of network ports, host ports, and status interfaces supported by the Diamond*Pak* is determined by the number of CSMs installed.

6.2 User Role

The Diamond*Pak*/CP106 can only be assigned to a *Static user (No Authentication Card Required)*. Because the Diamond*Pak* can only be assigned to a *Static user*, the Install card[6] will contain the *Static user's* unique ID number (8 – 32 bytes) for authentication, configuration settings, shared secret, and a checksum for integrity. In order to present the *Static user*'s unique ID number and shared secret to the Diamond*Pak* for validation, the Crypto-officer must select the correct channel on the Diamond*Pak*, insert the Install card and press the Reboot button. Once the Diamond*Pak* has validated the authentication credentials for the *Static user*, the Crypto-officer must remove the Install card and press the Reboot button. The credentials are sent to the Diamond*Central* using a trusted channel for policy download. If the validation fails or the policy request is denied, the error LED will be illuminated. A successful validation will result in authorized services being provided to the *Static user*.

6.3 Crypto Officer Role

The Diamond*Pak*/CP106 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. For the Diamond*Pak*, the authentication interface includes a card reader, a channel select button and a reboot button. When presenting the credentials, the Crypto Officer must use the Select button to activate the correct channel on the Diamond*Pak*. When the Administrator assigns the Diamond*Pak* 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.). A failed installation will result in an error LED being illuminated. A successful installation will result in authorized services being provided to the Crypto officer.

6.4 Administrator Role

The possession of the shared secret (14 bytes) provides authentication for the Diamond*Central* (Administrator role) to the Diamond*Pak*/CP106. The Administrator presents the authentication credentials to the Diamond*Pak* using a trusted channel. A failed validation by the Diamond*Pak* will require the Diamond*Pak* be re-installed by the Crypto officer. A successful validation will allow the Administrator access to the Diamond*Pak* 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 Diamond*Pak*.

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 Diamond*Pak*[7]	DES, 3DES, SHA-1 HMAC-SHA-1	X	X	X
Initiate Self-test of Diamond*Pak*	N/A	X	X	
Load Diamond*Central* shared secret	SHA-1		X	

[6] The installation of the Static user role is accomplished by the Crypto officer.

[7] The Administrator can initiate a state change on a Diamond*Pak* at any time using the trusted channel. The Static User and Crypto officer can initiate a state change by cycling power or pressing the Reboot button.

Services	Security Functions	User Role	Crypto-Officer Role	Administrator Role
Configure the Diamond*Pak* per predefined policy	DES, 3DES, SHA-1 HMAC-SHA-1			X
Zeroize Diamond*Pak*	DES, 3DES, SHA-1 HMAC-SHA-1			X
Update Diamond*Pak* 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 Diamond*Pak*.

CSP	Description
Diamond*Central* shared secret (**DCSS**)	Used to provide encrypted communication between the Diamond*Pak* and the Diamond*Central* for the Administrator interface (used as an IKE pre-shared secret)
Traffic encryption keys (**TEK**s)	Used to encrypt the traffic between the Diamond*Pak* and another Diamond*TEK* secure device 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 Diamond*Pak* and another Diamond*TEK* secure node or other IPSec device. These are generated as part of the IKE key generation process.
Diffie-Hellman private keys (**DHPK**)	Generated by the Diamond*Pak* for each used level of classification and used as part of the IKE key generation process.
Firmware update key (**FWUK**)	Sent to the Diamond*Pak* 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 PKI certificate value is used as the authentication mechanism for the IKE key generation process.
Deterministic Random Number Generator (RNG)	A RNG is used to generate random numbers. The Diamond*Pak* supports a deterministic random number generator (DRNG), in accordance with ANSI X9.31.
Unique Identification Number (**ID**)	A number between 8-32 bytes long used in authenticating the use to a network security device.

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 Diamond*Pak* 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

Note: For the following discussion, "Diamond*Pak*" references a single CSM in the Diamond*Pak*/CP106.

Transmit Packet Processing: The operation to transmit a packet shall first assess the current state of the Diamond*Pak*. If the Diamond*Pak* is off-line, then the packet is not processed until the state changes to on-line. If the Diamond*Pak* 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 Diamond*Pak* 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 Diamond*Pak*, 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 (Diamond*TEK* secure node 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 Diamond*Pak* shall check the label of the packet against the transmit security window (**TSW)** of the Diamond*Pak*. 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 Diamond*Pak*, 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 Diamond*TEK* secure node 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 Diamond*Pak* 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 Diamond*Pak* and the destination address.

Receive Packet Processing: The operation to receive a packet shall first access the current state of the Diamond*Pak*. If the Diamond*Pak* 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 Diamond*Pak* 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 Diamond*Pak* 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 Diamond*Pak*, 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 (Diamond*TEK* secure node 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 Diamond*Pak* shall check the label of the packet against the receive security window (**RSW)** of the Diamond*Pak*. If the label cannot 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 Diamond*Pak*, 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 Diamond*Pak* 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 Diamond*Pak* 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 Diamond*Pak* 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 Diamond*Pak* for communication with the Diamond*Central*. The Diamond*Pak* will copy the information from the credentials and store it in its on-board FLASH memory (**DCSS**).

Configure the Diamond*Pak* per a predefined policy: The Administrator (via the Diamond*Central*) shall download (under protection of the encrypted communication between the Diamond*Pak* 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 the Diamond*Pak* is initiated (either by a reboot or power cycle). 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 Diamond*Pak*: The Administrator can zeroize the all the CSPs (DCSS, TEKs, TAKs, DHPK, FWUK, NAV, RNG) and SRDIs stored and in use by the Diamond*Pak*. 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 Diamond*Pak* firmware: The Administrator (via the Diamond*Central*) can send a new version of the firmware of the Diamond*Pak* via the encrypted channel setup by the **DCSS**. The Diamond*Central* will first send an authentication key (**FWUK**) and the firmware. The Diamond*Pak* shall verify the signature of the firmware and only update the firmware if the signature is verified. Once the firmware is updated, the Diamond*Pak* will zeroize the **FWUK** and reset its self.

Initiate Bypass: To configure a Diamond*Pak* to operate in the Bypass mode requires two separate actions. The Administrator must configure the Diamond*Pak* to allow the bypass condition and the Crypto officer on the behalf of the Static user must present bypass credentials to the Diamond*Pak*. The Bypass mode signifies the Diamond*Pak* is configured to communicate with any CTN. While the Diamond*Pak* is in the Bypass mode, no encryption or information flow controls are supported.

Initiate State change of Diamond*Pak*: The Administrator (Diamond*Central*) can initiate a state change (e.g. suspend, shutdown, and online) using the encrypted channel setup by the **DCSS**. The Crypto officer on the behalf of the Static user can initiate a state change by cycling the power of the Diamond*Pak* or selecting the appropriate channel on the Diamond*Pak* and pressing the Reboot button. Note: Upon Static User/Crypto officer initiated state changes, authentication credentials must be submitted. Authentication credentials consist of a unique **ID** number (8-32 bytes) with shared secret.

Initiate Self-test of Diamond*Pak*: The Crypto officer can initiate the Diamond*Pak* to perform self-tests by cycling the power or selecting the appropriate channel on the Diamond*Pak* and pressing the Reboot button.

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	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										X	X	
Initiate State change[8]	A	WAZ	WAZ	WA		AZ	AZ	AZ	AZ	X	X	X
Load Diamond*Central* shared secret	W							W			X	
Configure the Diamond*Pak*/ a predefined policy	A	Z	Z			W	W					X
Zeroize Diamond*Pak*	Z	Z	Z	Z	Z	Z	Z	Z	Z			X
Update Diamond*Pak* 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 the Diamond*Pak* does not contain a modifiable operational environment.

[8] The Static User and Crypto officer can initiate a state change by cycling power or by pressing the Reboot button. Note: The Administrator (Diamond*Central*) can initiate a state change (e.g. suspend, shutdown, and online) using the encrypted channel.

10 Security Rules

Note: For the following discussion, "Diamond*Pak*" references a single CSM in the Diamond*Pak*.

This section documents the security rules enforced by the Diamond*Pak* to implement the security requirements of this FIPS 140-2 Level 2 device.

1. The Diamond*Pak* shall provide three distinct operator roles. These are the User, Crypto Officer, and the Administrator roles.

2. The Diamond*Pak* shall provide Role-Based authentication.
   - 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 Diamond*Pak* has not been placed in a valid role, the operator shall not have access to any cryptographic services.

4. The cryptographic device shall encrypt message traffic using the TDES algorithm.

5. The cryptographic device shall perform the following tests:
   A. Power up Self-Tests:

      1. Cryptographic algorithm tests:

         a. TDES Known Answer Test

         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 Diamond*Pak* is configured to support PKI.

      3. Policy Integrity Test (Alternating Bypass test)

      4. Firmware load Test (DES-MAC)

      5. Exclusive Bypass Test

6. When the Diamond*Pak* is in the bypass state (BYPASS) the BYPASS LED will illuminate Amber. When the Diamond*Pak* is in the alternating bypass (ONLINE) state the ONLINE & BYPASS LEDs will illuminate Green and Amber. The illumination of the single green ONLINE LED signifies the Diamond*Pak* does not support the bypass state (ONLINE-SECURE).

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 on a per CSM/channel basis.

9. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the device.

10. The Diamond*Pak* shall not support concurrent operators.

11. The Crypto officer shall be capable of commanding the device to perform the power-up self-tests by cycling the power or selecting the appropriate channel on the Diamond*Pak* and pressing the Reboot button..

12. The Diamond*Pak* shall not communicate with the Diamond*Central* (Administrator role) to login to the device until after it has been initialized by the Crypto officer's credentials.

13. The User is disallowed after one invalid attempt to initialize with the Diamond*Central* (Administrator role).

14. The Diamond*Pak* shall generate audits for all attempted Mandatory and Discretionary Access Control (MAC and DAC) violations.

15. The Diamond*Pak* 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 Diamond*Pak* has been commanded to transition to the Online state by the Diamond*Central* (Administrator role).

17. The Diamond*Pak* shall recognize the Crypto officer's credentials and attempt to initialize with the Diamond*Central* (Administrator role) using data on the Diamond*Central* shared secret.

18. The Diamond*Pak* shall have a bypass mode that is only enabled by requiring two separate actions. The Administrator must configure the Diamond*Pak* to allow the bypass condition and the Crypto officer must present bypass credentials too the Diamond*Pak* to activate the bypass mode. While the Diamond*Pak* is in the bypass mode no encryption or information flow controls are supported. The status LED will illuminate the BYPASS LED (Amber). The alternating bypass mode is enabled by configuring the Diamond*Pak* to communicate with Diamond*TEK* nodes, and/or OIPS nodes, and Clear Text Nodes (CTNs) on the Diamond*Central* (Administrator role).

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 Diamond*Pak* and the Diamond*Central* (Administrator role) shall use ISAKMP to negotiate keys during each initialization.

21. The Diamond*Pak* shall determine the encryption and authentication algorithms and keys based on the shared secret or PKI method of the IKE standard.

22. The Diamond*Pak* shall support a different key for each host/ label of data combination.

23. The Diamond*Pak* 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 Diamond*Pak* from the Diamond*Central* (Administrator role) via the trusted channel.

24. The Diamond*Pak* 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 Diamond*Pak*.

26. If the Diamond*Pak* is power cycled or rebooted, the Diamond*Pak* 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 Diamond*Pak* power is cycled or rebooted.

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 Diamond*Pak* to transition to the online state, download a transmit and receive mandatory access control policy to the Diamond*Pak*. 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 Diamond*Pak* shall only support or accept SHA-1 based signatures for the PKI node authentication value.

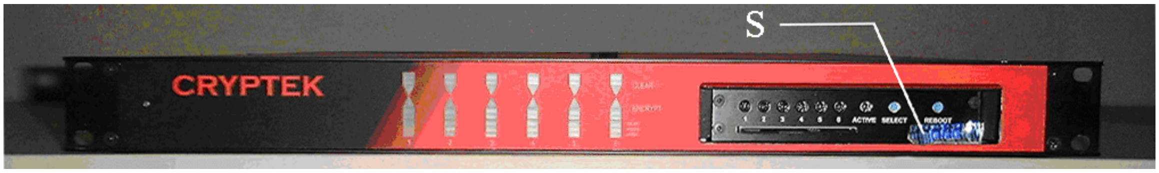
31. The Diamond*Pak* shall send all auditable events to the Diamond*Central* for logging.

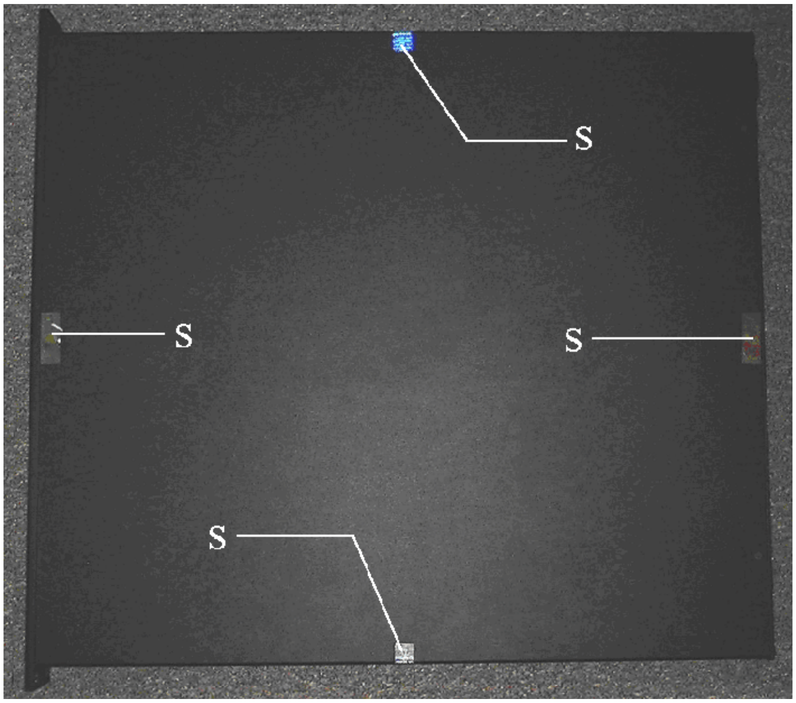
32. The ANSI 9.31 A.2.4 PRNG shall be used to generate all keys.

33. The Diamond*Central* (Administrator role) shall download communication rules (DAC policy) to the Diamond*Pak*. 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 Diamond*Pak*/CP106 is a multi-chip standalone device, with six CSMs enclosed in a commercial grade metal case. The factory affixes 4 tamper-evident seals on the top of the case (over access screws) and 1 in the card-reader bay (over an access screw) to fulfill FIPS 140-2 level 2 physical security requirements.





Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	Daily	User should inspect each seal for tamper evidence. Tampering with the seals in any way will result in the metallic foil deforming.

12 Mitigation of Other Attacks Policy

The Diamond*Pak*/CP106 cryptographic device 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
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