# FIPS 140-2 Security Policy

# Thales Datacryptor Gigabit

## Firmware Version 2.2

## Hardware Version C

**ECO, Date, and Revision History**

Rev A  CB-078, 05/07/04, dtm Initial release
Rev B CB086,dtm, Mods requested by Domus
Rev C CB087, dtm, mods requested by DOMUS
Rev C CB087, dtm, mods requested by DOMUS  Rev C CB087, dtm, mods requested by DOMUS

| | | | |
|---|---|---|---|
| Contact:  Denise McQuillin | | THALES<br>2200 North Commerce Parkway, Suite 200<br>Weston, FL  33326 | |
| Checked: | Approved: | | |
| Filename: 007-002-201_c Thales.doc | | | |
| Title: | **FIPS 140-2 Security Policy**<br>**Thales Datacryptor Gigabit** | | |
| Date:<br>**12/15/04** | Document Number:<br>**007-002-201** | Rev:<br>**C** | Sheet:<br>**1 of  15** |

**Table of Contents**

# 1 Introduction Thales Datacryptor Gigabit Security Policy

This document describes the security policy of the Thales Datacryptor Gigabit as required and specified in the NIST FIPS-140-2 standard. Under the standard, the Datacryptor Gigabit system qualifies as a multi-chip stand-alone cryptographic module and satisfies overall FIPS 140-2 level 2 security requirements.

This document applies to Hardware Version C and Firmware Version 2.2.

The Datacryptor Gigabit is in FIPS mode when the module is powered on and processing traffic using FIPS approved cipher/authentication algorithms as established through the policy editor by the Crypto Security Officer. Datacryptor Gigabit refers to Thales Datacryptor Gigabit.

This security policy is composed of:
A definition of the Datacryptor Gigabit's security policy, which includes:

- an overview of the Datacryptor Gigabit operation
- a list of security rules (physical or otherwise) imposed by the product developer

A description of the purpose of the Datacryptor Gigabit's security policy, which includes:

- a list of the security capabilities performed by the Datacryptor Gigabit

Specification of the Datacryptor Gigabit's Security Policy, which includes:

- a description of all roles and cryptographic services provided by the system
- a description of identification and authentication policies
- a specification of the access to security relevant data items provided to a user in each of the roles
- a description of physical security utilized by the system
- a description of attack mitigation capabilities

# 2 Definition of Datacryptor Gigabit Security Policy

## 2.1 Datacryptor Gigabit Operation Overview

The Datacryptor Gigabit is a high performance, integrated security appliance that offers Gigabit Ethernet IPSec encryption. Housed in a tamper evident chassis, the Datacryptor Gigabit has two Gigabit Ethernet ports. The appliance receives plaintext data on the local port from the trusted network, and transmits encrypted data to the unsecured network on the remote (cipher) port. Encrypted data arrives from the unsecured network on the remote (cipher) port. The appliance then decrypts it and sends it out on the local port in plaintext.

Fully compatible with existing IP networks, the Datacryptor Gigabit can be seamlessly deployed into Gigabit Ethernet environments, including IP site-to-site VPNs and storage over IP networks. Its high-speed AES and 3DES IPSec processing eliminates bottlenecks while providing data authentication, confidentiality, and integrity.

Figure 1 shows the physical layout of the Datacryptor Gigabit. The back of the module (not displayed) contains a standard, enclosed line cord receptacle and cannot be exploited.

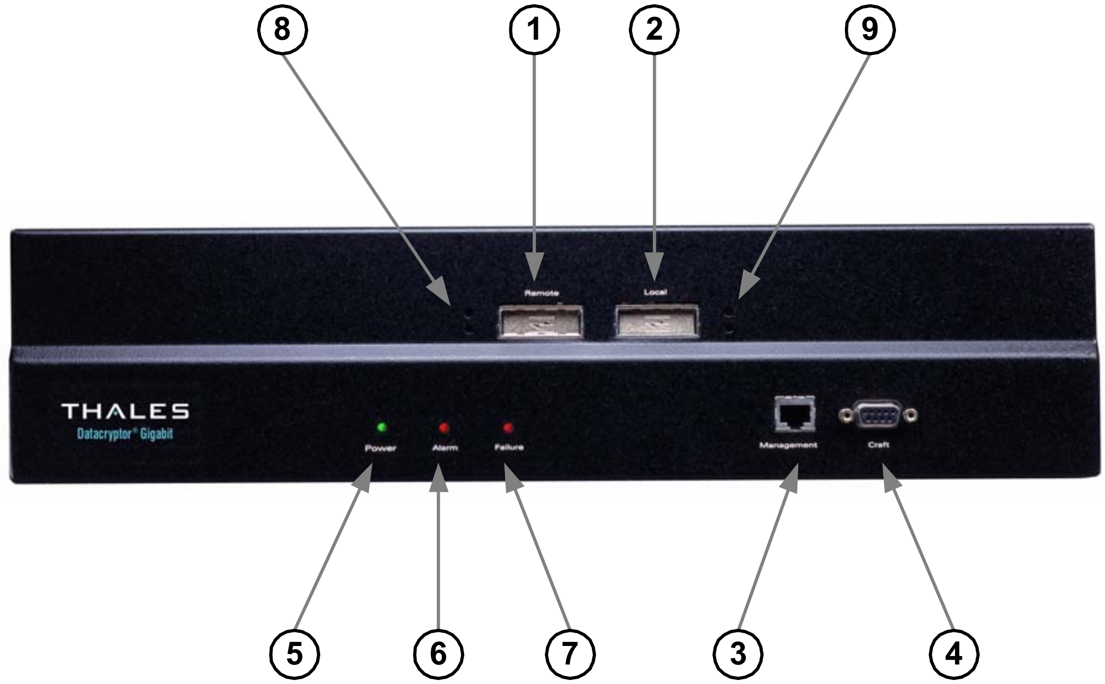

**Figure 1. Physical Layout of Indicators, and Receptacles (Front View)**

1. Remote Gigabit Ethernet Port
2. Local Gigabit Ethernet Port
3. 10/100 Ethernet Management Port
4. RS-232 Craft Port
5. Power LED
6. Alarm LED
7. Failure LED
8. Remote Port LEDs
9. Local Port LEDs

A typical operating environment is illustrated in Figure 2.

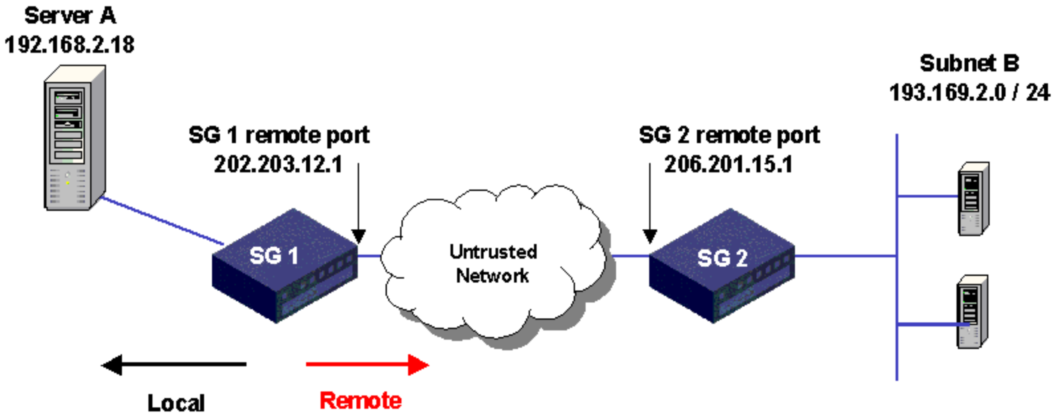

**Figure 2. Typical Operational Configuration**

## 2.2 Product Features

**Hardware-based IPSec encryption processing**

- Low latency
- 1024 concurrent tunnels

**Line rate Gigabit Ethernet**

- Full duplex 1.8 Gbps IPSec AES and 3DES encryption and decryption

**Comprehensive security standards support**

- Compliant with IPSec RFC 2401, 2408, 2409
- Encapsulating Security Payload (ESP) and Authentication Header (AH) supported in Tunnel mode

| *Approved Security Function* | *Certificate* |
|---|---|
| ***Symmetric Key Encryption*** | |
| **AES (CBC (e/d; 128, 192, 256))** | 156 |
| **TDES (TCBC (e/d; KO 1,2,3))** | 258 |
| **DES (CBC (e/d (for legacy systems only))** | 260 |
| ***SHS*** | |
| **SHA-1 byte-oriented** | 117 |
| **HMAC-SHA-1 (vendor affirmed)** | 117 |
| ***Asymmetric Keys*** | |
| **RSA (PKCS#1) (Sig Gen and Sig Ver) (vendor affirmed)** | |
| **Random Number Generation (ANSI X9.62)** | |
| *Non-Approved Security Function* | |
| **Diffie-Hellman (key agreement)** | |
| **MD5** | |
| **HMAC MD5** | |

**Encryption**

- DES-CBC (56 bit)  [ for legacy support only ]
- 3DES-CBC (168 bit)
- AES-CBC (256 bit)

**Message integrity**

- HMAC-MD5-96 (Available in Non FIPS mode only)
- HMAC-SHA-1

**Signature Verification**

- RSA (PKCS#1, Vendor Affirmed)

**Device management Thales Datacryptor Gigabit**

- Management access via the RS-232 craft port or secure 10/100 Ethernet port

- Secure management access via XML-RPC (see Glossary)
- Command line and web-based management interfaces
- Secure SSL-TLS session for management application
- Secure IPSec session for management application
- Secure telnet session for device configuration
- SNMPv2c MIB managed objects supported
- Alarm condition detection and reporting through audit log capability
- Secure remote authenticated software updates

## 2.3 IPSec Technology Overview

IPSec is a framework of standards developed by the Internet Engineering Task Force (IETF) that provides a method of securing sensitive information that is transmitted over an unprotected network such as the Internet.

IPSec does this by specifying which traffic to protect, how to protect it, and who to send it to. It provides a method for selecting the required security protocols, determining the algorithms to use for the services, and putting in place any cryptographic keys required to provide the requested services. Because the IP layer provides IPSec services, they can be used by any higher layer protocol.

### 2.3.1 IPSec Services

IPSec security services include:

- Data confidentiality - The sender can encrypt packets before sending them across a network, providing assurance that unauthorized parties cannot view the contents.
- Data integrity - The receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered in transit.
- Data origin authentication -The receiver can authenticate the identity of the sender. This service is dependent on the data integrity service.
- Anti-replay protection - The receiver can detect and reject replayed packets.

## 2.4 Security Rules for FIPS Level 2 Operation

The Datacryptor Gigabit is bound by the following rules of operation to meet FIPS 140-2 Level 2 requirements.

### 2.4.1 Operational Constraint

The Datacryptor Gigabit encryption module shall be operated in accordance with all sections of this security policy. The module shall be operated in accordance with all accompanying user documentation.

- Thales Datacryptor Gigabit User Guide, Release 2.2

### 2.4.2 Security Policy Limitation

This security policy is constrained to the hardware, software, and firmware contained within the cryptographic security boundary.

### 2.4.3 Discretionary Access Control

Discretionary access control based roles shall be assigned in accordance with this security policy.

### 2.4.4 Default Deny

This module is shipped with all encryption mechanisms disabled to allow installation test and acceptance. Prior to operation, encryption mechanisms shall be enabled, and the module placed in a default deny operational mode.

### 2.4.5 Power Requirements

It is assumed that this module is being powered at the specified line voltage (115 VAC, 60 Hertz nominal, for the United States) and that the internal DC power supply is operating normally.

### 2.4.6 Processing of Classified Information

This module shall not process, protect, or store classified information.

### 2.4.7 Security Modes

The Datacryptor Gigabit must always be configured to FIPS approved encryption and message authentication – AES, 3DES/DES and SHA1.

The Datacryptor Gigabit GUI Interface (browser) must always operate using FIPS approved cipher/authentication algorithms – AES, 3DES/DES and RSA (for authentication). The browser is used for Policy Management of the Datacryptor Gigabit.

The Datacryptor Gigabit management interface (telnet using IPSec) must always operate using FIPS-approved cipher/authentication algorithms – AES, DES, 3DES, and SHA1 authentication.

### 2.4.8 Physical Level Security

The Datacryptor Gigabit shall be installed in a controlled area with authorized personnel access only.

## 2.5 Secure Setup Procedure

The Datacryptor Gigabit must be set up, installed, and operated in accordance with the instructions in the User Guide.

- Thales Datacryptor Gigabit User Guide, Release 2.2

For secure device management using telnet, IPSec must be enabled on the management port and a VPN Client must be installed on the management workstation. For detailed instructions refer to the Thales Datacryptor Gigabit User Guide, Release 2.2. IPSec on the management port must always operate using FIPS-approved cipher and authentication algorithms (AES, DES, 3DES encryption and SHA1 authentication). MD5 authentication is also available in non-FIPS mode operation.

The Datacryptor Gigabit is shipped with all encryption mechanisms disabled to allow installation test and acceptance. Prior to operation, encryption mechanisms should be enabled.

- The Datacryptor Gigabit browser interface to the Policy Manager application must be operated using FIPS-approved cipher and authentication algorithms (AES, DES or 3DES encryption and RSA authentication).
  - Microsoft Internet Explorer version 6.0 or higher (www.microsoft.com ); or
  - Netscape version 7.0. (www.netscape.com)

  **Note**: The browser must support high-grade (128-bit) security.

The Datacryptor Gigabit's tamper-evident seal must be intact. If the tamper-evident seal is broken, the Datacryptor Gigabit is not FIPS-140-2 Level 2 compliant.

The following user-supplied software must be installed on the management workstation:

- VT-100 terminal emulation utility such as HyperTerminal or TeraTerm Pro (Used to connect to the CLI through a serial link)
- Adobe Acrobat Reader version 5.0 or higher (www.adobe.com) (used to open the PDF files on the Datacryptor Gigabit CD).
- VPN client application such as SSH Sentinel

The following operating systems are supported:

- Microsoft Windows 2000
- Linux 2.4 (Red Hat Linux 7.2)

## 2.6 Initiating FIPS Compliant Mode

As stated in section 2.5 (above), the Datacryptor Gigabit is shipped with all encryption mechanisms disabled.

For the Thales Datacryptor Gigabit to initiate the module in FIPS Compliant mode the Crypto-Officer (Ops User) must create and load a policy (via the Policy Editor) that uses AES, DES or 3DES for data encryption and HMAC SHA-1 for authentication.

**NOTE:** MD5 is not a FIPS-approved authentication algorithm. Using MD5 authentication in a security policy takes the Datacryptor Gigabit out of FIPS compliant operation.

# 3 Purpose of a Datacryptor Gigabit Policy

The Datacryptor Gigabit is a high performance security appliance that offers IPSec encryption for Gigabit Ethernet (1 Gbps) traffic. The Datacryptor Gigabit has two Gigabit Ethernet ports. The appliance receives plaintext data on the local port from the trusted network, and transmits encrypted data to the unsecured network on the remote (cipher) port. Encrypted data arrives from the unsecured network on the remote (cipher) port. The appliance then decrypts it and sends it out on the local port in plaintext.

The AES and 3DES algorithms employed by the Datacryptor Gigabit to encrypt/decrypt all sensitive data, is the current standard for the protection of Unclassified but Sensitive Information for the Federal Government. In addition, the SHA-1 algorithm is used to provide message integrity and authentication.

## 3.1 Datacryptor Gigabit Security Feature Overview

**Security Features**

- Hardware-based IPSec encryption processing
- Comprehensive security standards support
- Compliant with IPSec RFC 2401
- Encapsulating Security Payload (ESP) and Authentication Header (AH) supported in Tunnel mode

**Key Management**

- Internet Key Exchange (IKE) RFCs 2408, 2409

**Key Exchange**

- Authenticated Diffie-Hellman key exchange

**Key Types**

| Key Name | Description and /or Purpose | Type of Key | Storage Location | Storage Method |
|---|---|---|---|---|
| Manual Key<br>Cipher Secret | Encryption / Decryption | 32 Byte AES<br>24 Byte 3DES<br>8 Byte DES | Non-volatile Flash | Policy File – Plain-text |
| Manual Key<br>Hash Secret | Message Signing | 20 Byte HMAC-SHA-1-96 | Non-volatile Flash | Policy File – Plain-text |
| IPSec Session Encryption Key | One Symmetric Key per IPSec Security Association (SA) | 32 Byte AES<br>24 Byte 3DES | Volatile SDRAM | Plain-text |
| IPSec Session Authentication Key | One Authentication Key per IPSec Security Association (SA) | 20 Byte HMAC-SHA-1-96 | Volatile SDRAM | Plain-text |
| Management Interface Certificate Session Key | Encrypt messages to and from policy editor | 256 Bit AES<br>168 Bit 3DES | Volatile SDRAM | Plain-text |
| Module Keys | Authenticate messages to and from policy editor<br><br>Authenticate module to remote devices | 1024 Bit RSA | Non-volatile Flash | Plain-text |

**Zeroization**

- Sets module to factory default keys
- Sets module to factory default policies
- Sets module to factory default configurations
- All plaintext keys are zeroized

**Encryption**

- AES-CBC (256 bit)
- 3DES-CBC (168 bit)
- DES-CBC (56 bit)  [ for legacy support only ]

**Message integrity**

- HMAC SHA-1
- HMAC-MD5-96 (Available in Non FIPS mode only)

**Signature Verification**

- RSA (PKCS#1, Vendor Affirmed)

**Device management Thales Datacryptor Gigabit**

- Management access via the RS-232 craft port or secure 10/100 Ethernet port
- Secure management access via XML-RPC (see Glossary)
- Command line and web-based management interfaces
- Secure SSL-TLS session for management application
- Secure IPSec session for management application
- Secure telnet session for device configuration
- SNMPv2c MIB managed objects supported
- Alarm condition detection and reporting through audit log capability
- Secure Remote authenticated software updates.

**Role Based Access Control**

- Access to security configuration and device management controlled by strict userid/password authentication

## 3.2 Module Self-Tests

- As required by FIPS 140-2, the module performs the following self-tests at start-up:

**Power-Up Tests:**

- AES Known Answer Test
- 3DES Known Answer Test
- DES Known Answer Test
- HMAC-SHA-1 Known Answer Test
- Pair wise consistency test for RSA and Diffie-Hellman
- Software Integrity Test

**Continuous Random Number Generator Test:**

- The module includes a continuous test on the output from the FIPS compliant RNG to ANSI X9.62. The module compares the output of the RNG with the previous output to ensure the RNG has not failed to a constant value.

**Software Load Test:**

- The module includes a software/firmware load test with an RSA signature verification of downloaded software/firmware.
- In order for the module to maintain FIPS compliance the software/firmware to be upgraded must be validated to FIPS 140-2.

If any of these self-tests fail, the module enters an error state and all data is inhibited. Running of the power-on self-tests is automatically initiated whenever power to the module is cycled or, on demand, by issuing the “reboot” command.

# 4 Specification of the Datacryptor Gigabit Security Policy

Three roles, that either provide security services or receive services of the Datacryptor Gigabit, are the basis of the specification of the Datacryptor Gigabit security policy. These roles are:

- Crypto Security Officer: The Crypto Security Officer role consists of the Ops user.□ipherOptics The role defines and implements all security and network services. The role specifies the traffic to have security algorithms applied and the transforms to be applied, defines the IP network interfaces and remote management mechanisms, and performs any software updates or network troubleshooting.
- Crypto Security Officer A: The Crypto Security Officer “A” role consists of the Admin user.□ipherOptics. The role controls access to the Datacryptor Gigabit by maintaining all role-based userid/password configurations.
- User: The User role uses the security services implemented on the Datacryptor Gigabit. The User is any entity with an assigned IP address that matches the module’s IPSec policy as defined by the Crypto Security Officer User role. The Datacryptor Gigabit receives user traffic on its local port. It then applies the security services to that traffic and transmits the traffic out the remote port. In addition, the Datacryptor Gigabit can receive encrypted traffic on its remote port, decrypt the traffic and transmit the traffic to the user on the local port.

## 4.1 Identification and Authentication Policy

Login by UserID and Password, which are maintained by the Crypto Security Officer A, is the primary Identification /Authentication mechanism used to enforce access restrictions for performing or viewing security relevant events. The following table defines the Identification and Authentication Policy:

| **Role** | **Identification/ Authentication** |
|---|---|
| | Thales Datacryptor Gigabit |
| Crypto Security Officer (CSO) | Ops UserId/Password |
| Crypto Security Officer A (CSOA) | Admin UserId/Password |
| User | IPSec Policy |

Note: Any reference of CSO and CSOA under the Access Control, Roles, and Services indicates the Identification/Authentication as found in the table above.

**Table 1 – Identification/Authentication Policy**

Access of the Crypto Security Officer may be denied after unsuccessful login attempts. The Crypto Security Officer may set inactivity time outs for Login sessions.

## 4.2 Access Control, Roles, and Services

The roles defined above use and/or implement a number of security services in the Datacryptor Gigabit. Those services are:

- Test Functions – internal system test of hardware and software at power up or reboot
- Encryption/Decryption – services executed on user data
- Key Generation – Services to generate and update secure key material
- Network Services – services to manage and configure the network interfaces of the system
- Security Services – services to configure and protect the security policy of the system
- Upgrade – upgrades system software

Table 2 below defines the services, the roles that use the services, the security relevant objects created or used in the performance of the service, and the form of access given to those security relevant objects.

The cryptographic boundary for the implementation of these services extends to the physical dimensions of a Datacryptor Gigabit module and includes all internal printed circuit cards, integrated circuitry, and so forth contained within its physical dimensions.

Note: Items highlighted in blue in Table 2 are Services with description of services detailed directly below highlighted area.

**Table 2 – Roles and Services**

| **Roles** | **Service** | **Security Relevant Data Item** | **SRDI Access Read, Write, Edit, Delete, Use** |
|---|---|---|---|
| | **Self-Test Functions Service** | | |
| **CSO:**<br>Reboot command initiated via CLI or Web Browser<br>**CSOA:**<br>Reboot command initiated via CLI only | Self-test (critical function test, memory test, encrypt hardware test, algorithm self-tests, software authentication, RNG test). | Encrypt/decrypt test of algorithms | Use |
| | **Encryption/Decryption Service** | | |
| **User** | ***Transparent to User:***<br>• Receive/Generate IP Packets<br>• User or server creates packet and transmits to system<br>• Clear packets (i.e. plain text) are presented to the input local network port for encryption. Encrypted packet is output on remote network port. | AES/3DES Session Key | Write |
| | **Key Generation Service** | | |
| **CSO:**<br>Login to the policy editor via the secure web browser | IKE policy definition | Diffie-Hellman | Write/Edit |
| **CSO:**<br>Login to the policy editor via the secure web browser | For IKE negotiated policy:<br>The CSO enters the pre-shared secret or module certificate<br>**Note:** *the pre-shared secret is used by the module in the generation of the Encryption/Decryption Keys.*<br>For manual key policy[1]:<br>The CSO enters the Encryption/Decryption Seed<br>**Note:** *The CSO sets the lifetime of the Cipher keys for an IKE negotiated policy (once the lifetime expires, new keys are automatically generated by the module).* | AES/3DES Session Key<br>RSA Certificate<br>Diffie-Hellman | Write/Use |
| [1] The Datacryptor Gigabit's "**Manual Key Policy**" is a form of **Electronic Key Entry** and should not be confused with "**Manual Key Entry**", as defined by the FIPS 140-2 Standard. The Admin User, after entering the Policy Editor via the secure web browser connection and creating a new Manual Key Policy, manually types into the GUI interface 48 HEX values (which equals 192 bits) for 3DES and 64 HEX values (which equals 256 bits) for AES. When the new Manual Key Policy is saved and loaded, the HEX values are sent to the module via the secure web browser connection and the module's internal mechanism uses these bits to create the keys.<br>’“” | | | |
| | **Network Services** | | |
| **CSO:** | Specification of remote/ local network addresses* | Network Data | Write/Use |

| **Roles** | **Service** | **Security Relevant Data Item** | **SRDI Access Read, Write, Edit, Delete, Use** |
|---|---|---|---|
| via CLI only | Specification of management address* | Network Data | Write/Use |
| | Specification of SNMP attributes | Network Data | Write/Use |
| | Show status<br>• Display network statistics | Data | Read |
| | Show configuration<br>• Display network configuration | Data | Read |
| | **Security Services** | | |
| **CSOA:**<br>via CLI | Define and maintain userids and passwords | Userid/ Passwords | Write/Edit/Use |
| **CSO:**<br>Defined in policies using Policy Editor via secure web browser | Define security policies for encryption/discard | Desired filters | Write/Edit |
| **CSO:**<br>via CLI | Show status<br>• Display security status of each established channel/path - Terminal output also indicates error status<br>• Show Configuration<br>• Display current network and security configuration. | Data | Read |
| **CSO:**<br>via CLI<br>(command "Clear All") | System Zeroization<br><br>Manual Keys<br>All pre-shared secrets<br>Diffie-Hellman Keys<br>IPSec Session Keys (DES, 3DES, AES)<br>Module Keys | Cryptographic Key data<br><br>Policies<br><br>Configurations<br><br>RSA public/private keys | Delete/Write<br><br>**Note***: During zeroization, the factory default keys, polices & configurations overwrite the current information on the module.* |
| **CSO:**<br>via secure web browser | Expiration of key lifetime<br>**Note:** *The CSO sets the lifetime of the Cipher keys for an IKE negotiated policy (once the lifetime expires, new keys are automatically generated by the module).* | Encryption Key<br><br>AES/DES/3DES | Delete/Write |
| **CSO:**<br>via CLI and secure web browser<br>**CSOA:**<br>via CLI | System reboot<br><br>Policy Reload | Clear IKE negotiated keys | Read/Delete |
| | **Upgrade** | | |
| **CSO:**<br>via CLI | New firmware downloaded to system | RSA 2048 bit firmware verification public key | Use |

## 4.3 Physical Security Policy

The Datacryptor Gigabit system has been designed to□ipherOptics satisfy the Level 2 physical security requirements of FIPS140-2. The system is housed in an opaque, steel chassis with external connections provided for the local and remote data network ports, as well as the Craft (serial) port, 10/100 Ethernet port, and status LEDs. The top lid and baseboard sub-assembly are attached to the case using screws. A tamper evident seal is provided over one screw in such a manner that an attempt to remove the cover requires removal of that screw and indicates subsequent evidence of tampering.

The Crypto Security Officer shall periodically check the tamper evident seal to verify that the module has not been opened. If the seal is broken, the module is no longer FIPS-140-2 compliant. The tampered module shall be returned to Thales for re-certification (following the required return procedures). Other modules with which it exchanged keys and have no evidence of tampering, shall be zeroized.

## 4.4 Strength of Function

Within the cryptographic security boundary, the Datacryptor Gigabit will only act on traffic for which a security policy has been defined. Therefore any data received for which no policy exists will be discarded. In addition, any clear traffic destined for the Datacryptor Gigabit's network address will be discarded. The Datacryptor Gigabit will only respond to IP protocol 50 and 51 and TCP/UDP port 500 packets. Thus port scans and DOS attacks are mitigated.

A secure environment relies on security mechanisms, such as firewalls, intrusion detection systems and so forth, to provide mitigation of other attacks, which could lead to a loss of integrity, availability, confidentiality, or accountability, outside of the cryptographic security boundary. Further, no mitigation is provided against clandestine electromagnetic interception and reconstruction or loss of confidentiality via covert channels (such as power supply modulation), or other techniques, not tested as part of this certification.

# 5 Glossary of Terms

**Authentication**
Authentication is the process of identification of a user, device or other entity, (typically based on a password or pass phrase) known only to a single user, which when paired with the user's identification allows access to a secure resource.

**CBC**
The cipher-block chaining mode of DES – See FIPS Publication 81 for a complete description of CBC mode.

**Confidentiality**
Confidentiality is the assurance that information is not disclosed to unauthorized persons, processes, or devices.

**Configuration Management**
Management of security features and assurances through control of changes made to hardware, firmware, software, or documentation, test, test fixtures, and test documentation throughout the lifecycle of the IT.

**Crypto Security Officer (CSO)**
The Crypto Security Officer is the individual responsible for all security protections resulting from the use of technically sound cryptographic systems. The Crypto Security Officer duties are defined within this document.

**Crypto Security Officer A (CSOA)**
The Crypto Security Officer A is the individual responsible for controlling access to the Datacryptor Gigabit by maintaining all role-base userid/password configurations. The Crypto Security Officer A duties are defined within this document.

**DES**
A cryptographic algorithm for the protection of UNCLASSIFIED data, published in Data Encryption Standard FIPS Publication 46, DES was approved by the National Institute of Standards and Technology (NIST), and is intended for public and private use.

**End to End Encryption**
The totality of protection of information passed in a telecommunications system by cryptographic means, from point of origin to point of destination.

**IKE**
Internet Key Exchange

**IP**
Internet Protocol
**IPSEC**
Security standard for IP networks
**NIST**
National Institute of Standards and Technology
**Role**
A Role is a pre-defined mission carrying with it a specific set of privileges and access based on required need-to-know
**Role Based Access Control (RBAC)**
RBAC is an access control mechanism, which restricts access to features and services used in the operation of a device based on a user's predefined mission.
**Session Key**
An encryption or decryption key used to encrypt/decrypt the payload of a designated packet.
**Security Policy**
The set of rules, regulations and laws which must be followed to ensure that the security mechanisms associated with the Thales Datacryptor Gigabit are operated in a safe and effective manner. The Thales Datacryptor Gigabit Security Policy shall be applied to all IP data flows through the Datacryptor Gigabit, per FIPS 140-2 (Level 2) requirements. It is an aggregate of public law, directives, regulations, rules, and regulates how an organization shall manage, protect, and distribute information.
**TCP**
Transmission Control Protocol
**Tunnel**
Logical IP connection in which all data packets are encrypted
**UDP**
User Datagram Protocol
**XML-RPC**
A Remote Procedure Calling protocol having a set of implementations that allow software running on disparate operating systems, running in different environments to make procedure calls over the Internet. It's remote procedure calling uses HTTP as the transport and XML as the encoding. XML-RPC is designed to be as simple as possible, while allowing complex data structures to be transmitted, processed and returned.

# 6 References

Federal Information Processing Standard Publication 140-2 "Security Requirements for Cryptographic Modules," (Supercedes FIPS Publication 140-1, 11 January 1994

□ipherOpticsThales Datacryptor Gigabit Release 2.2 User Guide

CipherOptics Security Gateway FIPS 140-2 Vendor Evidence Document, April 2004

Finite State Machine Document, November 23, 2002

Security Gateway IPSec Module Design Specification, November 27, 2002

# 7 Revisions

This document is an element of the Federal Information Processing Standard (FIPS) Validation process as defined in Publication 140-2. Additions, deletions, or other modifications to this document are subject to document configuration management and control. No changes shall be made once stamped FINAL, without the express approval of the Document Control Officer (DCO).

## 7.1 Revision History

| Revision | Change Description | Change Document | Approved |
|---|---|---|---|
| A | Original Issue | CB-078 | 05/07/04 |
| B | Mods per NIST comments | CB-086 | 11/29/04 |

|  |  |  |  |
|---|---|---|---|
| C | Mods per NIST comments | CB-087 | 12/15/04 |