THALES e-SECURITY

Datacryptor® SONET/SDH OC-3/12/48/192C

FIPS 140-2 Level 3 Security Policy

Firmware Version v5.0

Hardware Versions

OC-3/12C/48C	*1600X435, Rev. 02*
OC-192C	*1600X427, Rev. 02*

Thales e-Security, Inc 2200 North Commerce Parkway, Suite 200, Weston, FL 33326, USA

TEL: + 1-888-744-4976
FAX: + 1-954-888-6211

http://www.thalesesec.com

CONTENTS

Tables

Figures

1. INTRODUCTION

Thales e-Security is a global leader in the network security market with over 60,000 network security devices in operation, being one of the first companies to introduce a link encryption product to the market in the early 1980s.

The Datacryptor® family represents Thales' next generation of network security devices for a wide variety of communications environments. It is the culmination of 20 years' experience protecting wide-area and point-to-point networks for governments, financial institutions and information-critical industries worldwide.

This document is the Security Policy[1] for the Thales e-Security Datacryptor® SONET/SDH OC-3/12/48/192C, conforming to the FIPS140-2 Security Policy Requirements [1].

Further information on the Datacryptor® family and the functionality provided by the Datacryptor® SONET/SDH OC-3/12/48/192C is available from the Thales web site: http://iss.thalesgroup.com

Overview

The Datacryptor® SONET/SDH OC-3/12/48/192C is a multi-chip standalone cryptographic module which facilitates secure data transmission across SONET networks using OC-3C, OC-12C, OC-48C or OC-192C.

This Security Policy defines the Datacryptor® SONET/SDH OC-3/12/48/192C cryptographic module for two hardware versions, 1600X435, Rev. 02 (low speed module) which supports data transmission using OC-3C, OC-12C or OC-48C, and 1600X427, Rev. 02 (high speed module) which supports data transmission using OC-192C. These variants utilize a different hardware platform but are functionally identical therefore all references to Datacryptor® SONET/SDH OC-3/12/48/192C or module refer to both variants unless explicitly stated otherwise.

Figure 1-1 shows a typical Datacryptor® SONET/SDH OC-3/12/48/192C configuration where 2 LANs are securely linked across a public domain SONET network.

Modes of Operation

The Datacryptor® SONET/SDH OC-3/12/48/192C can only operate in an FIPS 140-2 Approved mode (this includes cryptographic services and bypass services). The modes of operation are detailed below:

- Standby Mode — The module transmits/receives no data via either its Host or Network interfaces on that channel. This mode is automatically entered if the module detects an error state or at start-up. This mode is indicated by the green flashing Encrypt LED.

- Plain Text Mode[2] — All data received through the Host interface on that channel is transmitted through the Network interface as plain text. Similarly, all data received through the Network interface on that channel is

[1] This document is non-proprietary and may be reproduced freely in its entirety but not modified or used for purposes other than that intended.

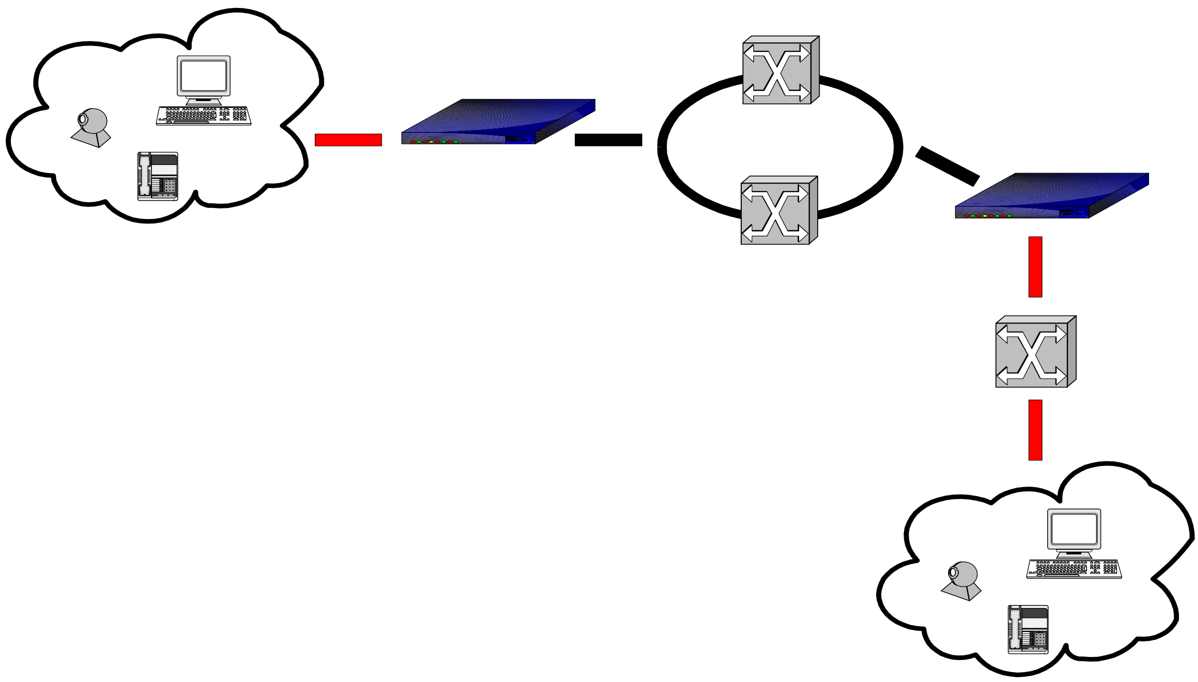
[2] This is the bypass mode.

transmitted through the Host interface with no decryption applied. This mode should only be used for diagnostic purposes, or if there is no security risk to the data if it is transferred unencrypted. This mode is indicated by the solid red Plain LED. The module does not support an alternating plaintext mode.

- Encrypt Mode — All data received through the Host interface on that channel is encrypted using the transmit Data Encryption Key (DEK) and then the encrypted data is transmitted through the Network interface. Similarly, all data received through the Network interface on that channel is decrypted using the receive DEK and then the decrypted data is transmitted through the Host interface. This mode is indicated by the solid green Encrypt LED.

The mode of operation is selectable by the Crypto Officer using the Secure Remote Management facility and the current mode of operation is displayed using both the Front Panel LEDs and the Secure Remote Management (Element Manager PC) facility. Refer to the User Manual [3] for further details.

Figure 1-1 Datacryptor® SONET/SDH Crypto Module Example Network Configuration



Physical Ports

Both variants of the Datacryptor® SONET/SDH OC-3/12/48/192C provide the same set of physical ports with the exception of the host and network line interfaces, which use Small Form Factor Pluggable (SFP) for low speed modules and 10 Gigabit Small Form Factor Pluggable (XFP) for high speed modules.

The physical ports are described below in Table 1-1 Physical Ports and Status Indicators:

Table 1-1 Physical Ports and Status Indicators

Port	Description
Network	Connects to the public network for sending and receiving encrypted user data and inter-module key exchange data. This is an optical port.
Host	Connects to the private network for sending and receiving plaintext user data. This is an optical port.
RS-232	Connects to a local terminal for initialization of the module and also allows remote management from the Element Manager application utilizing the Point-to-Point (PPP) protocol.
Ethernet	Allows the remote management of a unit using the Element Manager application and status report using an SNMP management application.
Front Panel LEDs	Indicates the operational state of the unit, including Alarm state, Error state, Plain or Encrypt mode and Host and Network line status.
Line Interface LEDs	Indicates module present and laser input detected.
PSU LEDs	Indicates the status of the PSUs (powered/unpowered)
Power	Dual redundant power interface supporting customer options of AC or DC and international power cord standards.

The physical ports are mapped to four logical ports defined by FIPS 140-2 as described below in Table 1-2 Physical Port to Logical Port Mapping:

Table 1-2 Physical Port to Logical Port Mapping

Logical Interface	Description and Mapping to Physical Port
Data Input	Host Line Interface Network Line Interface
Data Output	Host Line Interface Network Line Interface
Control	RS-232 Interface Ethernet Interface
Status	RS-232 Interface Ethernet Interface Front Panel LEDs Line Interface LEDs PSU LEDs

User Data Security

The communications channel between two Datacryptor® SONET/SDH OC-3/12/48/192Cs is assumed to be vulnerable and therefore the Datacryptor® SONET/SDH OC-3/12/48/192C encrypts the entire user data stream[3].

The Datacryptor® SONET/SDH OC-3/12/48/192C uses public key cryptography for authentication and key agreement[4]. Symmetric key cryptography is used for data confidentiality. The authentication mechanism employs signed X.509 v3 certificates using the Elliptic Curve Digital Signature Algorithm (ECDSA) for signature verification. The Elliptic Curve Diffie-Hellman (ECDH) protocol is used to establish a Key Encryption Key (KEK) between modules. Data Encryption Keys (DEKs), used for encrypting and decrypting data traffic, are derived from the KEK.

Random Number Generation

This consists of a hardware random number source which provides entropy to a NIST SP800-90 Section 10.1 [2] approved deterministic random bit generator (DRBG).

Establishment of the module's generated private and secret keys (Elliptic Curve Diffie-Hellman static/ephemeral and Data Encryption Keys) uses the above random bit generation mechanism.

Algorithm Support

The Datacryptor® SONET/SDH OC-3/12/48/192C contains the following algorithms:

- AES-256 for data encryption
- ECDSA using the P-384 curve for signature verification
- SHA-384 hashing algorithm
- ECDH using the P-384 curve for key agreement

Physical Security

The multi-chip standalone embodiment of the circuitry within the Datacryptor® SONET/SDH OC-3/12/48/192C is contained within a strong metal production-grade enclosure that is opaque within the visible spectrum to meet FIPS 140-2 Level 3. The enclosure completely covers the module to restrict unauthorized physical access to the module. The physical security includes measures to provide both tamper evidence and tamper detection and response. In the case of tamper response all sensitive information stored within the module will be zeroised.

The Datacryptor® SONET/SDH OC-3/12/48/192C's cryptographic boundary (FIPS 140-2 [1], section 2.1) is the physical extent of its enclosure but excludes the dual redundant power supplies which are external to this boundary and may be hot-swapped by a customer and does not require a "return to factory" operation.

[3] Providing the module is configured to operate in Encrypt mode.

[4] This key agreement method provides 192-bits of encryption strength.

Secure Remote Management

The Datacryptor® SONET/SDH OC-3/12/48/192C may be remotely and securely managed using the Element Manager.

SNMP Status Management

The Datacryptor® SONET/SDH OC-3/12/48/192C can also be managed (for status only) using an SNMP v1, v2c or v3 management application. Only one management session is permitted at a time with a Datacryptor® SONET/SDH OC-3/12/48/192C.

Diagnostics

A variety of diagnostics are available to maintain secure operation. These diagnostics include cryptographic mechanisms, critical functions and environmental monitoring. In addition the module supports a local loop back mode to aid in diagnosing network connectivity. Log files are maintained in the Datacryptor® SONET/SDH OC-3/12/48/192C and can be viewed or printed.

If the Datacryptor® SONET/SDH OC-3/12/48/192C is faulty, as indicated by the failure of a self-test diagnostic, it will render itself inoperable until the fault is rectified.

- **Power-Up Tests** On power-up known answer tests (KAT) are performed on all cryptographic algorithms and the deterministic random bit generator. In addition the integrity of all firmware is checked.

Table 1-3 Power-Up Tests

Function Checked	Description
ECDSA (CA Algorithm)	KAT Test
AES-256 (KEK Algorithm)	KAT Test
AES-256 (DEK Algorithm)	KAT Test
Primitive “Z” Computation	KAT Test
SHA-384	KAT Test
Deterministic Random Bit Generator	KAT Test
Firmware Integrity	16 bit Error Detection Code (EDC) Checksum

- **Conditional Tests**
  - The output of both the hardware random number generator and the deterministic random bit generator are checked whenever random data is requested by the module. Subsequent random numbers are compared against the last generated value to verify that these values are not the same.
  - The module performs periodic health tests on the instantiate, generate, reseed and uninstantiate functions of the deterministic random bit generator. The tests performed

are known answer tests (KATs) designed to ensure the deterministic random bit generator is functioning as expected.

- The module also performs a bypass test before entering an encrypted channel mode. When switching from a plain to an encrypted channel mode the module issues an encrypted challenge to its peer using the Data Encryption Key (DEK). The challenge is then decrypted by the peer using its DEK, and if verified, an encrypted response is returned to the module (using the DEK). The response is decrypted by the module (using the DEK) and verified. If successful the channel is established as being in an encrypted state with matching DEKs in each module.
- In the case of a firmware upgrade, this is digitally signed by a CA using ECDSA with the P-384 curve allowing the module to verify the image so preventing unauthorized firmware upgrades. After loading firmware onto this module it will no longer be a FIPS 140-2 validated module unless the firmware has been FIPS 140-2 validated. This feature is used as an upgrade path for future FIPS 140-2 approved modules.
- The module performs a public key validation routine during ECDH and ECDSA operations which check all the arithmetic properties of the specified ECC public key.
- The module performs a pair-wise consistency test on the modules own ECDSA key pair that the module generates. This key pair is used to generate and verify digital signatures so the pair-wise consistency test consists of the generation and verification of a digital signature.

Table 1-4 Conditional Tests

Function Checked	Description
Hardware RBG	CRNG
Deterministic Random Bit Generator	CRNG
Deterministic Random Bit Generator	Health Tests
Bypass	Bypass Test
Firmware Upgrade Authentication	Verify (ECDSA)
Public Key Validation	ECDH and ECDSA
Pair-wise Consistency Test	Sign / Verify

2. IDENTIFICATION AND AUTHENTICATION POLICY

The two roles associated with the Datacryptor® SONET/SDH OC-3/12/48/192C are:

Crypto-Officer	Commissioning and configuration of the Datacryptor® SONET/SDH OC-3/12/48/192C.
User	This role occurs when two Datacryptor® SONET/SDH OC-3/12/48/192Cs are communicating with each other.

The Datacryptor® SONET/SDH OC-3/12/48/192C does not support multiple concurrent roles.

2.1 Crypto-Officer Role

The Datacryptor® SONET/SDH OC-3/12/48/192C can be managed by the Crypto-Officer using either of the following two methods:

- **Element Manager** - This PC-based software application enables a Crypto-Officer to commission and administer the module.
- **SNMP Management Station** - This is limited to requesting and obtaining status information from the Datacryptor® SONET/SDH OC-3/12/48/192C.

The Crypto-Officer role utilizes the Element Manager to commission and configure the module via the dedicated Ethernet or serial management port.

Commissioning a module installs a X.509 certificate (containing the CA public key, certificate name, unit serial number and certificate life time) and the required Elliptic Curve Diffie-Hellman parameters to allow the Datacryptor® SONET/SDH OC-3/12/48/192C to generate a corresponding Elliptic Curve Diffie-Hellman key set. This information is digitally signed allowing the unit to authenticate the certificate's signature using the issuing CA Public key held within the module. The module must be commissioned before it may be administered.

When administering the module the Element Manager establishes a secure connection (connection authentication and data confidentiality) to the module. This connection is established and protected in the same manner as a module to module connection. To establish the secure connection the Crypto-Officer uses a removable media key-material set containing the Crypto-Officer's name and access rights, Elliptic Curve Diffie-Hellman key set and own certificate. To access the key-material set the Crypto-Officer must login to the Element Manager by presenting the key-material set and the Crypto-Officer's own password of at least 8 ASCII printable characters. This allows the Element Manager to verify the identity of a Crypto-Officer before establishing a secure connection using the key material set.

2.2 User Role

The Crypto-Officer can download one or more signed X.509 User Certificates to the Datacryptor® SONET/SDH OC-3/12/48/192C. Each User Certificate gives a Datacryptor® SONET/SDH OC-3/12/48/192C an identity.

Identity-based authentication is implemented between two communicating Datacryptor® SONET/SDH OC-3/12/48/192C. The modules are then operating in the User role. This identity can be authenticated to another module which verifies the User Certificate's signature using the issuing CA Public key held within the module.

If the issuing CA Public key is not held within the authenticating module then verification cannot be undertaken. Therefore no communications channel can be established between the two Datacryptor® SONET/SDH OC-3/12/48/192Cs.

2.3 Authentication

The types and strengths of authentication for each Role identified for the Datacryptor® SONET/SDH OC-3/12/48/192C are given in *Table 2-1* and *Table 2-2* below.

Table 2-1 Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Crypto-Officer	Identity based	Signed X.509 Digital Certificate
User	Identity based	Signed X.509 Digital Certificate

The identity of each entity performing a role that requires authentication is held within the X.509 Digital Certificate allowing the identity and authorization of the operator to be validated by checking the signature (ECDSA) of the certificate.

Table 2-2 Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Signed X.509 Digital Certificate	The strength depends upon the size of the private key space. The Datacryptor® SONET/SDH OC-3/12/48/192C uses ECDSA with the P-384 curve, which is a FIPS Approved algorithm. Therefore the probability of successfully guessing the private key (384 bits), and hence correctly signing an X.509 certificate, is significantly less than one in 1,000,000 (2^{384}). Multiple attempts to use the authentication mechanism during a one-minute period do not constitute a threat for secure operation of the Datacryptor® SONET/SDH OC-3/12/48/192C. This is because each attempt requires the Datacryptor® SONET/SDH OC-3/12/48/192C to check the signature on the certificate that is to be loaded. Therefore the total number of attempts that can be made in a one-minute period will be limited by the Datacryptor® SONET/SDH OC-3/12/48/192C signature verification and response operation, which takes on average approximately 30 seconds. The majority of this time is accounted for by the communications overheads since the signature checking operation within the module is relatively fast. Given the very large size (384 bits) of the private key space used by the FIPS Approved signature algorithm (ECDSA) loaded in the Datacryptor® SONET/SDH OC-3/12/48/192C it follows that the probability that an intruder will be able to guess the private key, and thereby gain authentication, by making multiple attempts is significantly less than one in 100,000 (2^{384} / 2). There is no feedback of authentication data to the Crypto-Officer or User that might serve to weaken the authentication mechanism.

3. ACCESS CONTROL POLICY

3.1 Roles and Services

Table 3-1 Services Authorized for Crypto Officer lists the authorized services available for each role within the Datacryptor® SONET/SDH OC-3/12/48/192C. All services require authentication to the module.

For further details of each operation refer to the Datacryptor® SONET/SDH OC-3/12/48/192C User Guide [3].

Table 3-1 Services Authorized for Crypto Officer

Service	Description	Input	Output	Access
Access module	Login/logout of the module	password, crypto officer public key, crypto officer certificate	Command response	Peer Module Certificate - read
Manage Key Material	Loads module's key material, deletes module's key material	module public key, module certificate	Command response	CA Public Key – read/write, Module Certificate – read/write
General Configuration	Display/edit module's name, description, time and interface settings.	Commands and parameters	Command response	None
Diagnostics	Reboot or erase key material. Configure loopback mode	Commands and parameters	Command response	None
IP Management	Display/edit module's ports, Ethernet and serial, configuration.	Commands and parameters	Command response	None
SNMP	Display/edit general information, SNMP version, SNMP communities and SNMP traps.	Commands and parameters	Command response	None
IP Routes	Display/edit IP routing information	Commands and parameters	Command response	None
Security	Display/edit key lifetimes, and general key exchange parameters	Commands and parameters	Command response; key exchange if forced.	Key Encryption Key – write (delete), Data Encryption Key – write (delete)
RIP	Display/edit RIP version and RIP password	Commands and parameters	Command response	None
Communications	Display/edit SONET path mode, SONET line mode, laser mode and interface mode	Commands and parameters	Command response	None
Path	Display/edit current setting of the connection – one of standby, plain or	Commands and parameters	Command response	None

Service	Description	Input	Output	Access
	encrypt.			
Line	Display current connection mode - one of standby, plain or encrypt and ping the connected unit.	Commands and parameters	Command response, ping packet to connected peer.	None
Environment	Display fan speed, module temperature and unit power status.	Commands and parameters	Command response	None
License	Display/edit currently loaded license file for the Datacryptor OC-3/12/48C module.	License file	Command Response	None
Plaintext	Enable module to perform bypass.	Commands and parameters.	Bypass test pass or fail indicated by Front Panel Status LEDs.	None

Table 3-2 Services Authorized for User

Service	Description	Input	Output	Accessed
Encrypt	Encrypt data received from the Host interface and transmit on the Network interface.	User traffic (plain)	User traffic (encrypted)	DEK – read
Decrypt	Decrypt data received from the Network interface and transmit on the Host interface.	User traffic (encrypted)	User traffic (plain)	DEK - read

Table 3-3 Unauthenticated Services

Service	Description	Input	Output	Accessed
Show Status via SNMP	View status of the module.	Commands and parameters	Status information over Element Manager or SNMP Traps	None
Show Status via LEDs	View status of the module.	None	Front Panel LEDs Status Indicators	None
Operator Callable Self Tests via Reboot	Module performs self-test	Reboot Module	Front Panel LEDs Status Indicators	None

3.2 Cryptographic Keys, CSPs and Access Rights

The cryptographic keys and CSPs stored in the Datacryptor® SONET/SDH OC-3/12/48/192C module are listed in *Table 3-4*.

All private and secret keys (Elliptic Curve Diffie-Hellman, KEKs and DEKs) are generated internally in the module and may not be either loaded or read by the Crypto Officer or User.

Table 3-4 Cryptographic Keys and CSPs

Keys/CSPs	Description	Key/CSP Type and Size	Generated/ Established	Stored	Zeroised
Master Key	Encrypts all non-volatile Keys and CSPs stored on the module.	AES (256 bits)	Generated at start-up if not present, using the module's hardware random number generator and an approved DRBG (cert #188).	FRAM (plaintext)	Upon tamper detect or by user initiated erasure of key material.
CA Public Key	The public key of the CA key pair use to verify subsequent key material loaded into the module.	ECDSA (384 bits)	Generated external and loaded as part of the commissioning process.	Non-volatile memory – Compact Flash (encrypted)	Upon tamper detect or by user initiated erasure of key material.
Own Module Certificate/Elliptic Curve Diffie-Hellman Static Key Pair	An X.509 certificate containing the module name, Elliptic Curve Diffie-Hellman static public key (the static private key is stored separately) and associated parameters. This key pair is used during the establishment of the KEK and the Management KEK.	ECDH (384 bits)	The Elliptic Curve Diffie-Hellman static key pair is generated locally by the module, using the module's hardware random number generator and an approved DRBG (cert #188) from the parameters supplied during the commissioning process. The module name and Elliptic Curve Diffie-Hellman static public key is then exported to be signed by issuing CA so forming the module certificate.	Own Module Certificate Non-volatile memory – Compact Flash (encrypted) ECDH static private key – Non-volatile memory – FRAM (encrypted)	Upon tamper detect or by user initiated erasure of key material.
Elliptic Curve Diffie-Hellman Ephemeral Key Pair	The Elliptic Curve Diffie-Hellman ephemeral key pair.	ECDH (384 bits)	The Elliptic Curve Diffie-Hellman ephemeral key pair is generated locally by the module, using the module's hardware random number generator and an approved DRBG (cert #188) from the parameters supplied during the commissioning process. This key pair is used in conjunction	Volatile memory - SRAM (encrypted)	Upon tamper detect or by user initiated erasure of key material.

Keys/CSPs	Description	Key/CSP Type and Size	Generated/ Established	Stored	Zeroised
			with the static key pair to establish the KEK.		
Peer Module Certificate/ Elliptic Curve Diffie-Hellman Static Public Key	Received during link establishment between two modules to allow authentication of the peer module using signature verification (ECDSA).	ECDH (384 bits)	Generated by peer in the same manner as Own Module Certificate.	Non-Volatile memory – Compact Flash (encrypted)	Upon tamper detect or by user initiated erasure of key material.
Key Encryption Key (KEK)	Key used to derive data encryption keys in conjunction with DEKDD	AES (256 bits)	Established during link establishment with Elliptic Curve Diffie-Hellman using the static and ephemeral key pairs.	Volatile memory – BRAM (encrypted)	Upon tamper detect or by user initiated erasure of key material.
Data Encryption Key Derivation Data/Nonce (DEKDD)	Random data used to derive data encryption keys in conjunction with KEK	256 bits	Generated during DEK derivation using the module's hardware random number generator and an approved DRBG (cert #188).	Not stored.	Not zeroised directly. The memory that holds this CSP is erased upon the tamper response/restart process.
Data Encryption Keys (DEKs)	A pair of keys (one for transmit and one for receive) used for encryption and decryption of line data.	AES (256 bits)	Generated during link establishment using AES (KEK), DEKDD and CMAC KDF operations.	Volatile memory – BRAM (encrypted)	Upon tamper detect or by user initiated erasure of key material.
Management Key Encryption Key (MKEK)	Key used to derive management data encryption keys in conjunction with MDEKDD	AES (256 bits)	Established during management link establishment with Elliptic Curve Diffie-Hellman using the static and ephemeral key pairs.	Not Stored.	Not zeroised directly. The memory that holds this CSP is erased upon the tamper response/restart process.
Management Data Encryption Key (MDEK)	A pair of keys (one for transmit and one for receive) used for encryption and decryption of management line data.	AES (256 bits)	Generated during management link establishment using AES (MKEK), MDEKDD and CMAC KDF operations.	Not Stored.	Not zeroised directly. The memory that holds this CSP is erased upon the tamper response/restart process.

Keys/CSPs	Description	Key/CSP Type and Size	Generated/ Established	Stored	Zeroised
Management Data Encryption Key Derivation Data/Nonce (MDEKDD)	Random data used to derive management data encryption keys in conjunction with MKEK.	256 bits	Generated during MDEK derivation using the module's hardware random number generator and an approved DRBG (cert #188).	Not stored.	Not zeroised directly. The memory that holds this CSP is erased upon the tamper response/restart process.
Entropy Input String	Entropy input into the approved DRBG during instantiation	Entropy (256 bits)	Generated via internal hardware RBG	Not stored.	Not zeroised directly. The memory that holds this CSP is erased upon the tamper response/restart process.
Seed	Used by the approved DRBG	Seed (888 bits)	Generated during the instantiation and reseed functions of the DRBG	Not stored.	Not zeroised directly. The memory that holds this CSP is erased upon the tamper response/restart process.
C Value	Internal state value of the approved DRBG	C Value (888 bits)	Generated as part of the internal state of the DRBG.	Not stored.	Not zeroised directly. The memory that holds this CSP is erased upon the tamper response/restart process.
V Value	Internal state value of the approved DRBG	V Value (888 bits)	Generated as part of the internal state of the DRBG.	Not stored.	Not zeroised directly. The memory that holds this CSP is erased upon the tamper response/restart process.
Thales e-Security Firmware Upgrade Public Key	A public key embedded within the firmware which is used to verify the integrity of the firmware during firmware upgrade.	ECDSA (384 bits)	Generated externally and embedded within the firmware.	Embedded in the firmware – Compact Flash.	Not zeroised.

3.3 Zeroisation

The Crypto Officer can zeroise keys through the Element Manager application. As indicated in the table above, the Crypto Officer has the choice to directly delete keys, establish a new link with another peer module or force the module to generate new keys. Keys that are not zeroised are encrypted by the master key. The module zeroises the master key when the tamper response and zeroisation circuitry responds to an intrusion of the enclosure which renders all other keys indecipherable.

3.4 Other Security-Relevant Information

FIPS Approved Mode of Operation

The Datacryptor® SONET/SDH OC-3/12/48/192C only operates in an Approved mode and does not support any unapproved modes of operation.

1. **FIPS 140-2 Approved and Certified**
   - AES #2014 (AES-256, PowerPC Core 405)
   - AES #2030 (CMAC using AES-256, Generation only)
   - AES #2061 (AES-256, Xilinx XC2VP30 FPGA)
   - AES #2063 (AES-256, Xilinx XC2VP50 FPGA)
   - ECDSA #289 (Application)
   - ECDSA #304 (Bootstrap)
   - Key Agreement Scheme #34 (ECDH, key agreement; key establishment methodology provides 192 bits of encryption strength)
   - NIST SP800-90 DRBG #188
   - NIST SP800-108 KDF #1 (Counter Mode)
   - SHS #1764 (SHA-384, Application)
   - SHS #1808 (SHA-384, Bootstrap)
2. **Non-Approved Allowed**
   - Hardware RBG for generating entropy for approved and certified DRBG

Datacryptor® SONET/SDH OC-3/12/48/192C FPGA Details

This Security Policy defines the Datacryptor® SONET/SDH OC-3/12/48/192C cryptographic module for two hardware versions which utilize different FPGAs as described below:

- 1600X435, Rev. 02 (low speed module) utilizes a Xilinx VirtexII-Pro XC2VP30 FPGA.
- 1600X427, Rev. 02 (high speed module) utilizes two Xilinx VirtexII-Pro XC2VP50 FPGAs.

4. PHYSICAL SECURITY POLICY

The Datacryptor® SONET/SDH OC-3/12/48/192C is a multiple-chip standalone cryptographic module consisting of production-grade components to meet FIPS 140-2 Level 3.

The Datacryptor® SONET/SDH OC-3/12/48/192C is protected by a strong metal production-grade enclosure that is opaque within the visible spectrum with tamper evident labels and tamper response mechanisms. Attempts to access the module without removing the cover will cause visible physical damage to the module and/or tamper evident labels.

The module’s ventilation holes on the sides and back on the enclosure are fitted with baffles to prevent physical probing of the enclosure.

The module has a removable top cover which is protected by tamper response circuitry, which zeroises all plaintext CSPs. Access to the internal components of the module requires that these covers are removed.

The module's cryptographic boundary (FIPS 140-2 [1], section 2.1) is the physical extent of its external casing but excludes the field replaceable dual redundant power supply.

4.1 Inspection/Testing of Physical Security Mechanisms

The following guidelines should be considered when producing a Security Policy for the network in which the module is deployed.

The Datacryptor® SONET/SDH OC-3/12/48/192C should be periodically checked for evidence of tampering, in particular damage to the tamper evident labels (highlighted in solid red for opaque silver labels and outline red for clear labels) as these are part of the security of the unit. In addition the audit logs should be checked for activation of the tamper response mechanism.

The frequency of a physical inspection depends on the information being protected and the environment in which the unit is located. At a minimum it would be expected that a physical inspection would be made at least monthly and audit logs daily.

Figure 4-1 1600X435, Rev. 02 Front

Figure 4-2 1600X435, Rev. 02 Rear

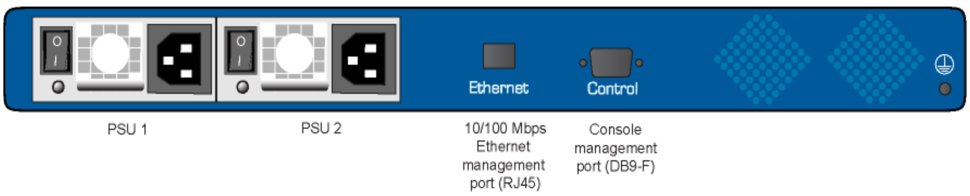


Figure 4-3 1600X427, Rev. 02 Front

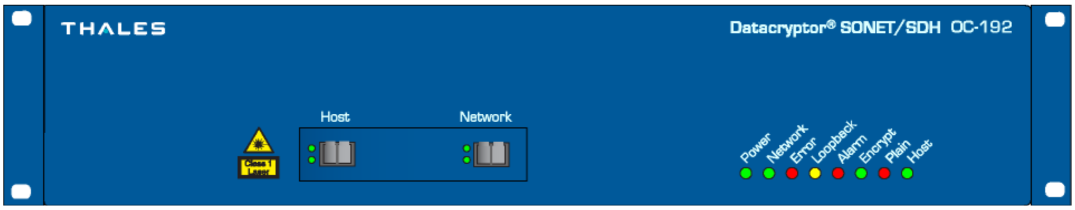


Figure 4-4 1600X427, Rev. 02 Rear

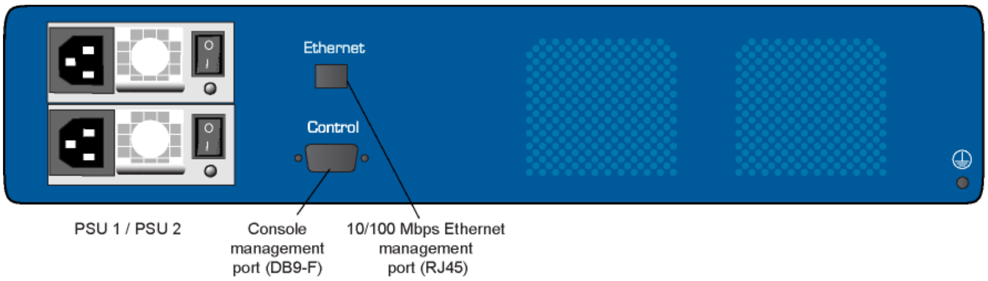


Figure 4-5 1600x435, Rev. 02 Top

Figure 4-6 1600x427, Rev. 02 Top

5. MITIGATION OF OTHER ATTACKS POLICY

None.

ACRONYMS AND ABBREVIATIONS

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CA	Certification Authority
DEK	Data Encryption Key
DRBG	Deterministic Random Bit Generator
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
EDC	Error Detection Code
FIPS	Federal Information Processing Standards
ITU	International Telecommunications Union
KAT	Know Answer Test
KEK	Key Encryption Key
LAN	Local Area Network
NIST	National Institute of Standards and Technology
PPP	Point-to-Point
PRNG	Pseudo Random Number Generator
PSU	Power Supply Unit
RIP	Routing Information Protocol
RBG	Random Bit Generator
SDH	Synchronous Digital Hierarchy
SFP	Small Form Factor Pluggable
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical NETwork
XFP	10 Gigabit Small Form Factor Pluggable

REFERENCES

1. FIPS 140-2 Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication, 25th May 2001. Including Change Notices 2,3,4: 12/03/2002

   Available from the NIST web site: http://www.nist.gov/cmvp

2. NIST SP800-90 Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology Special Publication, March 2007.

   Available from the NIST web site: http://www.nist.gov/cmvp

3. Datacryptor® SONET/SDH OC-3/12/48/192C User Manual, 1270A427-013, June 2012.

   Available from Thales e-Security.

-- END OF DOCUMENT --