THALES e-SECURITY

Datacryptor® 100M Ethernet

FIPS 140-2 Level 3 Security Policy

Firmware Version v4.2

Hardware Version 1600X439

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://iss.thalesgroup.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 of protecting wide-area network communications for governments, financial institutions and information-critical industries worldwide.

This document is the Security Policy[1] for the Thales e-Security Datacryptor® 100M Ethernet, conforming to the FIPS140-2 Security Policy Requirements [1].

Further information on the Datacryptor® family and the functionality provided by the Datacryptor® 100M Ethernet is available from the Thales web site: http://iss.thalesgroup.com

Overview

The Datacryptor® 100M Ethernet is a multi-chip (Xilinx Virtex 4 XC4FX40 FPGA with two embedded PPC 405 processor cores) standalone cryptographic module which facilitates secure data transmission across Ethernet networks at 100Mb/s.

Operating at OSI Layer 2, the Data Link Layer of the protocol stack the Datacryptor® 100M Ethernet is targeted at high speed/high data throughput applications between telecommunication facilities introducing virtually no overhead or latency to the network. Unlike Layer 3 IP security devices (IPSEC) the Datacryptor® 100M Ethernet is independent of network configurations resulting in a solution that is simple and inexpensive to manage.

As a solution for high speed/high-bandwidth data transport over LANs and WANs, a layer 2 device enable customers to take advantage of the most cost effective transport services available while ensuring the confidentiality of the information carried through these connections.

The Datacryptor® 100M Ethernet uses the strongest commercially cryptography (AES 256-bit key). It is designed to easily fit into a variety of network configurations supporting multiple modes of operation, point-to-point and switched networks, and bulk and tunnel modes with Virtual LAN (VLAN) traffic.

The Datacryptor® 100M Ethernet is built on a 19 inch rack-mountable tamper-proof metal enclosure with internal AC and DC power options. With the exception of the mains power connection, all interfaces are located in the front panel for easy access. In addition to RJ-45 Host and Network interfaces, dual serial and Ethernet management connections are provided along with Light Emitting Diodes (LEDs) status indicators.

Figure 1-1 shows a typical Datacryptor® 100M Ethernet configuration where 2 LANs are securely linked across a public domain Ethernet network.

[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.

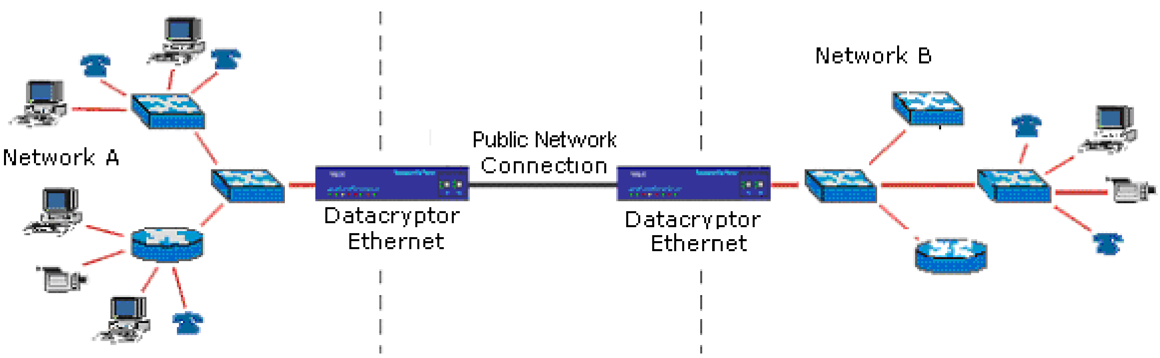
Modes of Operation

The Datacryptor® 100M Ethernet 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 Encrypt LED being flashing green.
- 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 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 Plain LED being solid red. 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 Encrypt LED being solid green.

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 either the Front Panel LEDs or the Secure Remote Management (Element Manager PC) facility. Refer to the User Manual [3] for further details.

Figure 1-1 Datacryptor® Ethernet Crypto Module Example Network Configuration



Physical Ports

[2] This is the bypass mode.

The Datacryptor® 100M Ethernet use 100BASE-T ports for user traffic and 10/100BASE-T ports for management traffic.

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 send and receiving encrypted user data and inter-module key exchange data.
Host	Connects to the private network for send and receiving plaintext user data.
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.
Power	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

User Data Security

The communications channel between two Datacryptor® 100M Ethernets is assumed to be vulnerable and therefore the Datacryptor® 100M Ethernet encrypts the entire user data stream[3].

The Datacryptor® 100M Ethernet uses public key cryptography for authentication and key agreement[4] and symmetric key cryptographic for data confidentiality. The authentication mechanism employs signed X.509 v3.0 certificates using the Digital Signature Algorithm (DSA) for signature verification. The Diffie-Hellman 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 a seed key to a FIPS 186-2 Appendix 3.1 [2] Approved pseudo random number generator.

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

Algorithm Support

The Datacryptor® 100M Ethernet contains the following algorithms:

- AES-256 for data encryption
- DSA for signature verification
- SHA-1 hashing algorithm
- Diffie-Hellman for key agreement

Physical Security

The multi-chip standalone embodiment of the circuitry within the Datacryptor® 100M Ethernet 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 zeroized.

The Datacryptor® 100M Ethernet's cryptographic boundary (FIPS 140-2 [1], section 2.1) is the physical extent of its enclosure.

Secure Remote Management

The Datacryptor® 100M Ethernet may be remotely and securely managed using the Element Manager.

The Datacryptor® 100M Ethernet can also be managed (for status only) using an SNMP v3.0 management application. Only one management session is permitted at a time with a Datacryptor® 100M Ethernet.

[3] Providing the modules are configured to operate in Encrypt mode.

[4] This key agreement method provides 80-bits of encryption strength.

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® 100M Ethernet and can be viewed or printed.

If the Datacryptor® 100M Ethernet 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 pseudo-random number generator. In addition the integrity of all firmware is checked.

Table 1-3 Power-Up Tests

Function Checked	Description
CA Algorithm (DSA)	KAT Test
KEK Algorithm (AES-256)	KAT Test
DEK Algorithm (AES-256)	KAT Test
SHA-1	KAT Test
SHA-1 RNG	KAT Test
Firmware Integrity	16 bit Error Detection Code (EDC) Checksum

- **Conditional Tests**
  - The output of both the hardware random number generator and the pseudo-random number generator are checked when ever 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 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 DSA allowing the module to verify the image so preventing unauthorized firmware upgrades. The firmware upgrade is currently a factory only service. After loading firmware onto this module it may 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.

Table 1-4 Conditional Tests

Function Checked	Description
Hardware RNG	CRNG
SHA-1 RNG	CRNG
Bypass	Bypass Test
Firmware Upgrade Authentication	Verify (DSA)

2. IDENTIFICATION AND AUTHENTICATION POLICY

The two roles associated with the Datacryptor® 100M Ethernet are:

Crypto-Officer Commissioning and configuration of the Datacryptor® 100M Ethernet.

User This role occurs when two Datacryptor® 100M Ethernets are communicating with each other.

The Datacryptor® 100M Ethernet does not support multiple concurrent roles.

2.1 Crypto-Officer Role

The Datacryptor® 100M Ethernet 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® 100M Ethernet.

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 Diffie Hellman parameters (base and modulus) to allow the Datacryptor® 100M Ethernet to generate a corresponding Diffie Hellman key set. This information is digital 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, 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® 100M Ethernet. Each User Certificate gives a Datacryptor® 100M Ethernet an identity.

Identity-based authentication is implemented between two communicating Datacryptor® 100M Ethernets. 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® 100M Ethernets.

2.3 Authentication

The types and strengths of authentication for each Role identified for the Datacryptor® 100M Ethernet 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 (DSA) 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® 100M Ethernet uses DSA, which is a FIPS Approved algorithm. Therefore the probability of successfully guessing the private key (160 bits), and hence correctly signing an X.509 certificate, is significantly less than one in 1,000,000 (2^{160}). Multiple attempts to use the authentication mechanism during a one-minute period do not constitute a threat for secure operation of the Datacryptor® 100M Ethernet. This is because each attempt requires the Datacryptor® 100M Ethernet 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® 100M Ethernet 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 (160 bits) of the private key space used by the FIPS Approved signature algorithm (DSA) loaded in the Datacryptor® 100M Ethernet 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^{160} / 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® 100M Ethernet. All services require authentication to the module.

For further details of each operation refer to the Datacryptor® 100M Ethernet 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 Ethernet mode (bulk, tunneling), laser mode and interface mode	Commands and parameters	Command response	None

Service	Description	Input	Output	Access
Encryption	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
Expert	Display/edit Cipher Text Stealing mode[5], enabled or disabled.	Commands and parameters	Command response	
Tunneling	Display own MAC address, display/edit peer MAC address, filter rules, VLAN identification and fragmentation size.	Commands and parameters	Command response.	
Environment	Display fan speed, and module temperature.	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
Show Status	View status of the module.	None Commands and parameters	Front Panel LEDs Status Indicators Status information over Element Manager or SNMP Traps	None
Operator Callable Self-Test	Module performs self-test	Reboot Module	Front Panel LEDs Status Indicators	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	User traffic (plain)	User traffic (encrypted)	DEK – read

[5] Ciphertext Stealing (CTS) is a CBC method of manipulating the data in the last two blocks of messages that are not exactly divisible into 128 bit blocks such that the last incomplete block can be sent securely without increasing the overall message size.

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

3.2 Cryptographic Keys, CSPs and Access Rights

The cryptographic keys and CSPs stored in the Datacryptor® 100M Ethernet module are listed in *Table 3-3*.

All private and secret keys (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 3-3 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)	At start-up if not present using the module's hardware random number generator and an approved RNG (cert# 588).	FRAM (plaintext)	On tamper detect or by user.
CA Public Key	The public key of the CA key pair use to verify subsequent key material loaded into the module.	DSA (1024 bits)	Generated external and loaded as part of the commissioning process.	Non-volatile memory – Compact Flash (encrypted)	When the key is deleted or replace by a subsequent key.
Own Module Certificate/Diffie-Hellman Static Key Pair	An X.509 certificate containing the module name, Diffie-Hellman static public key (the static private key is stored separately) and associated parameters.	Diffie-Hellman (1024 bits)	The Diffie-Hellman static key pair is generated locally by the module, using the module's hardware random number generator and an approved RNG (cert#588) from the parameters supplied during the commissioning process. The module name and 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) Diffie-Hellman static private key – Non-volatile memory – FRAM (encrypted)	When the certificate is deleted or replaced by a subsequent certificate. The Diffie-Hellman static private key may deleted by a user.
Diffie-Hellman Ephemeral Key	The Diffie-Hellman ephemeral key pair.	Diffie-Hellman	The Diffie-Hellman ephemeral key pair is	Volatile memory -	Zeroised when a new link is

Keys/CSPs	Description	Key/CSP Type and Size	Generated/ Established	Stored	Zeroised
Pair		(1024 bits)	generated locally by the module, using the module's hardware random number generator and an approved RNG (cert#588) from the parameters supplied during the commissioning process. This key pair is used in conjunction with the static key pair to establish the KEK.	SRAM (encrypted)	established.
Peer Module Certificate	Received during link establishment between two modules to allow authentication of the peer module using signature verification (DSA).	Diffie-Hellman (1024 bits)	Generated by peer in the same manner as Own Module Certificate.	Non-Volatile memory – Compact Flash (encrypted)	Zeroised when a new link is established.
Key Encryption Key (KEK)	Key used to derive data encryption keys in conjunction with DEKID	AES (256 bits)	Established during link establishment with Diffie-Hellman using the static and ephemeral key pairs.	Volatile memory – BRAM (encrypted)	Zeroised when a new link is established or when a new KEK is generated at a user defined time interval.
Data Encryption Key Derivation Data (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 RNG (cert# 588).	Not stored.	N/A
Data Encryption Keys (DEKs)	Two 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 XOR operations.	Volatile memory – BRAM (encrypted)	Zeroised when a new link is established or when a new DEK is generated at a user defined time interval.
Seed Key	Used by the Approved RNG	RNG Seed Key (256 bits)	Generated via internal hardware RNG	Not stored.	Zeroised when a subsequent seed key is generated and the CRNG comparison is successful.

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® 100M Ethernet only operates in an Approved mode and does not support any unapproved modes of operation.

1. **FIPS 140-2 Approved and Certified**
   - SHA-1 (FIPS Certificate #985)
   - DSA (FIPS Certificate #349)
   - FIPS 186-2 (FIPS Certificate #588).
   - AES-256 (FIPS Certificate #1033 and 1078)
2. **Non-Approved Allowed**
   - Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength)
   - Hardware RNG for generating seed key for Approved RNG

4. PHYSICAL SECURITY POLICY

The Datacryptor® 100M Ethernet is a multiple-chip standalone cryptographic module consisting of production-grade components to meet FIPS 140-2 Level 3.

The Datacryptor® 100M Ethernet is protected by a strong metal production-grade enclosure that is opaque within the visible spectrum with tamper evident labels (highlighted in red) 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 zeroizes 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.

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® 100M Ethernet should be periodically checked for evidence of tampering, in particular damage to the tamper evident 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 1600X439 Front

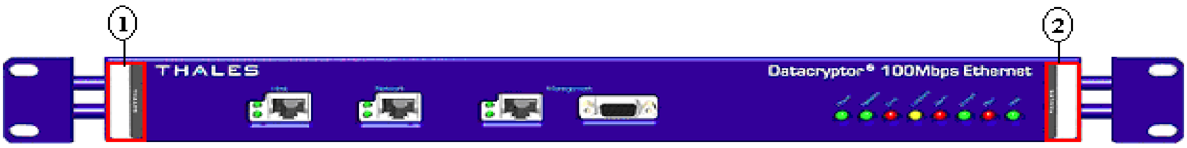


Figure 4-2 1600X439 AC and DC Rear

Figure 4-3 1600x439 Top

Figure 4-4 1600x439 Bottom

The tamper evident labels shall only be applied at the Thales facility. Tamper evident labels are not available for order or replacement from Thales.

Two undamaged tamper evident labels must be visible for the module to be operated in a FIPs approved mode of operation. They shall be in the positions shown (see Figure 4-1), one on the left side of the front panel (position 1) and one on the right side of the front panel (position 2)

5. MITIGATION OF OTHER ATTACKS POLICY

None.

ACRONYMS AND ABBREVIATIONS

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CA	Certification Authority
CTS	Cipher Text Stealing
DEK	Data Encryption Key
DSA	Digital Signature Algorithm
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
MAC	Media Access Control
NIST	National Institute of Standards and Technology
PPP	Point-to-Point
PRNG	Pseudo Random Number Generator
PSU	Power Supply Unit
RIP	Routing Information Protocol
RNG	Random Number Generator
SDH	Synchronous Digital Hierarchy
SHA-1	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
VLAN	Virtual LAN

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://csrc.nist.gov/cryptval/

2. FIPS 186-2 Digital Signature Standard, Federal Information Processing Standards Publication, 27th January 2000. Including Change Notice 1: 5th October 2001.

   Available from the NIST web site: http://csrc.nist.gov/cryptval/

3. Datacryptor® 100M Ethernet User Manual, 1270A427, Issue 8 June 2008.

   Available from Thales e-Security.