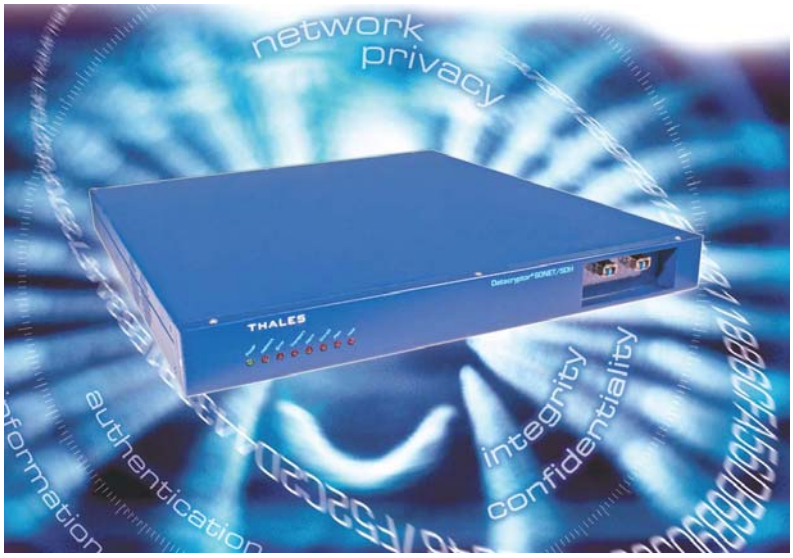
THALES e-SECURITY



Datacryptor® Gig Ethernet v1.0 and v1.1

FIPS 140-2 Level 2

Firmware Version v1.0 and v1.1

Hardware Version 1600X409 v1.0

Security Policy

Draft 2B, 3rd August 2009

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

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's 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® Gig Ethernet, conforming to the FIPS140-2 Security Policy Requirements [1].

Further information on the Datacryptor® family and the functionality provided by the Datacryptor® Gig Ethernet is available from the Thales web site: http://www.thalesesec.com

Overview

The Datacryptor® Gig Ethernet is a multi-chip standalone cryptographic module which facilitates secure data transmission across gigabit ethernet networks using 1000baseX (802.3z) with supported media types of 1000BaseSX (short-haul fiber), 1000BaseLX (long-haul fiber) or 1000BaseCX (single twisted-pair copper).

Figure 1-1 shows a typical Datacryptor® Gig Ethernet configuration where 2 LANs are securely linked across a point to point link. The units may also be configured to operate across a public domain LAN or virtual LAN environment.

Modes of Operation and Physical Ports

The Datacryptor® Gig Ethernet only supports a single FIPS Approved mode but can be configured to operate in three different sub-modes by the Crypto-Officer:

- **Standby** — The module transmits/receives no data via either its Host or Network interfaces on that channel.
- **Plain Text[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.
- **Encrypt** — 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

[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 capability.

decrypted data is transmitted through the Host interface.

The physical ports are listed below:

- NET Line Interface – Plain Text I/O
- HOST Line Interface – Cipher Text I/O
- Serial Management – RS-232 Control and Status
- Ethernet Management – 10/100 BaseT Control and Status
- Power – AC or DC input

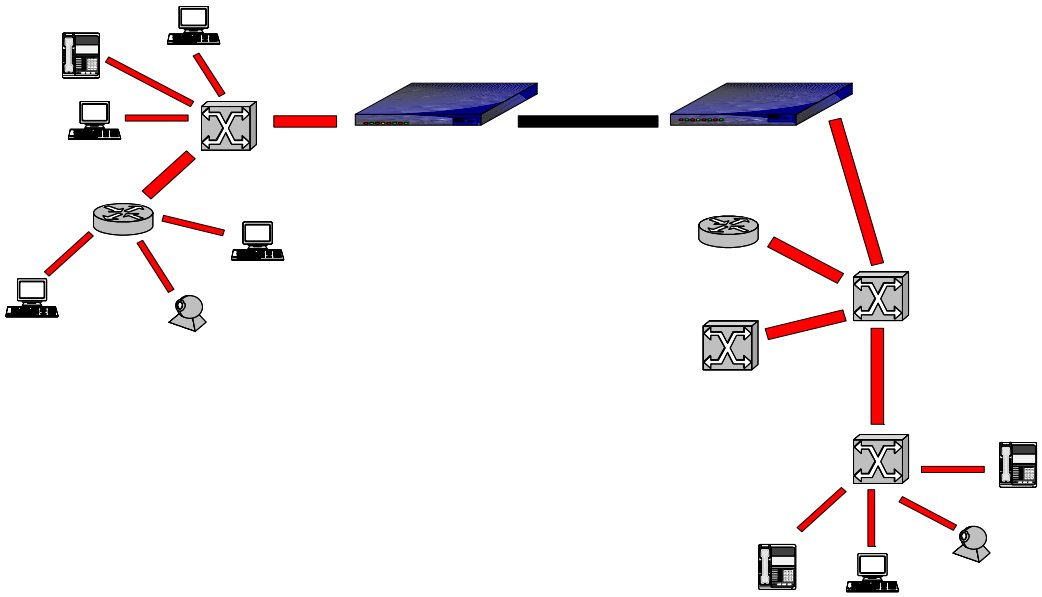


Figure 1-1 Datacryptor® Gig Ethernet Example Network Configuration

Public Key Cryptography

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

The Datacryptor® Gig Ethernet uses public key cryptography for authentication and key agreement. The authentication mechanism employs signed X.509 certificates using the Digital Signature Algorithm (DSA) for signature verification. The Diffie-Hellman protocol is used for key agreement between modules. This key agreement method provides 80-bits of encryption strength.

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

Random Number Generation

Data Encryption Keys (DEKs), used for encrypting and decrypting data traffic, are generated using a random number generator within the Datacryptor® Gig Ethernet. This consists of a hardware random number source which provides a seed to a FIPS 186-2 Appendix 3.1 [2] Approved pseudo random number generator.

For maximum security and flexibility DEKs can be automatically updated at user defined intervals.

Algorithm Support

The Datacryptor® SONET/SDH contains the following algorithms:

- AES-256 for data encryption
- DSA for signature verification
- SHA-1 hashing algorithm
- Diffie-Hellman (ANSI X9.42 Hybrid 1) for key agreement

Physical Security

The multi-chip standalone embodiment of the circuitry within the Datacryptor® Gig Ethernet is contained within a metal production-grade enclosure that is opaque within the visible spectrum to meet FIPS 140-2 Level 2.

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

Secure Remote Management

The Datacryptor® Gig Ethernet may be remotely managed using the Element Manager. This connection is secured using the same key agreement and data encryptions algorithm so allowing authentication of the link establishment and confidentiality of management traffic.

The Datacryptor® Gig Ethernet can also be managed (for monitoring only) using an SNMP management application. Only one management session is permitted at a time with a Datacryptor® Gig Ethernet.

Diagnostics

A variety of diagnostics are available to maintain trouble-free operation. Log files are maintained in the Datacryptor® Gig Ethernet and can be viewed or printed.

If the Datacryptor® Gig 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 know answer tests (KAT) are performed automatically without operator intervention on all cryptographic algorithms and the pseudo-random number generator. In addition the integrity of all firmware is checked. The power-up tests are run automatically without operator intervention.

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	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.
  - 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 authenticate the image so preventing unauthorized firmware upgrades. The firmware upgrade is currently a factory only service. After loading firmware onto this module it will no longer be a FIPS 140-2 validated module. This feature is used as an upgrade path for future FIPS 140-2 approved modules.

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

2. IDENTIFICATION AND AUTHENTICATION POLICY

The three roles associated with the Datacryptor® Gig Ethernet are:

Crypto-Officer	Commissioning and configuration of the Datacryptor® Gig Ethernet.
User	This role occurs when two Datacryptor® Gig Ethernets are communicating with each other.
Maintenance	Performing maintenance actions for Datacryptor® Gig Ethernet module.

The Datacryptor® Gig Ethernet does not support multiple concurrent roles.

2.1 Crypto-Officer Role

The Datacryptor® Gig Ethernet can be managed by the Crypto-Officer using either of the following two methods:

- **Element Manager** - This PC-based software application is used by the Crypto-Officer to commission and administer the module.
- **SNMP Management Station** - This is limited to requesting and obtaining status information from the Datacryptor® Gig Ethernet.

The Crypto-Officer utilizes the Element Manager to commission and configure the module via the dedicated ethernet 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® Gig 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 X.509 certificate. The key material is used by the Crypto-Officer to 'commission' the Element Manager PC software application so allowing the secure connection to the module to be created.

To access the key-material set the Crypto-Officer must login to the Element Manager[4] by presenting the key-material set and the Crypto-Officer's own password of at least 8 ASCII displayable characters. This allows the Element Manager to

[4] The validation of the password is performed by the Element Manager which is not within the modules cryptographic boundary. This is an additional security measure and not part of the FIPS 140-2 authentication requirements.

authenticate 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® Gig Ethernet. Each User Certificate gives a Datacryptor® Gig Ethernet an identity.

Identity-based authentication is implemented between two communicating Datacryptor® Gig Ethernet. The modules are then operating in the User role.

This identity can be authenticated by another module which authenticates 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 authentication cannot be undertaken. Therefore no communications channel can be established between the two Datacryptor® Gig Ethernets.

2.3 Maintenance Role

The maintenance role is assumed by the Crypto-Officer. The services defined for this role do not utilize FIPS approved cryptographic algorithms.

The Crypto-Officer must zeroize the unit of all private cryptographic keys and CSPs before any maintenance service can be performed, using the Element Manager. The procedure for performing this service is detailed in sec. 4.2.1

2.4 Authentication

The types and strengths of authentication for each Role identified for the Datacryptor® Gig 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
Maintenance	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® Gig Ethernet uses DSA, which is a FIPS Approved algorithm. Therefore the probability of successfully guessing the private key, and hence correctly signing an X.509 certificate, is significantly less than one in 1,000,000. Multiple attempts to use the authentication mechanism during a one-minute period do not constitute a threat for secure operation of the Datacryptor® Gig Ethernet. This is because each attempt requires the Datacryptor® Gig 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® Gig 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 of the private key space used by the FIPS Approved signature algorithm (DSA) loaded in the Datacryptor® Gig 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. There is no feedback of authentication data to the Crypto-Officer or User that might serve to weaken the authentication mechanism.
Crypto-Officer Password[5]	The removable media key-material set used by an individual Crypto-Officer to establish a secure connection to a defined group of modules[6], is protected by their own password which is a minimum of 8 ASCII displayable characters, and hence correctly entering the correct password using a random password is significantly more than one in 1,000,000. In a one minute period it is only possible, on average, to attempt to enter 10 random passwords and hence the probability of correctly guessing the password in a one minute period is significantly more than one in 100,000. When entering the password it is masked using a '*' character and after three failed attempts the Element Manager software application will shut down and will have to be restarted before any additional login attempts may be performed.

[5] The password is not passed to the module for validation.

[6] A Crypto-Officer may only manage those modules which contain the same CA public key as held on the key-material set.

3. ACCESS CONTROL POLICY

3.1 Roles and Services

Table 3-1 lists the authorized services available for each role within the Datacryptor® Gig Ethernet. For further details of each operation refer to the Datacryptor® Gig Ethernet User Guide [3].

Table 3-1 Services Authorized for Roles

Role	Authorized Services
Crypto-Officer	Add Module Connection
Crypto-Officer	Delete Module Connection
Crypto-Officer	Restore Module Connection
Crypto-Officer	Configure Module Connection (a module's IP address, connection method and name)
Crypto-Officer	Login (to Datacryptor® Gig Ethernet)
Crypto-Officer	Logout
Crypto-Officer	Add CA
Crypto-Officer	Delete CA
Crypto-Officer	Add Certificate
Crypto-Officer	Delete Certificate
Crypto-Officer	Change Module Name
Crypto-Officer	Delete KEK
Crypto-Officer	Configure Channel for Encrypt Mode
Crypto-Officer	Configure Channel for Plain Text Mode
Crypto-Officer	View Audit Logs (show status service)
Crypto-Officer	Clear Audit Logs
Crypto-Officer	Modify KEK Change Interval
Crypto-Officer	Modify DEK Change Interval
Crypto-Officer	Change KEK With DEK
Crypto-Officer	Zeroize Unit
Crypto-Officer	Self-Test
Maintenance	Replace power supply
User	KEK and DEK Exchange
User	Channel Encryption

3.2 Cryptographic Keys, CSPs and Access Rights

The cryptographic keys and CSPs stored in the Datacryptor® Gig Ethernet module are listed in *Table 3-2*.

Table 3-2 Cryptographic Keys and CSPs

#	Cryptographic Item	Description
1	CA Public key component	The public key of the CA key pair is stored in the Datacryptor® Gig Ethernet and is never exported. CA private keys are not directly used by the module, and are never loaded into the module.
2	Module's own X.509 Certificates and key pair	A Datacryptor® Gig Ethernet generates its own X.509 User Certificates and corresponding Diffie-Hellman key pairs using parameters supplied by the Element Manager. The Diffie-Hellman private key and public key are generated within the module. The private key is never exported from the module. The public key is exported to the Element Manager for signing by the issuing CA private key. The signed public key is then loaded into the module and the signature verified.
3	Peer Module X.509 Certificates	During the first stages of link establishment between two modules they exchange certificates and authenticate each other using signature verification. Once received, these peer Certificates are stored within the module, which reduces overheads for any subsequent link establishment.
4	Key Encryption Keys (KEKs) and Data Encryption Keys (DEKs)	The Datacryptor® Gig Ethernets generate a Key Encryption Key (KEK) and a Data Encryption Key (DEK) in order to establish a secure link between two modules. The KEKs are derived and exchanged between modules using Diffie-Hellman key agreement. The DEKs are derived, within the module, by combining self generated data with encrypted data received from the peer. This combined data is then encrypted. The self generated data is from the FIPS approved Pseudo-Random Number Generator (PRNG). The encryption uses the AES algorithm with the KEK as the key.
5	Audit Logs	The Crypto-Officer has access to the Datacryptor® Gig Ethernet Audit Logs via the Element Manager. Access can be obtained only after the Crypto-Officer has been authenticated by the Datacryptor® Gig Ethernet (via the *Login* service).

Table 3-3 identifies the services (listed in *Table 3-2*) and access, if any, to the cryptographic keys and CSPs within the Datacryptor® Gig Ethernet. The type of access is also shown.

Table 3-3 Access Rights within Services

Service	**Cryptographic Item # (see *Table 3-2*)**	**Type of Access**
Configure Module Connection	None	N/A
Login	3	Write
Add CA	1	Write
Delete CA	1	Write
Add Certificate	2	Write
Delete Certificate	2	Write
Change Module Name	2, 4	Write
Delete KEK	4	Write
View Audit Logs	5	Read
Clear Audit Logs	5	Write
Change KEK With DEK	None	N/A
Zeroize Unit	2, 4	Write
KEK And DEK Exchange	None	N/A
Channel Encryption	2, 3, 4	Read (2, 3) Write (4)

3.3 Other Security-Relevant Information

FIPS Approved Mode of Operation

The Datacryptor® Gig Ethernet only operates in an approved mode and does not support any unapproved modes of operation.

1. **FIPS 140-2 Approved security methods**

   The following methods are used:

   - SHA-1 (FIPS Certificate #517)
   - DSA (FIPS Certificate #184)
   - Datacryptor® Gig Ethernet pseudo random number generator which conforms to FIPS 186-2 Appendix 3.1 [2] (FIPS Certificate #239).

   The following method is only required when operating in encrypt mode:

   - AES-256 (FIPS Certificate #454)

2. **Diffie-Hellman key distribution is performed each time the Data Encryption Key (DEK) changes**

   The Crypto-Officer can configure the Datacryptor® Gig Ethernet to force an update to the KEK each time the DEK is changed via the *Change KEK with DEK* service.

4. PHYSICAL SECURITY POLICY

The Datacryptor® Gig Ethernet is a tamper-evident multiple-chip standalone cryptographic module consisting of production-grade components intended to meet FIPS 140-2 Level 2. The Datacryptor® Gig Ethernet is protected by a metal production-grade enclosure that is opaque within the visible spectrum with tamper evident labels.

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 Datacryptor® Gig 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.

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 an inspection would be made at least monthly.

Figure 4-1 Tamper Evident Labels below shows the position of the tamper evident labels.

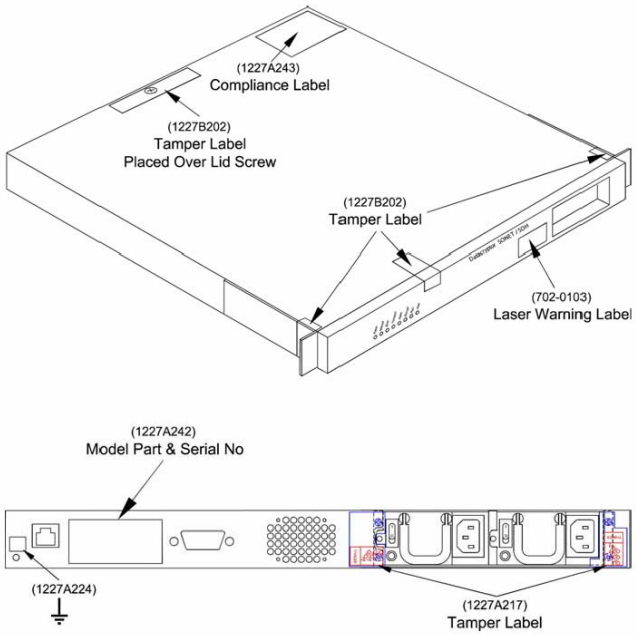


Figure 4-1 Tamper Evident Labels

4.2 Maintenance Interface

The module has a single tamper evident maintenance interface at the rear of the chassis to allow a failed power supply[7] to be replaced in the event of a failure.

4.2.1 Swapping Out Power Supply

In the event that a power supply is required to be swapped out this should only be performed once the Crypto Officer has zeroized the unit of all private cryptographic keys and CSPs. The Maintenance role should then remove the appropriate power supply's tamper evident label and fixing plate. This allows the defective power supply to be removed and replaced. The Maintenance role should then remove any residue left on the tamper evident fixing plate and reattach the fixing plate to the unit. A new tamper evident label can then be applied to the fixing plate. Figure 4-1 Tamper Evident Labels shows the correct position of the tamper evident labels and fixing plates.

It should be noted that the module supports two types of power supply units, AC and DC.

4.2.2 Replacement of Internal Battery

The internal battery is not considered a customer replaceable item. If the internal battery is required to be replaced the module should be 'returned to factory'.

[7] Although the dual redundant power supplies are contained within the cryptographic boundary they are excluded from the security requirements.

5. MITIGATION OF OTHER ATTACKS POLICY

None.

GLOSSARY

Term	Definition
Link	A single point-to-point communications link between two Datacryptor® Gig Ethernets involving no protocol.
X.509	The most widely used "standard" (actually an ITU recommendation) for defining digital certificates.

ACRONYMS AND ABBREVIATIONS

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CA	Certification Authority
DEK	Data Encryption Key
DSA	Digital Signature Algorithm
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
PRNG	Pseudo Random Number Generator
RNG	Random Number Generator
SDH	Synchronous Digital Hierarchy
SHA-1	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical NETwork

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® Gig Ethernet User Manual, 1270A450-00C February 2006.

   Available from Thales e-Security.