THALES e-SECURITY

DC2K Security Module

FIPS 140-2 Level 3

Security Policy

7th December 2004

Thales e-Security Limited, Meadow View House, Long Crendon, Aylesbury, BUCKS HP18 9EQ United Kingdom
Tel. +44 (0) 1844 201800
Fax. +44 (0) 1844 208550
http://www.thales-esecurity.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 DC2K Security Module provides the entire security functionality for the Datacryptor® 2000 product. As such it represents Thales's next generation of network security devices. 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 for the Thales e-Security DC2K Security Module, hardware and software version 3.411, conforming to the FIPS140-2 Security Policy requirements [1].

Further information on the Datacryptor® 2000 and the functionality provided by the DC2K Security Module is available from the Thales web site: http://www.thales-esecurity.com

Figure 1-1 Datacryptor® 2000

Overview

The DC2K Security module is a multi-chip embedded cryptographic module which facilitates secure data transmission across the following net work protocols:

- Link
- Channelised
- Frame Relay
- X.25
- I P

The DC2K Security Module installed in a Datacryptor® 2000 is shown in *Figure 1-2*.

Figure 1-2 Datacryptor® 2000 Internal Layout

The DC2K Security Module is identified by its large rectangular black casing. The Module implements the Datacryptor® 2000's cryptographic functionality and secure cryptographic material storage. The DC2K Security Module is embedded in a hard epoxy resin and enclosed within a metal casing.

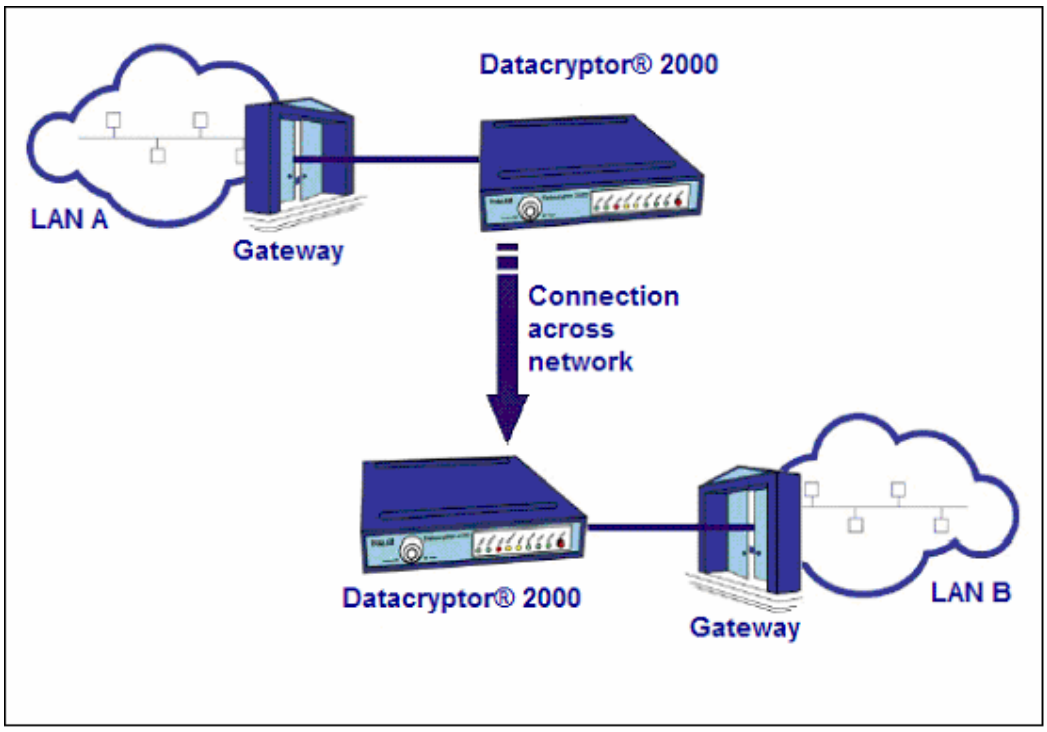

Figure 1-3 Datacryptor® 2000 Example LAN Configuration

Figure 1-3 shows a typical Datacryptor® 2000 configuration where 2 LANs are securely linked across a public domain IP network.

As well as securing point-to-point links, DC2K Security Modules can also secure multiple channel links, where each channel can be distinctly operated with its own individual mode of operation and unique data encryption keys.

Modes of Operation and Physical Ports

The DC2K Security Module can operate in three modes:

- Encrypt Mode — Data transmitted between two modules is encrypted.
- Plain Text Mode — Data transmitted between two modules is not encrypted.
- Standby Mode — No data is transmitted.

The physical connection for the DC2K Security Module is a 100 Pin connector that plugs into the Datacryptor® 2000's baseboard.

Public Key Cryptography

The communications channel between two Datacryptor® 2000s is assumed to be vulnerable and therefore the DC2K Security modules encrypt the entire data stream[1].

The DC2K Security Module uses public key cryptography for authentication and key distribution. The authentication mechanism employs signed X.509 certificates using the Digital Signature Algorithm (DSA) for signature verification. Diffie-Hellman key agreement protocol is used for key exchanges between modules.

[1] 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 DC2K Security Module. This consists of a hardware random number generator 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 DC2K Security Module supports a variety of data encryption algorithms including Triple DES (168 bit) and the Rijndael Advanced Encryption Standard (AES: 128, 192 and 256 bit).

Customers can load their own algorithm only if the algorithm has been correctly signed. The algorithm must be FIPS Approved and FIPS 140-2 tested for the module to operate in FIPS Approved mode.

Each DC2K Security Module is factory loaded with at least the following:

- Triple DES or AES for data encryption
- DSA for signature verification
- SHA-1 hashing algorithm
- Diffie-Hellman (ANSI X9.42 Hybrid 1) for key exchange

Physical Security

The multi-chip embedded embodiment of the circuitry within the DC2K Security Module is covered with a hard epoxy material that is opaque within the visible spectrum intended to meet FIPS 140-2 Level 3.

The module's cryptographic boundary (FIPS 140-2 [1], section 2.1) is the physical extent of its external casing and the internal surface of the baseboard covered by the casing. The module contains no removable doors or covers.

Further information concerning the physical security mechanisms of the DC2K Security Module can be found in section 5.1.

Secure Remote Management

The DC2K Security Module may be remotely and securely managed using the Element Manager.

The DC2K Security Module can also be managed (for monitoring only) using an SNMP management application. Only one management session is permitted at a time with a DC2K Security Module.

Diagnostics

A variety of diagnostics are available to maintain trouble-free operation. Log files are maintained in the DC2K Security Module and can be viewed or printed.

If the DC2K Security Module is faulty, as indicated by the failure of a self-test diagnostic, it will render itself inoperable until the fault is rectified.

2. IDENTIFICATION AND AUTHENTICATION POLICY

The two roles associated with the DC2K Security Module are:

Crypto-Officer Commissioning and configuration of the DC2K Security Module.

User This role occurs when two DC2K Security Modules are communicating with each other.

There is no Maintenance Role associated with the DC2K Security Module.

2.1 Crypto-Officer Role

The DC2K Security Module can be managed by the Crypto-Officer using the Element Manager. This PC-based software application enables a Crypto-Officer to commission and administer the module

The Crypto-Officer is authenticated to the module using identity-based authentication. A signed X.509 Certificate is submitted to the DC2K Security Module. The module then authenticates the Certificate's signature using the issuing CA Public key held within the module.

The Crypto-Officer can control all Certificate lifetimes.

2.2 User Role

The Crypto-Officer can download one or more signed X.509 User Certificates to the DC2K Security Module. Each User Certificate gives a DC2K Security Module an identity.

Identity-based authentication is implemented between two communicating DC2K Security Modules. The modules are then operating within 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 link can be established between the two DC2K Security Modules.

2.3 Authentication

The types and strengths of authentication for each Role identified for the DC2K Security Module 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

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 DC2K Security Module 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 DC2K Security Module. This is because each attempt requires the DC2K Security Module 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 DC2K Security Module 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 DC2K Security Module 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.

2.4 SNMP Management

As well as the Idenitification and Authentication functions described above the DC2K Security Module can be managed through an SNMP interface. This is limited to requesting and obtaining read-only status information from the DC2K Security Module. The operator is not required to assume an authorized role for the SNMP service as it does not modify, disclose or substitute cryptographic keys and CSPs, or otherwise affect the security of the module

3. ACCESS CONTROL POLICY

3.1 Roles and Services

Table 3-1 lists the authorised services available for each role within the DC2K Security Module. For further details of each operation refer to the Datacryptor® 2000 User Guide [3] at the section indicated in the table.

Table 3-1 Services Authorised for Roles

Role	Authorised Services	User Manual [3] Section #
Crypto-Officer	Add Module Connection	6-29
Crypto-Officer	Delete Module Connection	10-4
Crypto-Officer	Restore Module Connection	10-4
Crypto-Officer	Configure Module Connection (a module's IP address, connection method and name)	10-14
Crypto-Officer	Login (to DC2K Security Module)	8-3
Crypto-Officer	Logout	8-6
Crypto-Officer	Add CA	10-31
Crypto-Officer	Delete CA	10-33
Crypto-Officer	Add Certificate	10-32
Crypto-Officer	Delete Certificate	10-33
Crypto-Officer	Change Module Name	10-32
Crypto-Officer	Delete KEK	10-30
Crypto-Officer	Install Algorithms (data encryption algorithm and key exchange algorithm)	10-29
Crypto-Officer	View Audit Logs (show status service)	10-21
Crypto-Officer	Clear Audit Logs	10-23
Crypto-Officer	Enable Movement And Temperature Sensors	3-5, 10-45
Crypto-Officer	Modify KEK Change Interval	10-44
Crypto-Officer	Modify DEK Change Interval	10-44
Crypto-Officer	Change KEK With DEK	10-44
Crypto-Officer	Self-Test	Automatic[2]
User	KEK And DEK Exchange	Automatic [3]
User	Channel Encryption	Automatic [4]

[2] An automatic operation that tests for correct cryptographic function at power up and during operation .

[3] An automatic operation between two modules establishing a link

[4] An automatic operation between two modules sending data across a link

3.2 Cryptographic Keys, CSPs and Access Rights

The cryptographic keys and CSPs stored in the DC2K Security Module 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 DC2K Security Module and is never exported. CA Secret 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 DC2K Security Module generates its own X.509 User Certificates and corresponding Diffie-Hellman key pairs using parameters supplied by the Element Manager. The Secret key and Public key are generated within the module. The Secret key is never exported from the module. The Public key is exported to the Element Manager for signing by the issuing CA Secret key. The signed Public key is then loaded into the module and the signature verified. The Secret key is stored in the module in plaintext but is protected by the tamper detection circuitry of the module. This circuitry will delete the Secret key if tampering is detected.
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 DC2K Security Modules 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 generated within a module using a FIPS approved Pseudo-Random Number Generator (PRNG). The data encryption algorithm used with the DEKs is the encryption algorithm loaded within the module (only 1 encryption algorithm can be loaded at any one time). The standard algorithms are Triple DES and AES.

#	Cryptographic Item	Description
5	Audit Logs	The Crypto-Officer has access to the DC2K Security Module Audit Logs via the Element Manager. Access can be obtained only after the Crypto-Officer has been authenticated by the DC2K Security Module (via the *Login* service).

Table 3-3 identifies the services (listed in *Table 3-2*) which have access to the cryptographic keys and CSPs within the DC2K Security Module. The type of access is also shown.

Services which are not shown in *Table 3-3* have no access to the cryptographic keys or CSPs within the module.

Table 3-3 Access Rights within Services

Service	Cryptographic Item # (see *Table 3-2*)	Type of Access
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
Channel Encryption	4	Read

3.3 Other Security-Relevant Information

Algorithm Loading

A replacement data encryption and key exchange algorithm can be loaded into the DC2K Security Module using the *Load Algorithm* service.

The algorithms must be signed by the Secret key of a CA loaded in the module.

Any algorithm loaded into the module must be FIPS approved and FIPS 140-2 tested or the module will no longer be FIPS validated.

FIPS Approved Mode of Operation

The DC2K Security Module only has an Approved mode of operation. The following conditions must be satisfied to achieve the FIPS 140-2 Level 3 Approved mode.

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

   The following methods must be used:

   - Triple DES (FIPS Certificate #251) magazine DHDES3_V1_81 or
     AES (FIPS Certificate #151) magazine DHAES128_V1_19 or
     AES (FIPS Certificate #152) magazine DHAES192_V1_10 or
     AES (FIPS Certificate #153) magazine DHAES256_V1_10
   - SHA-1 (FIPS Certificate #230)
   - DSA (FIPS Certificate #104)
   - RNG (FIPS Certificate #17)

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

   The Crypto-Officer can configure the DC2K Security Module 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 DC2K Security Module is a tamper-resistant multiple-chip embedded cryptographic module consisting of production grade components intended to meet FIPS 140-2 Level 3.

The DC2K Security Module is potted with a hard epoxy resin that is opaque within the visible spectrum. The potted module is contained in a hard, solid copper shell. These components provide the module's tamper evidence. The components should be inspected for evidence of tamper.

The physical security mechanism described above uses passive techniques and therefore no testing of the mechanism is required.

5. MITIGATION OF OTHER ATTACKS POLICY

5.1 Movement, Temperature, Voltage and Intrusion Alarms

The following alarm mechanisms are employed by the module:

Movement	If an unauthorised attempt is made to move or physically tamper the module its Movement Alarm will be triggered.
Temperature	If the temperature sensor detects ambient temperature outside a predetermined range an alarm is triggered.
Voltage	If the power levels surge or are actively driven above the normal levels then an alarm is triggered.
Intrusion	An electrically conductive intrusion barrier covers the secure area within the module, which is potted in a hard opaque resin. Any intrusion into this area will trigger an alarm.

The triggering of an alarm will immediately erase all protected algorithms, certificates and keys that have been loaded into, or generated by, the DC2K Security Module irrespective of whether the module is powered or not. To return the module to service following an alarm it must be re-commissioned by the Crypto-Officer.

Further details concerning these alarms (which were not tested as part of the DC2K Security Module FIPS 140-2 Level 3 validation) are given below.

5.1.1 Movement Alarm

If an unauthorised attempt is made to move or physically tamper the module its Movement Alarm will be triggered.

The Movement Alarm can only be enabled or disabled by the Crypto-Officer.

5.1.2 Temperature Alarm

If the temperature sensor inside the module detects temperatures outside a predetermined range (regardless of whether the module is powered on or off) an alarm is triggered.

The Temperature Alarm can only be enabled or disabled by the Crypto-Officer.

5.1.3 Voltage Alarm

If the voltage sensor inside the module detects that the power levels surge or are actively driven above the normal levels then an alarm is triggered.

The Voltage Alarm is permanently enabled.

5.1.4 Intrusion Alarm

An electrically conductive intrusion barrier covers the secure area within the module, which is potted in a hard opaque resin. Any intrusion into this area will trigger an alarm.

If the Intrusion Alarm is triggered the module is likely to be permanently disabled, requiring return to Thales for resetting/repair.

5.2 Fault Induction Attacks

Fault induction attacks make use of fluctuations in external forces to cause processing errors within a module.

The module provides protection against certain types of fault induction attack. It contains a temperature sensor and a mechanism to detect abnormal voltage variations (see sections 5.1.2 and 5.1.3 above). The temperature sensor can only be enabled or disabled by the Crypto-Officer.

The temperature sensor (if enabled) and the outside range voltage sensor will not require any further action on the part of the Crypto-Officer. If either of these alarms is triggered then the module's functionality will be automatically disabled.

There are no conditions under which the temperature and abnormal voltage mechanisms are known to be ineffective.

5.3 TEMPEST Attacks

TEMPEST attacks are mitigated by the inclusion of measures to reduce the electromagnetic emanations on which TEMPEST attacks rely.

These measures cause the module's emanation profile to be restricted to that specified in 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

The mitigation of TEMPEST attacks does not require any action on the part of the Crypto-Officer as the low level of electromagnetic signals emitted by the module is an inherent part of the module's design.

5.4 Summary

Other Attacks	Mitigation Mechanism	Specific Limitations
Unauthorised movement/tamper	Movement alarm. Module is disabled if the alarm triggers.	None.
Fault induction	Temperature sensor and abnormal voltage sensor. Module is disabled if either alarm triggers.	None.
Physical intrusion	Intrusion alarm. Module is disabled if the alarm triggers.	None.
TEMPEST	Low level of electromagnetic signals.	None.

Table 5-1 Mitigation of Other Attacks

GLOSSARY

Term	Definition
Link	A single point-to-point communications link between two DC2K Security modules involving no protocol.
PPP	Point-to-point protocol. Defined in RFC 1661, the Internet standard for transmitting network layer datagrams (e.g. IP packets) over serial point-to-point links.
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
CSP	Critical Security Parameter
DEK	Data Encryption Key
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
FIPS	Federal Information Processing Standards
IP	Internet Protocol
ITU	International Telecommunications Union
KEK	Key Encryption Key
LAN	Local Area Network
NIST	National Institute of Standards and Technology
PRNG	Pseudo Random Number Generator
SHA-1	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
WAN	Wide Area 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® 2000 Commercial Version User Manual, 1270A357-002, 06/2003

   Available from Thales e-Security.