UK IT SECURITY EVALUATION AND
CERTIFICATION SCHEME

UKAS PRODUCT CERTIFICATION
122-B

COMMON CRITERIA CERTIFICATION REPORT No. P208 A

Datacryptor 2000

Application Software Version 3.3

Issue 2.0

April 2005

UK IT Security Evaluation and Certification Scheme, Certification Body,
CESG, Hubble Road, Cheltenham, GL51 0EX
United Kingdom

Trademarks:

The following trademark is acknowledged:

Datacryptor is a registered trademark of Thales e-Security Ltd.

All other product or company names are used for identification purposes only and may be trademarks of their respective owners.

CERTIFICATION STATEMENT

Thales e-Security's Datacryptor 2000 is a network encryption product that supports several network protocols. It uses public key cryptography techniques to minimise the administrative overhead of key management, and implements sophisticated measures to resist physical attack in order to safeguard key material and algorithms.

Datacryptor 2000 Application Software Version 3.3 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL5 for the specified Common Criteria Part 2 conformant functionality in the specified environment.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Head of the Certification Body UK IT Security Evaluation and Certification Scheme
Date authorised	25 April 2005

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

CA	Certificate Authority
CAPS	CESG Assisted Products Scheme
CC	Common Criteria
CEM	Common Evaluation Methodology
CLEF	Commercial Evaluation Facility
DEK	Data Encryption Key
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
HMG	Her Majesty's Government
ITSEC	Information Technology Security Evaluation Criteria
KEK	Key Encryption Key
SFR	Security Functional Requirement
SGSS	Secure Generic Sub-System
SoF	Strength of Function
TOE	Target of Evaluation
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

a. DC2000 Security Target (Common Criteria),
Thales e-Security,
Ref 0562A218, Issue 00M, 5 April 2005.

b. Datacryptor 2000 Version Under Evaluation (Common Criteria),
Thales e-Security,
Ref 0562A226, Issue 00C, 12 January 2004.

c. Datacryptor 2000 Protocols Under Evaluation (Common Criteria),
Thales e-Security,
Ref 0562A227, Issue 00D, 28 January 2004.

d. Datacryptor 2000 Cryptographic Algorithms Under Evaluation (Common Criteria),
Thales e-Security,
Ref 0562A228, Issue 00B, 7 March 2003.

e. Datacryptor 2000 – Evaluation Assurance Level,
Thales e-Security,
Ref 0562A244, Version 00B , 2nd April 2004.

f. Key Management Specification,
Racal-Airtech Ltd,
Ref 0550A109, Issue 00I, 17 March 2000.

g. Common Criteria Part 1,
Common Criteria Interpretations Management Board,
CCIMB-99-031, Version 2.1, August 1999.

h. Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-99-032, Version 2.1, August 1999.

i. Common Criteria Part 3,
Common Criteria Interpretations Management Board,
CCIMB-99-033, Version 2.1, August 1999.

j. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
Version 1.0, CEM-099/045, August 1999.

k. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 5.0, July 2002.

l. CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

m. CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 1.0, October 2003.

n. DC2K EAL5 Evaluation Technical Report,
Logica CMG Security Group,
Ref 111407/T/5, Issue 1.0, July 2004

o. DC2000 Evaluated Configuration (Common Criteria),
Thales e-Security,
Ref 1270A377, Issue 00E, 2nd August 2004.

p. Datacryptor 2000 Series Installation Guide,
Thales e-Security,
Ref 1270A274, Fifth edition, August 2001.

q. Datacryptor 2000 Series User Guide,
Thales e-Security,
Ref 1270A275, Fifth edition, August 2001.

r. Certification Report No. P126,
Datacryptor 2000 Application Version 1.01.2a using specified algorithms,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, July 1999.

s. FIPS PUB 140-1,
Security Requirements for Cryptographic Modules,
US Department of Commerce, National Institute of Standards and Technology,
11 January 1994.

t. FIPS PUB 180-1,
Secure Hash Standard (SHS),
US Department of Commerce, National Institute of Standards and Technology,
April 1995.

u. FIPS PUB 186-2,
Digital Signature Standard (DSS),
US Department of Commerce, National Institute of Standards and Technology,
27 January 2000.

v. FIPS PUB 46-3,
Data Encryption Standard (DES),
US Department of Commerce, National Institute of Standards and Technology,
25 October 1999.

w. Common Criteria Certification Report No. P208,
Datacryptor 2000 Application Software Version 3.3,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, September 2004.

x. Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology for the Common Criteria for Information Technology Security Evaluation,
Common Criteria Interpretations Management Board,
Version 1.2, CCIMB-2001/031, October 2001.

(This page is intentionally left blank)

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Datacryptor 2000 Application Software Version 3.3 to the Sponsor, Thales e-Security, and is intended to assist consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Consumers are advised to read this report in conjunction with the Security Target which specifies the functional, environmental and assurance evaluation requirements. The Security Target comprises both a main document [Reference a] and a series of supplementary documents [b - f] which address specific aspects of the evaluated claims. When further referencing the Security Target below, this Certification Report references the relevant document(s).

3. In particular, consumers should note that the scope of evaluation, as outlined below under 'TOE Scope', did not encompass the whole of the Datacryptor 2000 product.

Evaluated Product

4. The version of the product evaluated was:

Datacryptor 2000 Application SoftwareVersion 3.3.

Datacryptor 2000 is sometimes described, in other documents, as DC2000 or as DC2K. The evaluated subset of the product is also described in this report as the Target of Evaluation (TOE). The Developer was Thales e-Security.

5. The Datacryptor 2000 product incorporates a Secure Generic Sub-System (SGSS).

a. Physically the SGSS is housed within an application unit, holds all components relevant to the secure operation of the unit, encases these within a mesh and resin covering, and protects them with alarm circuitry which erases the unit's sensitive contents on detecting any of a number of specified trigger conditions.

b. The SGSS provides cryptographic protection to securely load an application into a unit, and provides a random number generator capability for use by the application. The Datacryptor 2000 comprises both a physical unit, incorporating the SGSS, and application code designed to run on the unit (note that alternative applications, comprising code and unit hardware, can be engineered for use with SGSS).

6. Other primary Datacryptor 2000 product features are as follows:

a. The application in turn provides cryptographic protection to securely load cryptographic algorithms and key material, which are then used to provide the product's network encryption functionality (between units loaded with compatible algorithms and key material).

b. The product line can be used with a variety of algorithms, key material types and communications protocols, suitable for a range of government and commercial use.

c. Management software, running on a Management Centre PC, exists to commission and configure a unit for use. Communication between the Management Centre and unit is also encrypted.

7. Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

8. An overview of the product's security architecture can be found in Annex B.

TOE Scope

9. Security functions were specified by the Security Target [a, f] in respect of the following product functionality:

a. Random number generation by SGSS, and periodic, diagnostic, statistical testing of this functionality.

b. Erasure by SGSS of sensitive content on detecting any of the following alarm conditions:
- intrusion through the mesh and resin covering;
- transgression of high or low voltage thresholds;
- transgression of high or low temperature thresholds; and
- movement of the unit.

c. Cryptographic authentication of an application loaded into SGSS.

d. Cryptographic authentication of each of the following loaded into Datacryptor 2000:
- Certificate Authorities (CA);
- Key exchange algorithm keysets;
- Key exchange algorithm ; and
- Encryption algorithm.

e. Establishment of a shared Key Encryption Key (KEK) by Datacryptor 2000.

f. Establishment of a shared Data Encryption Key (DEK) by Datacryptor 2000.

g. Encryption of network traffic by Datacryptor 2000.

10. The precise subset of this product functionality included in the TOE defined for evaluation purposes is specified in the Security Target [a, f]. Significant points of this scoping are as follows:

a. Only core components relating to this functionality were included (however cryptographic algorithms were excluded, complementary Federal Information Processing Standards (FIPS) and CESG Assisted Products Scheme (CAPS) results being quoted as outlined in paragraph 20 below).

b. Only encryption of user traffic (and not management traffic) was included

c. The following were excluded:

i. Management Centre software (other than use of Element Manager commissioning and configuration functionality used in accordance with the CC evaluated configuration guide [o]);

ii. Some functionality providing interaction between the claimed security functions, as specified in section 5.2.2 of the Security Target [a];

iii. Use of the communications ports (other than in respect of the cryptographic protection given to user traffic, e.g. remote monitoring via the network port);

iv. Use of the unit's front panel keyswitch and erase button;

v. Unit status indications given by the unit's LEDs;

vi. Use of multiple user groups (communication within such a group being authenticated by the group CA);

vii. Forced standby mode (requiring password authentication after power on of the unit); and

viii. Hot standby functionality.

11. Whilst not subjected to EAL5 evaluation, some of the excluded product functionality listed above was however used in testing the TOE, as outlined in Annex C below.

12. The CC evaluated configuration guide [o] assumes that the consumer takes delivery of a Datacryptor 2000 unit with Datacryptor 2000 application and cryptographic algorithms pre-loaded by the Developer. The functions to cryptographically authenticate an application loaded into SGSS and algorithms loaded into Datacryptor 2000 effectively therefore give protection against alternative applications or algorithms being loaded.

13. The TOE was evaluated for use of the product with the following cryptographic algorithms, as claimed by the Security Target [d]:

a.	Authentication	DSA (FIPS PUB 186-2 [u]) with SHA-1 hashing (FIPS PUB 180-1 [t]).
b.	Key Exchange	Diffie Hellman (ANSI X9.42 Hybrid1, see [f] section 8.2) with SHA-1 hashing (FIPS PUB 180-1 [t]).
c.	Encryption	Triple DES (FIPS PUB 46-3 [v]).

14. The TOE was evaluated for use of the product with the following communications protocols, as claimed by the Security Target [c]:

a. IP (tunnelling encryption mode was used).

b. Frame Relay.

c. Link (framed).

d. Link (unframed).

15. The following G.703 card options were used:

a.	Frame Relay	no G.703 card
b.	Link (framed)	G.703 card (configured for E1 timeslots).
c.	Link (unframed)	no G.703 card

Protection Profile Conformance

16. The Security Target [a] did not claim conformance to any protection profile.

Assurance

17. The Security Target [a, e] specified the assurance requirements for the evaluation. Predefined evaluation assurance level EAL5 was used. Common Criteria Part 3 [i] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [g].

18. Note that an EAL4 evaluation of the same product was performed concurrently with the EAL5 evaluation. The Security Target [a, e] accordingly specified both EAL4 and EAL5 assurance requirements.

Strength of Function Claims

19. No minimum Strength of Function (SoF) was claimed as such a metric was not directly relevant to the evaluated functionality.

20. The consumer is however advised that this CC certification is complemented by the following evaluation results, which confirmed correct implementation of the product's cryptographic algorithms:

a.	DSA	FIPS certificates 24 and 104.
b.	SHA-1	FIPS certificates 24 and 230.
c.	Triple DES	FIPS certificate 251.
d.	Diffie Hellman	CESG CAPS evaluation (of Application Software Version 3.13).

Security Policy

21. The product security policy is evident from the Security Target [a, d, f]. This includes use of the publicly known cryptographic algorithms specified in paragraph 13 above.

Security Claims

22. The Security Target [a, f] fully specifies the TOE's security objectives, the threats which these objectives counter and security functional requirements (SFRs) and security functions to elaborate the objectives. All of the SFRs are taken from CC Part 2 [h]; use of this standard facilitates comparison with other evaluated products.

23. Note that a triggering condition of sufficient degree is required to trigger the various alarms for which security functionality is claimed by section 9.1.3.2 of the Security Target [a], e.g. temperature sensors do not respond immediately to changes in ambient temperature.

Evaluation Conduct

24. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 [k -m]. The Scheme has established a Certification Body which is managed by CESG on behalf of Her Majesty's Government. .

25. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [a - f], which consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated, in accordance with CC Part 3 [i], the Common Evaluation Methodology (CEM) [j] and relevant interpretations. The TOE was then evaluated against this baseline. The working draft [x] of an international CC project update to CEM was used as a basis for interpreting and applying the EAL5 assurance requirements.

26. As noted in paragraph 18 above, an EAL4 evaluation [w] was performed concurrently with this evaluation. The Evaluators combined the activities for the respective evaluations wherever this was valid for the EAL4 and EAL5 requirements.

27. The TOE security functionality and security environment, together with much of the supporting evaluation deliverables, remained similar to or unchanged from that of Datacryptor 2000 Application Version 1.01.2a, which had previously been certified by the IT Security Evaluation and Certification Scheme to the ITSEC E3 assurance level [r]. For the evaluation of Datacryptor 2000 Application Version 3.3, the Evaluators addressed every CC Part 3 [i] EAL5 criterion but made some use of Datacryptor 2000 Application Version 1.01.2a evaluation results where these were valid for both Datacryptor 2000 Application Version 3.3 and the EAL5 requirements.

28. Developer test evidence for the claimed alarm functionality was that previously supplied as input to a CAPS evaluation of Datacryptor 2000 Application Version 3.13. The Evaluators first checked the validity of this Developer test evidence by confirming that the specification of alarm circuitry and sensors was sufficiently precise and unchanged from that version of the product.

29. Complementary FIPS and CAPS results for cryptographic algorithms, quoted above in paragraph 20, exist for Datacryptor 2000 Application Software Versions 3.1, 3.13 and 3.41. To confirm the validity of these results for Datacryptor 2000 Application Software Version 3.3 the Evaluators checked configuration management records and compared source code to confirm that the implementation of the algorithms excluded from the scope of the TOE by the Security Target [a] exhibited no significant differences.

30. The Certification Body monitored the evaluation which was carried out by the LogicaCMG Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the Evaluation Technical Report (ETR) [n] to the Certification Body in July 2004. The Certification Body then produced issue 1.0 of this Certification Report. Issue 2.0 merely caters

for a change in the SGSS acronym definition, in both this Certification Report and the Security Target.

31. Annex D of the ETR [n] references a number of Activity Reports for each of the various CC Part 3 [i] assurance classes. Within this Certification Report, these activity reports are regarded as being part of the ETR.

General Points

32. The evaluation addressed the security functionality claimed in the Security Target [a, f] with reference to the assumed operating environment specified by the Security Target. The evaluated configuration was that specified in Annex A. Consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

33. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification. Consumers should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and what assurance exists for such patches.

34. The issue of a Certification Report is not an endorsement of a product.

Note for HMG Consumers

35. The Developer has submitted certain versions of Datacryptor 2000 for CESG cryptographic evaluations (formerly known as CAPS evaluations). These are distinct from CC evaluations, and are required to give assurance where cryptographic protection is to be given to protectively marked UK government data. HMG consumers wishing to check on versions of the product evaluated to these standards are advised to check the CESG web site at www.cesg.gov.uk.

II. EVALUATION FINDINGS

Introduction

36. The evaluation addressed the requirements specified in the Security Target [a - f]. The results of this work were reported in the ETR [n] under the CC Part 3 [i] headings. The following sections note considerations that are of particular relevance to the consumer.

Delivery

37. On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

38. The following delivery items exist for the TOE:

a. The Datacryptor 2000 product, comprising Datacryptor 2000 units (with pre-loaded Datacryptor 2000 application software and algorithms) and the 'Backup' CD (holding backup Datacryptor 2000 application software and algorithms, Management Centre software and the installation and user guides [p, q]), is despatched to the consumer in response to an order.

b. The Security Target [a - f] and CC evaluated configuration guide [o] are obtainable from the Developer on a need to know basis.

39. The following measures provide for secure delivery of the Datacryptor 2000 product:

a. An Order Acknowledgement, sent on company stationery using normal mail, is sent to the consumer. This details the type and quantity of product ordered and the expected delivery date.

b. Each unit is individually shrink wrapped A number of shrink wrapped units, together with a copy of the 'Backup' CD, are packed in a carton, each of which is itself sealed.

c. Cartons are delivered to the consumer using an approved courier. The Consumer may specify their own courier, or ask to be informed of the Courier selected by the Developer, if they so desire.

d. A delivery note attached to each carton matches the previously despatched Order Acknowledgement.

e. Each unit is designed to detect tampering and render itself unusable if tampering occurs.

40. The following provide for identification of the delivered product:

a. The 'Backup' CD is clearly marked as applying to Datacryptor 2000 Application Software Version 3.3.

b. Once loaded onto a Management Centre, the Management Centre software identifies itself as part of a Datacryptor 2000 Application Version 3.3 product set.

c. The Security Target [b] also specifies identifiers for the hardware of the units. These are marked on the base of the unit and relate to the protocol variants as follows:

1600A321	Link (unframed) or Frame Relay;
1600B321	Link (framed); and
1600E321	IP.

41. The following MD5 hash values can be used to authenticate the component documents of the evaluated Security Target:

Main Security Target document [a]	ee78b6b8d78be3007689271c80520f14
Version under evaluation [b]	7b9e563f841da0e7a0812a39e0fc48db
Protocols under Evaluation [c]	387b3d3ecd19fd6948b5ebf16960341d
Algorithms under evaluation [d]	f3440c5b5ccefe48dd4589099b91ad42
Evaluation assurance level [e]	a8dfa911c4e270091b2fac83abc3ea6d
Key management specification [f]	186bd7c779ea1adb8c1ca1226bb21a73

Installation and Guidance Documentation

42. The installation and user guides [p, q] provide a variety of information relevant to the operation and use of the unit, including information relating to security and general communication settings. The CC evaluated configuration guide [o] lists the security settings which should be made to establish the evaluated configuration of the TOE, by referencing the appropriate sections of the installation and user guides.

43. In addition Appendix A of the installation guide is of note in that it contains useful information concerning the various unit status LEDs, some indicating alarms triggered by alarm functionality within the evaluated TOE. (Sections 4.2 and 4.3 of the installation guide contain useful descriptions of the various alarm functions themselves).

44. The Evaluators drew particular attention to the need to ensure that an encrypt mode is set for each connection; i.e. to ensure that traffic is encrypted and not passed as plaintext.

45. Note that for evaluation purposes, as in the evaluated configuration guide [o], key material signed by a Developer CA was used. By contrast the usual recommendation is to use key material signed by an alternative CA. Strictly the installation process to load the certificate of an alternative CA was thus not followed when installing the evaluated TOE; however the authentication mechanism then called is understood to be identical to that used to authenticate the Developer CA, and the risk of unexpected effects if using key material signed by an alternative CA is considered low.

Strength of Function

46. Based on their examination of the evaluation deliverables, the Evaluators confirmed that there were no probabilistic or permutational mechanisms in the TOE warranting a SoF claim.

47. With regard to the checks outlined in paragraph 29 above, the Evaluators confirmed that the implementations of the cryptographic algorithms in the Datacryptor 2000 Software Application Version 3.3 product exhibited no significant differences from those for which complementary FIPS and CAPS results are quoted.

Vulnerability Analysis

48. The Evaluators' vulnerability analysis was based on visibility of the TOE given by the evaluation process, a general awareness of the functionality of the overall product and its associated management software, and public domain vulnerability sources.

49. The Evaluators found no potential vulnerability for which exploitability was related to the protected asset value of £500,000 claimed by section 6.1.2 of the Security Target [a]. No exploitable or residual vulnerabilities were identified during the overall course of vulnerability analysis and penetration testing.

(This page is intentionally left blank)

III. EVALUATION OUTCOME

Certification Result

50. After due consideration of the ETR [n], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Datacryptor 2000 Application Software Version 3.3 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL5 for the specified Common Criteria Part 2 conformant functionality in the specified environment

Recommendations

51. Consumers of Datacryptor 2000 Application Software Version 3.3 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a - f]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

52. Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under 'TOE Scope' and 'Evaluation Findings'.

53. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

54. The above 'Evaluation Findings' include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE consists of selected components of:

Datacryptor 2000 Application Software Version 3.3.

2. The TOE comprises a Datacryptor 2000 application unit, with pre-loaded application software and algorithms. Protocol variant dependent hardware identifiers, marked on the base of the units, are:

- 1600A321 Link (unframed) or Frame Relay.
- 1600B321 Link (framed).
- 1600E321 IP.

3. The supporting guidance documents evaluated were:

a. DC2000 Evaluated Configuration (Common Criteria) [o],
1270A377.00E, 2nd August 2004.

b. Datacryptor 2000 Series Installation Guide [p],
1270A274-005, August 2001.

c. Datacryptor 2000 User Installation Guide [q];
1270A275-005, August 2001.

4. Further discussion of the supporting guidance material is given above under 'Installation and Guidance Documentation'.

5. A backup CD, marked as applying to Datacryptor 2000 Application Sofware Version 3.3, holds backup Datacryptor 2000 application software and algorithms, Management Centre software, and installation and user guides [p, q].

TOE Configuration

6. The product configuration used for testing was in accordance with the CC evaluated configuration guide [o]. Some test versions of the Datacryptor 2000 application code were used, as outlined below in Annex C.

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of product architectural features that are relevant to its security. Details of the scope of the evaluation are given in various sections above.

Physical Product Architecture

2. The SGSS incorporates the following components:

a. A Motorola Coldfire CPU.

b. Further processing components handling encryption and decryption.

c. Flash memory, from where code is loaded into processing components and other memory areas on unit reset or power-up.

d. Battery-backed RAM holding code and data that is persistent over a unit reset or power-down.

e. RAM holding code and data that is non-persistent over a unit reset or power-down.

f. Sensors for the following alarm conditions:

- intrusion through the mesh and resin covering (in which the SGSS is encased);
- transgression of high or low voltage thresholds;
- transgression of high or low temperature thresholds; and
- movement of the unit.

g. Alarm circuitry which causes erasure of the contents of the encryption/decryption processing components and both persistent and non-persistent RAM on transgression of any of the alarm conditions.

h. A random number generator capability.

3. The Datacryptor 2000 unit incorporates the following components in addition to those of the SGSS:

a. Further processing components handling communications.

b. G703 or IP card, in accordance with the following options:

- IP: IP card required;
- Frame Relay: G703 card optional (configured to use selected E1 or T1 timeslots);
- Link (framed) : G703 card required (configured to use selected E1 or T1 timeslots); and
- Link (unframed) : G703 card optional (configured to use all E1 or T1 timeslots).

c. Host and network ports (these are provided on the motherboard; however those on an IP or G.703 card are used if such a card is installed).

d. Ethernet and serial management ports.

e. Front panel keyswitch (for setting alarms).

f. Unit status indicator LEDs.

g. Front panel erase button.

h. Tamper evident external casing.

4. The Datacryptor 2000 unit is used in conjunction with a Management Centre, which may take the following forms:

a. Image Load Application: A PC-based application, usually used in the factory, to load SGSS and Datacryptor 2000 application software.

b. Element Manager: A PC-based Datacryptor 2000 management application, incorporating the 'Front Panel View' GUI. It may be used to manage one or more locally connected Datacryptor 2000 units, or a remote unit via a locally connected unit. Communication between the Element Manager and Datacryptor 2000 unit is usually encrypted using broadly similar cryptographic mechanisms to those used to protect the data traffic passed between a pair of units; where a unit is managed remotely then the management commands are passed as encrypted traffic between the local and remote units' network ports.

c. Crypto Manager: A unit, broadly equivalent to a Datacryptor 2000 unit, which is physically separate from the Element Manager but connected to it and providing encryption/decryption of management traffic with Datacryptor 2000 units on its behalf.

d. A general-purpose SNMP-based network management node may be used to communicate with a Datacryptor 2000 unit for the purpose of remotely viewing non TOE Security Policy enforcing communications settings.

Logical Product Architecture

5. SGSS software, which is loaded into flash memory in the factory, comprises bootstrap functions and a means of loading Datacryptor 2000 application code into the unit. The application code is concatenated with a digital signature, generated using the Developer's private key; this signature is then used to authenticate the application on loading into SGSS, using the Developer's public key embedded in the SGSS software.

6. The cryptographic architecture of the Datacryptor 2000 application is as follows:

a. A choice of publicly known and more sensitive algorithms is available for use with the Datacryptor 2000 application, for both key exchange and encryption. The Datacryptor 2000 application authenticates each algorithm when it is loaded into the unit using the public key held by the Datacryptor 2000 application.

Note that:

- For sensitive algorithms a pair of signatures can be used, one generated by the Developer and another by an appropriate CA; otherwise only Developer signatures are used.

b. Each unit needs to possess a keyset which can be verified by a common CA. The CA must first be authenticated when its certificate is loaded into the unit using the CA's public key held by the Datacryptor 2000 application. The keyset must also be authenticated on loading using the CA's public key.

Note that:

- the precise nature of the keyset depends on the key exchange algorithm used (e.g. Diffie-Hellman parameters p and g are used in the formulation of a keyset).
- A Developer CA is used initially; however the option exists to then install an alternative CA.
- A set of units operating under a common CA constitute a 'user group'. A given unit can be a member of multiple user groups if multiple CAs are installed.

c. To establish secure communication between a pair of units, the units first confirm that they are operating under a common CA by exchanging key certificates signed by the CA and authenticating each other. The key exchange algorithm is then used to establish a common KEK between the units. To derive a unique KEK, each unit uses both its signed keyset and a one-time keyset generated using the SGSS random number generator.

Note that:

- As an alternative to use of a key exchange algorithm, 'red' KEKs may be installed into a unit.

d. Each unit then generates random data using the SGSS random number generator, and exchanges this data with its peer. Each unit then uses this data, the KEK and the encryption algorithm to derive a transmit-receive pair of common DEKs.

e. Each unit uses the DEKs and encryption algorithm to encrypt and decrypt the actual data traffic being passed.

f. Encryption of data traffic is critically dependent on the mode for the connection between the pair of units being set to encrypt; otherwise the traffic may be passed as plaintext (if not discarded).

7. The Datacryptor 2000 application also includes functionality to:

a. support a unit's external communications for data and management traffic, in accordance with the relevant protocols.

b. operate the unit LEDs.

c. execute management commands received from a Management Centre and return any responses.

d. invoke periodic operations including:

- establishment of new keys on key expiry; and
- background diagnostic statistical checking of the SGSS random number generator every 10 minutes, failure of which causes the unit to cease data transmission.

e. restart the application on power-up (where the option of forced standby mode is employed, this includes blocking the transmission and receipt of host and network port traffic until a valid user password is supplied).

f. support the option of hot standby mode, in which a pair of Datacryptor 2000 units operate as master and standby.

8. The Datacryptor 2000 product suite also includes Management Centre software.

Evaluated Design Subsystems

9. The evaluated design subsystems corresponded to the subsections of sections 9.1.2 to 9.1.6 of the Security Target [a]. The role of each subsystem was that implied by the security functions specified in these subsections of the Security Target, together with the product architecture and TOE scope specified above.

ANNEX C: PRODUCT TESTING

IT Product Testing

1. The Developer performed testing of the claimed security functions. Supporting analyses demonstrated coverage of the various TOE design components, inputs and outputs, together with the associated effects and exceptions.

2. The Evaluators witnessed a sample of Developer testing and repeated a further sample of Developer tests; approximately one third of the Developer testing was either witnessed or repeated. The Evaluators also formulated and performed additional functional tests and penetration tests.

3. As the TOE comprised only a subset of core product components, it was tested through testing the product itself. Similarly the Evaluators used the visibility which they had of the overall product, e.g. that given by the guidance documentation [p, q], when performing independent vulnerability analysis and formulating penetration tests for the TOE itself. Thus a range of product functionality excluded from the TOE was exercised in the course of testing, including that:

   a. implementing cryptographic algorithms.

   b. associated with use of the communication ports (e.g. the unit's SNMP agent).

   c. associated with the unit's LEDs.

   d. providing interaction between the claimed security functions.

   e. running on the Management Centre.

4. To stimulate the desired set of effects and exceptions, a number of test versions of the Datacryptor 2000 software application were used, each of which included a variation from the standard software application engineered to produce the desired behaviours. Such behaviours included:

   a. Forcing exceptions (e.g. non-random output from the random number generation functionality).

   b. Dumping test output data to devices external to the product.

5. A number of test utilities were used, some developed for test purposes, to analyse the data generated in the course of testing. Such utilities included those which:

   a. Invoked the loading of applications into SGSS.

   b. Checked generated key material and encrypted data traffic.

   c. Checked the randomness of sequences of random numbers generated (to ensure that the TOE passed the random number generator tests specified in FIPS PUB 140-1 [s]).

6. The Evaluators were satisfied that the software developed for test purposes was appropriate for producing the intended behaviours.

7. A range of test equipment was used in conjunction with the units under test, including:

a. PCs used to exercise the units under test.

b. A PC used to record line traces of traffic passed between two units.

c. A PC used to host an SNMP network manager product.

d. That needed to test alarm conditions (e.g. heating and cooling equipment and a thermometer).

Protocol Variant Testing

8. The Evaluators were satisfied that sufficient testing was performed for the four communications protocol variants of the product:

a. Where necessary testing was repeated on all protocol variants.

b. When repeating tests which the Developer had performed only on certain protocol variants, the Evaluators repeated the tests on other protocol variants.

c. Otherwise it was demonstrated by analysis that the behaviour being tested was not sensitive to the protocol variations.