AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

Certification Report

Certificate Number: 2001/18

CTAM Pty Ltd

Cyphercell 155 ATM Encryptor Version 1.2.1 and CypherManager 3.2.0

Issue 1.0
July 2001

Issued by: -

Defence Signals Directorate - Australasian Certification Authority

CERTIFICATION STATEMENT

The Cyphercell ATM Encryptor (Version 1.2.1) is a link encryptor developed by CTAM Pty. Ltd. The Cyphercell ATM Encryptor can secure voice, data and video information transmitted over an Asynchronous Transfer Mode (ATM) network. CypherManager (Version 3.2.0) is a SNMPv3 management application that can be used to administer the Cyphercell ATM Encryptor.

This report describes the evaluation findings of the CTAM Cyphercell ATM Encryptor 1.2.1 and CypherManager 3.2.0 products to the Common Criteria (CC) Evaluation Assurance Level (EAL) 4. Recommendations are also included by the Australasian Certification Authority (ACA) that are specific to the secure use of the products to meet the CC EAL4 level of assurance. It concludes that both products have met the target Assurance Level of CC EAL4.

Originator

Chris Pennisi
Certifier
Defence Signals Directorate

Approval

Matthew Earley
Manager, Australasian Information Security Evaluation Program
Defence Signals Directorate

Authorisation

Lynwen Connick
Australasian Certification Authority
Defence Signals Directorate

TABLE OF CONTENTS

Chapter 1 Introduction

Intended Audience

1.1 This certification report states the outcome of the IT security evaluation of the CTAM Cyphercell 155 ATM Encryptor Version 1.2.1 and CypherManager Version 3.2.0 (hereafter referred to as the Cyphercell and CypherManager). It is intended to assist potential users when judging the suitability of the product for their particular requirements, and to advise security administrators on ensuring the product is used in a secure manner. Other users intending to use this product should seek advice from their relevant Security Advisory Authority to determine its suitability in meeting their particular requirements.

Identification of Target of Evaluation

1.2 The version of the software within various models of Cyphercell is version 1.2.1 and the CypherManager was version 3.2.0. CTAM Pty Ltd developed all components of the Cyphercell and CypherManager.

1.3 The security functionality offered by the Cyphercell is implemented in both the hardware and software. The CypherManager product is comprised purely of software.

1.4 The CypherManager consists of one CD-ROM. The CD-ROM contains the CypherManager software, and the administration and user guidance. The version of CypherManager on the CD-ROM should read **3.2.0** on its label**.**

1.5 The Cyphercell consists of software (version 1.2.1) installed in the hardware encryptor box. Listed below are the hardware models that are in the scope of the evaluation:

A1111A002	A1221A002	A1121A002	A1113A002	A1223A002	A1123A002
A1333A002	A1114A002	A1224A002	A1124A002	A1334A002	A1444A002
A1115A002	A1225A002	A1125A002	A1335A002	A1445A002	A1116A002
A1226A002	A1126A002	A1336A002	A1446A002	A1117A002	A1227A002
A1127A002	A1337A002	A1447A002	A1557A002	A1667A002	A1040A001

1.6 For further details of the evaluated components of the Cyphercell and CypherManager products, including details of how to identify the evaluated versions, refer to Appendix C.

Evaluation

1.7 The evaluation was carried out in accordance with the rules of the Australasian Information Security Evaluation Program (AISEP) which is described in AISEP Publication 1 and Evaluation Memorandum 2 (refs [1,2] respectively). In addition, the conditions outlined in the Common Criteria Recognition Arrangement (ref [18]) were also upheld during the evaluation and certification of their products.

1.8 The purpose of the evaluation was to provide assurance about the effectiveness of the Target of Evaluation (TOE), the Cyphercell and CypherManager products, in meeting their Security Target (ref [9]). The criteria against which the TOE is judged, are expressed in the Common Criteria Part 3 (ref [5]). This describes how the degree of assurance can be expressed in terms of the levels EAL1 to EAL7. The methodology used is described in the Common Evaluation Methodology (CEM) and Evaluation Memoranda 4 and 5 (refs [6,7,8]).

1.9 The evaluation was sponsored by CTAM Pty Ltd. The developer of the Cyphercell and CypherManager product was also CTAM Pty Ltd. A complete listing of the documentation used during the evaluation of this product is included or referenced in Appendix A of this Report.

1.10 The evaluation was performed by CSC Australia Pty Ltd between March 1999 and April 2001, and was monitored by the Certification Group on behalf of the Australasian Certification Authority (ACA). At the end of the evaluation, an Evaluation Technical Report (ETR) (ref [10]) describing the evaluation and its results was presented to the ACA. The Certification Report was then produced, based on the contents of the ETR and the Certification Group's knowledge of the evaluation.

1.11 The Security Target (ref [9]) claimed an assurance level for the product of CC EAL4.

General Points

1.12 Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher evaluation levels) that exploitable vulnerabilities remain undiscovered.

1.13 EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behaviour. Assurance is additionally gained through an informal model of the TOE security policy.

1.14 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

1.15 EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

1.16 The Cyphercell and CypherManager should only be used within the defined TOE security environment in accordance with the specified assumptions, as explained in section 3.1 of the ST (ref [9]). Also, the security requirements on the IT environment must be fully understood in order to determine the suitability of the product in its assumed operational environment, as explained in section 5.4 of (ref [9]). In addition, users should be aware of the certifiers' recommendations as given in Chapter 4 of this report.

1.17 Ultimately, it is the responsibility of the user to ensure that the Cyphercell and CypherManager products meet their requirements. For this reason, it is ***strongly*** recommended that a prospective user of the product obtains a copy of the Security Target (ref [9]) from the product vendor, and reads this Certification Report thoroughly prior to deciding whether to purchase the product.

Scope of the Evaluation

1.18 The scope of the evaluation is limited to those claims made in the Security Target (ref [9]). A summary of the Security Target is provided in Annex B of this Certification Report. All security related claims in the Security Target were evaluated by CSC Australia Pty. Ltd. The cryptographic mechanisms were evaluated by DSD and were found to be appropriate for Australian Government use.

1.19 Commonwealth Government users should consult Australian Computer-Electronic Security Instruction (ACSI) 33 (ref [17]) for advice on using the product for the protection of National and non-National classified material. This document may be obtained from DSD (www.dsd.gov.au/infosec).

1.20 Potential Commonwealth Government users are also encouraged to contact DSD for further advice on the suitability of these products when used in conjunction with other evaluated products to protect National and non-National classified information.

Chapter 2 Security Overview of the Cyphercell and CypherManager

2.1 Potential users are strongly recommended to read the Security Target (ref [9]). This explains the security functionality of the Cyphercell and CypherManager products in greater detail, as well as the intended environment and method of use for the products. A summary of the Security Target can be found in Appendix B. A full copy of the Security Target can be obtained from the sponsor of the evaluation.

Functionality of the TOE

2.2 This section provides a summary of the operational role of the TOE together with the security functions it is designed to perform.

2.3 The TOE is comprised of the Cyphercell and the CypherManager.

2.4 The Cyphercell is a high-speed encryptor, which can secure voice, data and video information transmitted over Asynchronous Transfer Mode (ATM) networks at data rates up to 155 Megabits per second. It can also provide access control facilities using access rules for defined virtual circuits.

2.5 The Cyphercell can be remotely managed by using CypherManager, a SNMPv3 compliant management station using a secure management session, or locally through an RS232 console port without the CypherManager application. However, Cyphercell cannot be initialised with an X.509 certificate through the console port.

2.6 Confidentiality of the transmitted information is achieved by encrypting the payload of the ATM cell while leaving the ATM header unchanged. This enables switching of the cell through ATM networks. Operation and Maintenance (OAM) cells and Virtual Path cells with Virtual Channel Identifier (VCI) values of 3, 4, and 6 to 15 are not encrypted enabling ATM management functionality to be maintained.

2.7 Key management and authentication are based on RSA public key cryptography and X.509 certificates providing an automated key management system.

2.8 Any combination of encrypted or unencrypted virtual circuits can be configured. Each encrypted virtual circuit uses different encryption keys.

2.9 The dedicated Ethernet management port on the Cyphercell supports 10baseT and AUI connections.

2.10 The Cyphercell provides the following security functionality:

a) Payload Encryption - Cyphercell provides selective encryption/decryption of cells transmitted or received. The payload of the cell is encrypted/decrypted according to the action specified for that particular Virtual Path Identifier/Virtual Channel Circuit (VPI/VCI) address contained in the cell header or the cell can be discarded. Secure virtual circuits are established by exchanging session keys using RSA public key cryptography. X.509 certificates are used to authenticate the RSA exchange. Cyphercell will only exchange sessions with other units whose X.509 certificate has been signed by the same certification authority as its own X.509 certificate.

b) Access Control - Any cells received that do not have a Virtual Channel Action Table (VCAT) entry for that particular VPI/VCI address are discarded. The default setting for all VPI/VCI addresses is discard. For defined VPI/VCI addresses time of access can be specified. Cells received outside the specified time period are discarded.

c) Auditing - An audit trail is generated and maintained by Cyphercell for security related events. The audit output can be viewed locally from the console port or remotely from the management station.

d) Management Interface - Cyphercell can be managed using a command line interface via a directly connected management console. Only authorised users, as defined by the administrator can gain access to the management facilities of the unit. Users are identified by a user name and password and are assigned one of three allowable access levels.

2.11 The CypherManager provides the following security functionality:

a) CypherManager, which implements SNMPv3 management sessions, provides secure remote management to the unit. Depending on the network security policy, a user may be required to have both an authentication password and a privacy password for remote management sessions. By default, CypherManager enforces the requirement for authentication passwords, and privacy passwords are enabled at the option of the Cyphercell/CypherManager administrator.

2.12 The evaluated security functions of the TOE counter the following types of threat:

a) Attackers eavesdropping on or capturing data being transmitted across a public ATM network in order to recover information that was to be kept confidential.

b) Unauthorised attempts to connect to another ATM network and transmit information that was to be kept confidential, to another destination.

c) Undetected compromise of information as a result of an authorised user of the TOE (intentionally or otherwise) performing actions that that individual is not authorised to perform.

d) Undetected compromise of information as a result of an attacker (insider or outsider) attempting to perform actions that that individual is not authorised to perform.

e) Attackers (insider or outsider) impersonating an authorised user of the TOE to gain access to transmitted information that was to be kept confidential.

f) Attackers observing multiple uses of services by an entity, and by linking these uses, deduce information, which the entity wishes to be kept confidential.

g) An attacker observing the legitimate use of the remote management service by an authorised user when that authorised user wishes their use of that remote management service to be kept confidential.

h) Possible physical attack of security critical parts of the TOE which may compromise security.

i) A compromise of information which may occur as a result of actions taken by careless, willfully negligent hostile administrators or other authorised users.

2.13 The evaluated security functions of the TOE do not counter the following types of threat, which must be addressed by environmental and procedural means as specified in the Security Target (ref [9]) and the guidance documentation (refs [11] - [14]):

a) Direct physical access to the Management Station or the Cyphercell on which the TOE is installed;

b) Compromise of the private keys used by the TOE; and/or

c) Malicious operation of the TOE by trusted administrators.

2.14 Cyphercell and CypherManager achieve eight security objectives for the TOE to create and maintain the confidentiality of the transmitted information. Availability and integrity concerns are not countered by the TOE. These security objectives for the TOE have been satisfied by eight categories of technical (IT) countermeasures implemented by the TOE (i.e. TOE Security Functions (TSF)) in software and hardware. These are provided individually or in collaboration with one or more of the Cyphercell and CypherManager components identified below.

2.15 In addition, Cyphercell and CypherManager achieve six security objectives for the environment. These security objectives for the environment have been satisfied by a collaboration of technical measures implemented by the IT environment, and by the enforcement of non-IT (e.g. procedural) measures.

2.16 The minimum software and hardware configurations have been stipulated in section 1.1 of the Security Target (ref [9]).

2.17 More detailed information on the Cyphercell and CypherManager products can be found in the Security Target (ref [9]), and in Appendix B of this report.

Architecture of the TOE

2.18 This section provides a summary of the architectural design of the TOE together with the security functions it is designed to perform.

2.19 The TOE is a hardware and software product. The TOE is made up of six distinct subsystems. These are the Management subsystem, Local Interface subsystem, Network Interface subsystem, Encryption subsystem, Decryption subsystem and CypherManager.

2.20 The Cyphercell has both hardware and software components and CypherManager is comprised purely of software. It should be noted that once the Cyphercell software is installed on the hardware models detailed in paragraph 1.5 above it is recognised as firmware.

2.21 The functionality is distributed between these mediums as described in the following sections and therefore does not require interaction from the administrator.

Hardware Description

2.22 The hardware contains the mechanisms for key destruction and the cryptographic functions. The TOE hardware executes the software of three hardware boards, namely the Management board, the Network interface board and the Local interface board.

2.23 The casing of the product is tamper-proof through the inclusion of micro-switches which disconnects the battery power to the memory that holds the keys, user accounts table and VCAT, when the case has been tampered with.

2.24 The purpose of the Encryption and Decryption systems is to ensure correct cryptographic operation. These interfaces enforce the encryption/decryption algorithms (DES/3DES) while ATM traffic is in transmission. All other operations concerning these subsystems are handled by the other subsystems (i.e. the local and network interface subsystems) through the appropriate interfaces.

Software Description

2.25 The Cyphercell has both hardware and software components, whilst the CypherManager consists of purely software. The functionality is distributed between these products as described below.

Cyphercell Software

2.26 The Cyphercell comprises the following architectural components:

a. Management subsystem, comprising:

i) Identification and Authentication;

ii) Access control; and

iii) Audit;

b. Local Interface subsystem, comprising:

i) Access control;

ii) Audit;

iii) Cryptographic Key Management; and

iv) Data Exchange.

c. Network Interface subsystem, comprising

i) Access control;

ii) Audit;

iii) Cryptographic Key Management; and

iv) Data Exchange.

2.27 The Management subsystem deals directly (i.e. interfaces) with all other subsystems in the TOE, and indirectly with the encryption and decryption subsystems.

2.28 The Local Interface subsystem is mostly concerned with the handling of unencrypted information to/from the protected network and preparing the payload to/from the encryption subsystem.

2.29 The Network Interface subsystem is mostly concerned with the handling of encrypted information to/from the unprotected network and preparing the payload to/from the decryption subsystem.

CypherManager Software

2.30 The CypherManager comprises the following architectural components:

a. CypherManager subsystem, comprising

i) X.509 Certificate Management;

ii) Cryptographic Key Management; and

iii) Data Exchange.

2.31 The main purpose of the CypherManager subsystem is to provide a graphical and remote user interface to the Cyphercell. The CypherManager is also instrumental in the installation of the Cyphercells as the Cyphercells require a single CypherManager to function as a Certificate Authority (CA) to allow communications. Functioning as a CA, the CypherManager is able to generate signed X.509 certificates and authenticate X.509 certificates and requests.

Security Policy

2.32 The following security policies are enforced by the Cyphercell and CypherManager:

Identification and Authentication Policy

2.33 The Identification and Authentication Policy describes the requirements for gaining access to the TOE. The TOE implements this policy based on the following rules:

a) There is no interaction with the TOE before a user is authenticated;

b) Users must have a valid account;

c) Users must enter a valid account name; and

d) Users must enter a valid password.

Cell Access Control Policy

2.34 The Cell Access Control Policy describes the requirements for accepting and processing cells sent through the TOE. The TOE implements this policy based on the following rules:

a) If a cell arrives in a channel that has an entry in the VCAT, the cell will be processed according to that entry, i.e. encrypted/decrypted, Bypassed (transmitted unchanged) or Discarded.

b) If a cell arrives on a channel that does not have an entry in the VCAT the cell is discarded.

Role Based Access Policy

2.35 The Role Based Access describes the requirements for communication between the users and the TSF and their privileges. Access to management functions is controlled by identification and authentication, and user roles. User roles are associated to user names and are managed by Administrators. The following roles exist and have the following privileges:

a) Administrator, who has full access rights;

b) Supervisor, who has full access rights except they cannot add, delete or modify user accounts and they cannot install X.509 certificates; and

c) Operator, who can view all available information but cannot delete, add or modify the information.

Audit Policy

2.36 The Audit Policy describes the requirements for auditing of TOE management actions. The TOE implements this policy based on the following rules:

a) The TOE will audit all TOE management actions outlined in the Security Target (ref[9]). The TOE will not audit ATM cell access.

2.37 The security policy model is summarised in chapter 3.3 of the ETR (ref [10]). Alternatively, the security policy model (ref [22]) may be requested directly from the developer.

2.38 In order for the TOE to comply with the security policy model, the Cyphercell and CypherManager products should only be used within the defined TOE security environment in accordance with the secure usage assumptions, as explained in section 3.1 of the Security Target (ref [9]).

Documentation

2.39 Before using the product, administrators and security managers should ensure that they are aware of and fully understand the relevant operational documentation. In addition, they should ensure that they read Chapter 4 of this document, and the associated administration and user manuals contained on the product CD-ROM (refs [11]-[14]).

Chapter 3 Evaluation Findings

Introduction

3.1. The evaluation of the Cyphercell and CypherManager followed a course consistent with the generic evaluation work program described in the ITSEM (ref [16]) and the CEM (ref [6]), with work packages structured around the evaluator actions described in the CC Part 3 (ref [5]). The results of this work are reported in the ETR (ref [10]) under the CC headings. This report summarises the general results, followed by the findings in relation to the security functionality claimed in the Security Target (ref [9]).

Security Target Evaluation

3.2. The purpose of a Security Target evaluation is to demonstrate that it is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

TOE Description (ASE_DES.1)

3.3. The TOE Description adequately described the product type, and the scope and boundaries of the TOE in general terms both in a physical and a logical way.

3.4. The above results have enabled the certifiers to conclude that the Security Target has met the requirements for the TOE Description, and consider it suitable to be used (in part) as a basis for the evaluation.

Security Environment (ASE_ENV.1)

3.5. The statement of the TOE security environment adequately identified and explained the assumptions about the intended usage of the TOE (and its environment), and the known threats to the protected assets of the TOE (and its environment). All organisational security policies were identified and explained. There were three identified organisational security policies with which the TOE had to comply with, P.CRYPTO, P.FILTER and P.ROLES.

3.6. The above results have enabled the certifiers to conclude that the Security Target has met the requirements for the Security Environment, and consider it suitable to be used (in part) as a basis for the evaluation.

ST introduction (ASE_INT.1)

3.7. The Security Target introduction identified and adequately described the document and the TOE. It contained an overview in narrative form, and contained a CC conformance claim to meet the predefined assurance level of EAL4.

3.8. The above results have enabled the certifiers to conclude that the Security Target has met the requirements for the Security Target introduction, and consider it suitable to be used (in part) as a basis for the evaluation.

Security Objectives (ASE_OBJ.1)

3.9. The statement of the TOE and environmental security objectives were adequately defined, and were clearly traceable back to the identified threats countered by the TOE, the assumptions on the TOE and its environment, and to organisational security policies.

3.10. The Security Target also contained a strength of function claim of SOF-basic. This was defined for an Identification and Authentication function, which is consistent with the Security Objectives defined in the TOE.

3.11. The security objective's rationale demonstrated that the security objectives were suitable to counter the identified threats and cover the identified assumptions and organisational security policies.

3.12. The above results have enabled the certifiers to conclude that the Security Target has met the requirements for the Security Objectives, and consider it suitable to be used (in part) as a basis for the evaluation.

Protection Profile (PP) Claims (ASE_PPC.1)

3.13. The Security Target did not claim conformance to any PPs.

IT Security Requirements (ASE_REQ.1)

3.14. The statement of the TOE Security Functional Requirements (SFRs) correctly identified the SFRs drawn from CC Part 2 (ref [4]), and the TOE Security Assurance Requirements (SARs) for EAL4 from CC Part 3 (ref [5]). The justification for using the pre-defined EAL4 assurance package was sufficient.

3.15. The Security Target included a statement with a minimum strength of function claim for the TOE SFRs of SOF-basic. All specific TOE SFRs for which an explicit strength of function is appropriate were identified with a specific metric defined. The security requirements rationale demonstrated that this was consistent with the security objectives of the TOE.

3.16. Security requirements on the IT environment were identified. All operations on the IT security requirements were completed, and the relevant dependencies were satisfied. The security requirements rationale demonstrated that the IT security requirements were suitable to meet the security objectives. It also demonstrated that the set of IT security requirements together forms a mutually supportive and internally consistent whole.

3.17. The above results have enabled the certifiers to conclude that the Security Target has met the requirements for the IT Security Requirements, and consider it suitable to be used (in part) as a basis for the evaluation.

Explicitly stated IT Security Requirements (ASE_SRE.1)

3.18. The Security Target did not contain any explicitly stated IT security requirements.

TOE Summary Specification (ASE_TSS.1)

3.19. The TOE summary specification (TSS) adequately described the IT security functions and the assurance measures of the TOE. The TSS traced and clearly mapped all IT security functions to the TOE security functional requirements demonstrating that all TOE security functions contribute to the satisfaction of at least one TOE security functional requirement.

3.20. The IT security functions were informally specified to an appropriate level of detail. Security mechanisms were easily traced back to the relevant TOE security functions.

3.21. The TOE summary specification rationale demonstrated that the IT security functions were suitable to meet the TOE security functional requirements, and that the combination of IT security functions work together to also satisfy the TOE security functional requirements. The rationale also demonstrated, aided by a mapping, that the assurance measures met the assurance requirements for EAL4.

3.22. The TOE summary specification stated that there were several functions where a strength of function claim was required. It is noted that probabilistic user password verification was identified and a strength of function claim of SOF-Basic was made. A password-based key generation function was also identified, as well as several other cryptographic security functions. A strength of function claim for these functions is not required, as DSD determines the appropriateness of cryptographic operations for

Australian Government use.

3.23. The above results have enabled the certifiers to conclude that the Security Target has met the requirements for the TOE Summary Specification, and consider it suitable to be used (in part) as a basis for the evaluation.

ST Evaluation Result

3.24. The certifiers consider that the above results have demonstrated that the Security Target is complete, consistent, technically sound, and hence suitable for use as the basis for the evaluation.

Common Criteria EAL4 Security Assurance Requirements

1.21 EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behaviour. Assurance is additionally gained through an informal model of the TOE security policy.

1.22 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

1.23 EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures. The results of this evaluation are discussed below.

Configuration Management (ACM)

3.25. Configuration management is one method or means for establishing that the functional requirements and specifications are realised in the implementation of the TOE. Configuration management meets these objectives by requiring discipline and control in the processes of refinement and modification of the TOE and the related information. Configuration management systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking any changes, and by ensuring that all changes are authorised.

Configuration Management (CM) Capabilities (ACM_CAP.4)

3.26. The TOE reference was assessed to be unique to each version of the TOE. In addition, the TOE was correctly labeled with its reference.

3.27. The CM documentation included a configuration list, CM plan, and an acceptance plan, and adequately described the method used to uniquely identify the configuration items. The configuration list correctly described the configuration items of the TOE. The CM plan adequately described how the CM system was being used to uniquely identify the configuration items.

3.28. The CM system was demonstrated to operate in accordance with the CM plan, and that all configuration items were being effectively maintained under the CM system. The CM system provided adequate measures to ensure that only authorised changes are made to the configuration items. The CM system appropriately supported the generation of the TOE.

3.29. An acceptance plan was also provided that adequately described the procedures used to accept modified or newly created configuration items as part of the TOE.

3.30. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in June 2000.

3.31. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Configuration Management Capabilities assurance component for EAL4.

Configuration Management Automation (ACM_AUT.1)

3.32. The CM system provided an adequate automated means by which only authorised changes were made to the TOE implementation representation (i.e. the source code and hardware drawings), and an automated means to support generation of the TOE.

3.33. The CM plan adequately described the automated tools and how they are used in the CM system.

3.34. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in June 2000.

3.35. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Configuration Management Automation assurance component for EAL4.

Configuration Management Scope (ACM_SCP.2)

3.36. The CM documentation correctly showed that the CM system tracks the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

3.37. The CM documentation adequately described how the configuration items were being tracked by the CM system.

3.38. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in June 2000.

3.39. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Configuration Management Scope assurance component for EAL4.

Delivery and Operation (ADO)

3.40. This aspect of the evaluation examines the requirements for the measures, procedures, and standards concerned with secure delivery, installation and operational use of the TOE, ensuring that the security protection offered by the TOE is not compromised during transfer, installation, start-up and operation.

Delivery (ADO_DEL.2)

3.41. The delivery documentation adequately described all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

3.42. The procedures and technical measures for the detection of modifications of the Cyphercell, or any discrepancy between the developer's master copy of CypherManager and the version received at the user site, were adequately described. The delivery documentation also adequately described how the various procedures allowed for the detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

3.43. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Delivery assurance component for EAL4.

Installation, Generation and Start-Up (ADO_IGS.1)

3.44. The operational documentation adequately described the steps necessary for secure installation, generation, and start-up of the TOE.

3.45. The evaluators confirmed that the installation and generation of the TOE was achieved through the application of the documented procedures.

3.46. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Installation, Generation and Start-Up assurance component for EAL4.

Development (ADV)

3.47. This aspect of the evaluation examines the requirements for the stepwise refinement of the TSF from the TOE summary specification in the Security Target down to the actual implementation. Each of the resulting TSF representations provide information to help determine whether the functional requirements of the TOE have been satisfied.

Functional Specification (ADV_FSP.2)

3.48. The functional specification informally described the TSF and its external interfaces, including a description on the purpose and method of use of all external TSF interfaces, while also providing complete details of all effects, exceptions and error messages.

3.49. The functional specification was found to be internally consistent and to completely represent the TSF. This was supported by a rationale justifying that the TSF did in fact completely represent the TSF.

3.50. Furthermore, the functional specification was determined to be an accurate and complete instantiation of the TOE security functional requirements.

3.51. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Functional Specification assurance component for EAL4.

High-Level Design (ADV_HLD.2)

3.52. The presentation of the High-Level Design was informal and found to be internally consistent. It adequately described the structure of the TOE in terms of sub-systems, and the security functionality provided by each sub-system of the TSF.

3.53. The TSF does not rely on any protection mechanisms implemented by the underlying hardware, firmware or software of the TOE.

3.54. The High-Level Design identified all interfaces to the sub-systems of the TSF, together with an identification of the interfaces that are externally visible. The purpose and method of use of all these interfaces were adequately described, including details of the effects, exceptions and error messages. Finally, the separation of the TOE into TSP-enforcing and other sub-systems was correctly described.

3.55. Furthermore, the High-Level Design was determined to be an accurate and complete instantiation of the TOE security functional requirements.

3.56. As a result of the above determinations, the certifiers conclude that the TOE fully meets the High-Level Design assurance component for EAL4.

Low-Level Design (ADV_LLD.1)

3.57. The presentation of the Low-Level Design was informal and found to be internally consistent. The Low-Level Design adequately described the TSF in terms of modules, and the purpose of each of these modules. The interrelationships between the modules in terms of provided security functionality and dependencies on other modules were also adequately described.

3.58. The Low-Level Design described how each TSP-enforcing function was provided, and identified all interfaces to the modules of the TSF, including all interfaces that are externally visible. The purpose and method of use of all these interfaces were adequately described, including details of the effects, exceptions and error messages. Finally, the separation of the TOE into TSP-enforcing and other modules was correctly described.

3.59. Furthermore, the Low-Level Design was determined to be an accurate and complete instantiation of the TOE security functional requirements.

3.60. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Low-Level Design assurance component for EAL4.

Implementation (ADV_IMP.1)

3.61. The developer provided the entire source code for the implementation representation. The evaluators chose a subset corresponding to approximately 18.9% of the TSF. Given the nature of the TOE, this sample size was considered sufficiently representative of the TSF.

3.62. The implementation representation was found to unambiguously define the TSF to a level of detail such that the TSF could be generated without any further design decisions. In addition, the implementation representation was confirmed to be internally consistent.

3.63. Furthermore, the implementation representation was determined to be an accurate and complete instantiation of the TOE security functional requirements.

3.64. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Implementation assurance component for EAL4.

Representation Correspondence (ADV_RCR.1)

3.65. An analysis of the correspondence between all adjacent pairs of the TSF representation was provided. This analysis demonstrated that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation, which was the implementation.

3.66. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Representation Correspondence assurance component for EAL4.

Security Policy Model (ADV_SPM.1)

3.67. The developer provided a TOE Security Policy (TSP) model that was presented informally, and described the rules and characteristics of all the relevant security policies. A rationale was included that appropriately demonstrated that it was complete and consistent with all of the identified security policies.

3.68. The developer also demonstrated that the correspondence between TSP model and the functional specification showed that all of the security functions in the functional specification were consistent and complete with respect to the TSP model

3.69. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Security Policy Model assurance component for EAL4.

Guidance Documents (AGD)

3.70. This aspect of the evaluation examines the requirements directed at the understandability, coverage and completeness of the operational documentation provided by the developer. This documentation, which provides two categories of information, for users and administrators, is an important factor in the secure operation of the TOE.

Administrator Guidance (AGD_ADM.1)

3.71. The administrator guidance clearly described the administrative functions and interfaces, instructions on how to administer the TOE securely, all assumptions regarding user behaviour that are relevant to the secure operation of the TOE, all security parameters under the control of the administrator, and each type of security-relevant event relative to the administrative functions being performed, including changing the security characteristics of entities under control of the TSF.

3.72. The guidance also contained appropriate warnings about functions and privileges that need to be controlled in a secure environment, and indicated secure values if applicable.

3.73. The administrator guidance described all security requirements for the IT environment that were relevant to an administrator, and was consistent with all other documentation supplied for the evaluation.

3.74. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Administrator Guidance assurance component for EAL4.

User Guidance (AGD_USR.1)

3.75. The user guidance clearly described the functions and interfaces available to the non-administrative users of the TOE, and the use of user-accessible security functions provided by the TOE. Appropriate warnings about user-accessible security functions and privileges that should be controlled in a secure processing environment were also described.

3.76. All user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of the TOE security environment, were clearly presented.

3.77. The user guidance described all security requirements for the IT environment that were relevant to a user, and was consistent with all other documentation supplied for the evaluation.

3.78. As a result of the above determinations, the certifiers conclude that the TOE fully meets the User Guidance assurance component for EAL4.

Life-Cycle Support (ALC)

3.79. This aspect of the evaluation examines the requirements for assurance through the adoption of a well-defined life-cycle model for all the steps of the TOE development, correct use of tools and techniques, and the security measures used to protect the development environment.

Development Security (ALC_DVS.1)

3.80. The development security documentation adequately described all the physical, procedural, personnel, and other security measures that were necessary to protect the confidentiality and the integrity of the TOE design and implementation in its development environment. It also provided evidence that these security measures were being followed during the development and maintenance phases of the TOE.

3.81. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in June 2000.

3.82. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Development Security assurance component for EAL4.

Life-Cycle Definition (ALC_LCD.1)

3.83. The life-cycle definition documentation adequately described the model used to develop and maintain the TOE, and how the model provides the necessary control measures used during these phases.

3.84. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in June 2000.

3.85. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Life-Cycle Definition assurance component for EAL4.

Tools and Techniques (ALC_TAT.1)

3.86. All development tools use during the implementation phase was determined to be well defined. The documentation associated with these tools unambiguously defined the meaning of all statements, including the implementation-dependent options, used in the implementation.

3.87. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in June 2000.

3.88. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Tools and Techniques assurance component for EAL4.

Tests (ATE)

3.89. Testing helps to establish that the TOE security functional requirements are met. Testing provides assurance that the TOE satisfies at least the TOE security functional requirements, although it cannot establish that the TOE does no more than what was specified. Testing at this level of assurance is also directed towards the internal structure of the TSF, such as the testing of subsystems (identified in the High-Level Design) against their specification.

Coverage (ATE_COV.2)

3.90. The test coverage analysis adequately demonstrated the correspondence between the tests identified in the test documentation and the TSF described in the functional specification, and that the coverage was complete.

3.91. The developer's functional testing covered all TSFs specified in the functional specification.

3.92. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Coverage assurance component for EAL4.

Depth (ATE_DPT.1)

3.93. The depth analysis adequately demonstrated that the tests identified in the test documentation were sufficient to demonstrate that the TSF operates in accordance with its high-level design.

3.94. The developer's functional testing covered all sub-systems and sub-system interfaces specified in the high-level design of the TSF.

3.95. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Depth assurance component for EAL4.

Functional Testing (ATE_FUN.1)

3.96. The provided test documentation consisted of test plans, test procedure descriptions, expected test results and actual test results. The documentation identified the security functions that were tested and the goals of each test. The test procedure descriptions described the scenarios for testing each security function. The scenarios did require that the some of the tests completed in a particular way; this requirement was specified in the test pre-requisites.

3.97. The expected test results showed the anticipated outputs from the successful execution of these tests, and the test results demonstrated that each security function behaved as specified.

3.98. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Functional Testing assurance component for EAL4.

Independent Testing (ATE_IND.2)

3.99. Independent testing was conducted to confirm that the TOE operates as specified in the documentation supplied for the evaluation. The configuration of the TOE (and its environment) used during testing was consistent with the evaluated configuration, as stipulated in the ST (ref [9]) and the operational guidance (refs [11] - [14]). In addition, an equivalent set of resources was used that were utilised during the developer functional testing of the TSF.

3.100. A 34% sample of the developer tests was selected to verify the developer's test results. All tests executed by the evaluators from the selected sample of developer tests produced the expected results, consistent with the results produced by the developer's own functional testing.

3.101. The evaluators based their own independent testing on the sample identified above, and extended their testing to investigate the behaviour of the VCAT operation which implements (with the encryption functions) the confidentiality of transmitted data, as well as testing SFRs that enforce the confidentiality of the TSF management data via user permission. Ad hoc testing was also performed where appropriate. All tests were sufficiently documented to enable the tests (and their results) to be reproducible.

3.102. The overall outcome of the evaluator testing effort showed that the TOE security functions have been implemented correctly in the TOE. A summary of the evaluator testing effort for this component can be found in section 5.6 of the ETR (ref [10]).

3.103. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Independent Testing assurance component for EAL4.

Vulnerability Assessment (AVA)

3.104. This aspect of the evaluation examines the requirements directed at the identification of exploitable vulnerabilities. Specifically, it addresses those vulnerabilities introduced in the construction, operation, misuse, or incorrect configuration of the TOE.

Misuse (AVA_MSU.2)

3.105. The guidance documentation appropriately identified all possible modes of operation of the TOE, including operation following failure or operational error, their consequences and implications for maintaining secure operation. The guidance documentation was also determined to be complete, clear, consistent and reasonable.

3.106. The guidance documentation appropriately listed the assumptions about the intended environment, and all the requirements for external security measures. The developer provided analysis of the guidance documentation demonstrated that it was complete. The evaluators confirmed that this analysis showed that relevant guidance is provided for secure operation in all modes of operation of the TOE.

3.107. The evaluators repeated the installation and configuration procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation, and that all insecure states could be detected using this documentation.

3.108. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Misuse assurance component for EAL4.

Strength of Function (AVA_SOF.1)

3.109. The Security Target made a strength of function claim of basic against three SFRs of the TOE. The evaluators confirmed that these claims were correct.

3.110. The cryptographic operations (i.e. key generation) were evaluated separately by DSD as the National Computer Security Advisory Authority. They were determined to be appropriate for Australian Government use.

Vulnerability Analysis (AVA_VLA.2)

3.111. The developer provided a vulnerability analysis searching for ways in which a user can violate the TSP. The documentation showed that none of the identified vulnerabilities were exploitable in the intended environment for the TOE. It also justified that the TOE is resistant to obvious penetration attacks.

3.112. The evaluators performed their own independent vulnerability analysis and conducted penetration testing to ensure that the identified vulnerabilities had been addressed.

3.113. Additional testing did not identify any vulnerabilities that were not considered by the developer. The overall outcome of the evaluator penetration testing effort showed that there are no exploitable vulnerabilities of the TOE in its intended environment.

3.114. Finally, the evaluators determined that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential. A summary of the evaluator testing effort for this component can be found in Annex B of the ETR (ref [10]).

3.115. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Vulnerability Analysis assurance component for EAL4.

Specific Functionality

3.116. The TOE Security Functional Requirements and the TOE Security Functions provided by Cyphercell and CypherManager are specified in sections 5.1 and 6.1 of the Security Target (ref [9]) and summarised in Appendix B of this report.

3.117. The evaluators found that the product provided the TOE security functionality and satisfied the TOE Security Functional Requirements, as specified in the Security Target (ref [9]).

Discussion of Unresolved Issues

3.118. At the conclusion of the evaluation there were no unresolved issues requiring the consideration of the certifiers.

General Observations

3.119. The certifiers would like to acknowledge the invaluable assistance provided by CTAM Pty Ltd staff during the evaluation. They provided helpful advice, and technical assistance during this process.

3.120. Further, the certifiers would like to acknowledge the efforts of CSC in ensuring prompt delivery of the ETR (ref [10]) for certification.

Chapter 4 Conclusions

Certification Result

4.1 After due consideration of the ETR (ref [10]) produced by the evaluators and the conduct of the evaluation as witnessed by the certifiers, the Australasian Certification Authority has determined that Cyphercell and CypherManager have met the requirements of the CC EAL4 Assurance level.

Scope of the Certificate

4.2 This certificate applies only to CypherManager (Version 3.2.0) and Cyphercell (Version 1.2.1). This certificate is only valid when the Cyphercell and CypherManager products correctly comprises the designated components. These components are identified in Appendix C and should be verified on receipt of the delivered product.

Recommendations

4.3 The following recommendations involve information highlighted by the evaluators during their analysis of the developer's deliverables, during the conduct of the evaluation, and during the additional activities performed by the Certification Group.

Functionality not part of the Cyphercell

4.4 Due to the nature of the TOE, the following considerations need to be taken into account when deploying the Cyphercell unit:

a) The Cyphercell is a network boundary device and as such does not provide protection of the integrity or availability of the internal network.

b) The Cyphercell can not distinguish between an intruder or an authorised user if a connection is established to the internal protected network through other means. Potential purchasers of the TOE are advised that additional security measures need to be put in place to provide this functionality.

Functionality excluded from the Evaluation

4.5 The Cyphercell unit is delivered containing several external interfaces to the unit. It should be noted that the smart card reader is outside the scope of the evaluation.

4.6 Potential users of the TOE are advised that when using CypherManager protection of the private key used to sign X.509 certificates is required in the absence of appropriate physical access controls.

4.7 Further, if a hardware token were to be used to protect the private key, the Certification Group recommends that an appropriate token be evaluated to a level commensurate with the evaluation so that it can be used in conjunction with the TOE to implement secure key storage.

Requirements for administration of the TOE

4.8 The Administrator of the Cyphercell should:

a) Ensure that if a modem is to be connected to the serial console port of the Cyphercell, administrators should ensure that the modem used meets the equivalent rating of the Cyphercell. If this is not the case, this may compromise the security of the Cyphercell and the protected network.

b) Ensure that a valid X.509 certificate is loaded into a Cyphercell unit before operational use to facilitate secure transmission of data with other Cyphercell units.

c) Maintenance and regular examination of audit logs in accordance with a defined network security policy to detect security related events.

d) Define appropriate roles concerning access control of the Cyphercell units. It is recommended that the following roles are defined:

i. Administrator who has full access rights.

ii. Supervisor who has full access rights except they cannot add, delete or modify user accounts and they cannot install X.509 certificates; and

iii. Operators who have read only access to all available information.

4.9 To ensure correct installation and configuration of the TOE, it is recommended that the Administrator of the TOE possess:

e) An understanding of the security policies and environmental assumptions as specified in the Security Target (section 3, ref [9]). This section mandates organisational security policies with respect to the use of cryptographic functionality, traffic filtering and administrator roles.

f) A knowledge of the ATM protocol and its limitations. Administrators need to be aware of this factor in the application of the organisational security policies stated above.

Availability considerations of the Cyphercell

4.10 Administrators should note that the evaluation did not include any threats to the availability of the Cyphercell. If the IP address of the Cyphercell is changed, remote management of the device is disrupted, as the CypherManager can not locate the Cyphercell. While this type of threat does not invalidate any security objectives of the TOE, administrators should ensure that the Cyphercell is located in a secure facility to prevent this possible attack.

Operational Considerations

4.11 Administrators need to ensure that the console equipment and the Cyphercell unit are co-located in a secure area. If these considerations are not met it is possible for an attacker to potentially monitor the console connection, whether it is through the serial port or an unencrypted modem link. Please note that TOE security environment assumptions outlined in the Security Target (ref [9]) stipulate that appropriate measures must be taken to reduce the likelihood of this type of threat being realised.

4.12 Administrators should ensure that a Virtual Channel Identifier (VCI) of no larger than 65,535 is to be entered into the Virtual Channel Action Table (VCAT) of the CypherManager. If an administrator attempts to delete this entry, they will be unable to do so as the TOE will incorrectly indicate that entry has been deleted.

4.13 Administrators need to be aware that configuration of the VCAT **must** be performed after setting the time on the Cyphercell internal time source. If the time source of the Cyphercell has been adjusted after the VCAT has been configured, VCIs will be unable to provide the correct access defined in the VCAT. It is recommended that Administrators follow the procedures outlined in the Getting Started Guide (ref [11]) to counter this problem.

Appendix A References

[1] AISEP Publication 1 - Description of the AISEP
Defence Signals Directorate
AP 1, Issue 2.0, January 2000

[2] Evaluation Memorandum No. 2 - The Licensing of AISEFs
Defence Signals Directorate
EM 2, Issue 1.0, August 1994

[3] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model (CC)
CCIMB-99-031, Version 2.1, August 1999

[4] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements
CCIMB-99-032, Version 2.1, August 1999

[5] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements
CCIMB-99-033, Version 2.1, August 1999

[6] Common Methodology for Information Technology Security Evaluation (CEM)
CEM-99/045, Version 1.0, August 1999

[7] Manual of Computer Security Evaluation Part I - Evaluation Procedures
Defence Signals Directorate
EM 4, Issue 1.0, April 1995
(EVALUATION-IN-CONFIDENCE)

[8] Manual of Computer Security Evaluation Part II - Evaluation Techniques and Tools
Defence Signals Directorate
EM 5, Issue 1.0, April 1995
(EVALUATION-IN-CONFIDENCE)

[9] Security Target for Cyphercell ATM Encryptor
CTAM Pty Ltd
Version 2.9, 31 January 2001

[10] Evaluation Technical Report for the CTAM Cyphercell 155 ATM Encryptor
CSC Australia Pty Ltd

Issue 2.0, April 2001.
(EVALUATION-IN-CONFIDENCE)

[11] Cyphercell ATM - Getting Started Manual
CTAM Pty Ltd
Version 1.0, 27 March 2000

[12] Cyphercell ATM Getting Started Guide
CTAM Pty Ltd
Version 1.5, 15 December 2000

[13] CypherManager - Installation and User Guide, SNMPv3 Management System for Cyphercell ATM Encryptors
CTAM Pty Ltd
Version 1.2, 15 November 2000

[14] Cyphercell.hlp (electronic help file) with CypherManager v 3.2.0
CTAM Pty Ltd

[15] Cyphercell ATM Encryptor - Security Policy Model ADV_SPM.1
CTAM Pty Ltd
Version 1.4, 27 September 2000
(COMMERCIAL-IN-CONFIDENCE)

[16] Information Technology Security Evaluation Methodology (ITSEM)
Commission of the European Communities
Version 1.0, 10 September 1993

[17] Australian Communications-Electronic Security Instruction (ACSI) 33,
Defence Signals Directorate

[18] Arrangement on the Recognition of Common Criteria Certificates (in the field Information Technology Security)
Available from: http://www.commoncriteria.org/registry/ccra-final.html
May 2000

Appendix B Summary of the Security Target

Security Target

B.1 A brief summary of the Security Target is given below. Potential purchasers should attempt to obtain a copy of the full Security Target to ensure that the TOE security functionality satisfies the requirements of their security policy.

Security Objectives for the TOE

B.2 The Cyphercell and CypherManager has the following IT security objectives:

a) The TOE must provide functionality which enables an authorised user to effectively manage the TOE and its security functions, and must ensure that only authorised users are able to access such functionality, while also maintaining confidentiality of sensitive management data.

b) The TOE must provide a means of recording any security relevant events, so as to assist an authorised user in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack, and also to hold users accountable for any actions that they perform that are relevant to security.

c) The TOE must provide authorised users with the means of controlling traffic flow, on the basis of ATM header information, in accordance with the set of rules defined in the P.FILTER security policy.

d) The TOE must provide the means of protecting the confidentiality of information transferred across a public ATM network between two ATM switches.

e) The TOE must uniquely identify all users, and must authenticate the claimed identity before granting a user access to the TOE management facilities.

f) The TOE must prevent users from gaining access to, and performing operations, on its resources for which their role is not explicitly authorised.

g) The TOE must provide the means for exchanging keys with only another authorised TOE.

h) The TOE must provide the means for generating signed X.509 certificates.

Security Objectives for the Environment

B.3 The Cyphercell and CypherManager has the following environmental objectives:

a) Authorised users of the TOE must ensure that audit facilities are used and managed effectively. In particular:

i) Appropriate action must be taken to ensure that continued audit logging, e.g. by regular archiving of logs.

ii) Audit logs should be inspected on a regular basis, and appropriate action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future.

b) Those responsible for the management of the TOE must ensure that the authentication data for each account on the TOE is held securely and not disclosed to persons unauthorised to use that account.

c) Those responsible for the TOE must ensure that no connections are provided to outside systems or users that would undermine IT security.

d) Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.

e) Those responsible for the TOE must ensure that those parts of the TOE that are critical to security policy enforcement are protected from physical attack, which might compromise IT security.

f) Those responsible for the TOE are competent to manage the TOE and can be trusted not to deliberately abuse their privileges so as to undermine security.

Secure Usage Assumptions

B.4 The following assumptions relate to the operation of the TOE:

a) Each unit has a valid X.509 certificate loaded into the unit before commencement of secure operation. The Cyphercell encryptor cannot operate securely without a valid X.509 certificate loaded in the TOE.

b) It is assumed that a password used to protect the private key of the CypherManager remote management station is restricted to only Administrators of the Cyphercell ATM encryptor. Users other than administrators could attempt to use the key to sign

X.509 certificate requests, if they could recover the CypherManager private key.

c) Only encryption of the ATM cell payloads is required and that single DES or triple DES in cipher block chaining mode, cipher feedback mode or counter mode is appropriate for the classification of information to be protected. DSD determines the appropriateness of cryptographic mechanisms and their suitability to protect classified information.

d) It is assumed that a communications pathway exists for each virtual circuit or path, for automated key exchange using RSA public key cryptography, to transfer an initial master key and session key between units, and that RSA public key cryptography is appropriate for transfer of keys between units. Exchange of session keys, based on time or number of cells encrypted, is set in accordance with the defined network security policy. DSD determines the appropriateness of cryptographic mechanisms and their suitability to protect classified information.

e) It is assumed that X.509 certificate based authentication is appropriate for authentication of RSA key exchange. Correctly implemented X.509 certificate based authentication provides a stronger authentication mechanism than password based authentication mechanisms.

f) Access control rules on the cell traffic, determined by the VPI/VCI address, which forms part of the cell header are defined, and that the rules to be applied are configured for each VPI/VCI address value and set in accordance with the defined network security policy. Defining access control rules that do not comply with the defined network security policy may result in an insecure network. The access control rules that can be applied are encrypt, bypass (the cell passes through unchanged) or discard. Additionally, for each VPI/VCI address an access time period can be set with cells received outside this time period being discarded.

g) It is assumed that appropriate audit logs are maintained and regularly examined in accordance with network security policy. Without capturing security relevant events or performing regular examination of audit records, a compromise of security may go undetected.

h) It is assumed there is as administrator who is responsible for controlling who has access to the unit for configuration and monitoring activities through use of defined roles. There are three roles: administrator who has full access rights; supervisor who has full access rights except they cannot add, delete or modify administrator accounts and they cannot install X.509 certificates; and operator who can view all available information but cannot delete, add or modify the information. Each user is allocated a user name and authentication and privacy passwords and an appropriate role.

Having defined roles provides a means of limiting access to security functions of the TOE to only those authorised users who need to access those security functions.

i) It is assumed that a console port or remote secure SNMPv3 management station is provided for managing the security features of the TOE. A means of securely managing the TOE must be provided to control its security features.

j) It is assumed that Cyphercell is installed between the secure local ATM switch and an insecure network switch. Cyphercell needs to be installed between a secure ATM switch and the insecure ATM network to ensure confidentiality of transmitted information.

k) It is assumed that only the CypherManager management station is used for remote management of the Cyphercell. Other unevaluated SNMPv3 remote management products cannot be relied upon to provide a secure session or to format commands changing Cyphercell security parameters correctly. If remote management is required then the dedicated Ethernet management port on the unit must be connected to an IP network that has connectivity to the management station.

l) It is assumed that CypherManager will be installed on a PC with the following minimum system configuration:

i) Windows 95/ 98/ NT 4.0/ 2000 or higher

ii) 166MHz or higher speed processor

iii) 64 MB of memory

iv) Hard disk drive with a minimum of 5MB of available application space

v) CD drive for installation

vi) 3.5" floppy drive for RSA private key backup

vii) SVGA or better display resolution

viii) Mouse or other pointing device

ix) Network adapter card

x) TCP/IP connectivity.

m) It is assumed that the IP network connected to the dedicated Ethernet management port is capable of passing the SNMPv3 packets used to securely manage remote Cyphercell encryptors. For example, some networks protected by a firewall may implement security policies that restrict the passage of SNMPv3 packets into and out of the protected network. In this case, either SNMPv3 packets must be allowed through the firewall or the console port management functions must be used.

n) Any other system with which the TOE communicates are assumed to operate under the same security policy constraints, otherwise the confidentiality of the information sent to/from a remote instance of the TOE could not be assured.

o) It is assumed that the Cyphercell is located in a secure area at the boundary of the site to be protected. It is required to be in a secure area to ensure that the unit is not physically bypassed.

p) CypherManager is assumed to be located within controlled access facilities, which will aid in preventing unauthorised users from attempting to compromise the security functions of the TOE. For example, unauthorised physical access to the private key used to sign Cyphercell X.509 certificates.

q) It is assumed that one or more administrators, together with any other supervisors or operators, who are assigned as authorised users are competent to manage the TOE, and who can be trusted not to deliberately abuse their privileges so as to undermine security.

r) Attackers are assumed to have a high level of expertise and resources and a low level of motivation. An attacker with a high level of expertise, resources and motivation would be able to gain access to the transmitted information given a sufficient amount of time.

Threats addressed by the TOE and the TOE Environment.

B.5 The following threats are addressed by both the TOE and the TOE Environment:

a) An attacker may eavesdrop on or otherwise capture data being transmitted across a public ATM network in order to recover information that was to be kept confidential.

b) An attacker (insider or outsider) may attempt to make unauthorised connections to another ATM network and transmit information that was to be kept confidential, to another destination.

c) An undetected compromise of information that may occur as a result of an authorised user of the TOE (intentionally or otherwise) performing actions the individual is authorised to perform.

d) An undetected compromise of information may occur as a result of an attacker (insider or outsider) attempting to perform actions that the individual is not authorised to perform.

e) An attacker (outsider or insider) may impersonate an authorised user of the TOE to gain access to transmitted information that was to be kept confidential.

f) An attacker may be able to observe multiple uses of services by an entity and, by linking these uses, be able to deduce information, which the entity wishes to be kept confidential.

g) An attacker could observe the legitimate use of the remote management service by an authorised user when that authorised user wishes their use of that remote management service to be kept confidential.

h) A compromise of information may occur as a result of actions taken by careless, willfully negligent or hostile administrators or other authorised users.

Threats addressed by the TOE Environment

B.6 The following threats are addressed exclusively by the TOE Environment:

a) Security critical parts of the TOE may be subject to physical attack, which may compromise security.

Organisational Security Policies

B.7 The following Organisational Security Policies are addressed by the TOE:

a) All encryption services including confidentiality, authentication, key generation and key management must conform to standards specified by the Defence Signals Directorate for the protection of nationally classified information up to and including RESTRICTED and all levels of nationally sensitive classified information.

b) Traffic flow is controlled on the basis of the information in the ATM cell header, the VCAT and the granting, by an authorised user, of explicit access controls. Any ATM cells, for which there is no VCAT entry, are discarded. By default, all ATM cells are discarded. This Organisational Security Policy must conform to the Cell Control SFP enforced by the TOE as defined in ADV_SPM.1 (Informal TOE security policy model). The P.FILTER OSP ensures that the correct protective action is applied to any given ATM cell received by the TOE.

c) Administration of the TOE is controlled through the definition of roles, which assign different privilege levels to different types of authorised users (administrators, supervisors, and operators). This Organisational Security Policy must conform to the *Remote Management Access Control SFP* and the *Local Management Access Control SFP* enforced by the TOE as defined in ADV_SPM.1 (Informal TOE security policy model). The P.ROLES OSP ensures that administration of the TOE is performed in accordance with the concept of *least privilege*.

Summary of TOE Security Functional Requirements

B.8 The TOE security functional requirements (SFRs) for the Cyphercell are tabulated below. Full description and explanation of these SFRs can be found in section 5.1 of the Security Target (ref [9]).

Class FAU: Audit

FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit Review

Class FCS: Cryptographic Support

FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation

Class FDP: User Data Protection

FDP_DAU.1	Basic data authentication
FDP_UCT.1	Basic data exchange confidentiality
FDP_ACC.1	Subset access control

FDP_ACF.1	Security attribute based access control

Class FIA: Identification and Authentication

FIA_UID.1	Timing of identification
FIA_UAU.2	User authentication before any action

Class FMT: Security Management

FMT_MTD.1	Management of TSF data
FMT_SMR.1	Security roles
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialisation

Class FPT: Protection of the TSF

FPT_AMT.1	Abstract machine testing
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_PHP.3	Resistance to physical attack
FPT_STM.1	Reliable time stamps

Class FTP: Trusted Path/Channels

FTP_ITC.1	Inter-TSF trusted channel

B.9 The TOE security functional requirements (SFRs) for the CypherManager are tabulated below. Full description and explanation of these SFRs can be found in section 5.1 of the Security Target (ref [9]).

Class FCS: Cryptographic Support

FCS_COP.1	Cryptographic operation
FCS_CKM.1	Cryptographic key generation

Class FDP: User Data Protection

FDP_DAU.1	Basic data authentication

Class FPT: Protection of the TSF

FPT_ITT.1	Basic internal TSF data transfer protection

Security Requirements for the IT Environment

B.10 In the absence of appropriate physical access controls, the private key used to sign X.509 certificates must be held in a secure environment.

Security Requirements for the Non-IT Environment

B.11 There are no identified Security Requirements for the non-IT Environment.

Summary of TOE Security Functionality

B.12 The Cyphercell and CypherManager TSFs are briefly listed below. Full description and explanation of these TSFs can be found in section 6.1 of the Security Target (ref [9]).

Cell Control

B.13 This TOE Security Function is achieved by the following functions:

FDP_ACC.1.1.A	Subset access control
FDP_ACF.1.1.A	Security attribute based access control
FDP_ACF.1.2.A	Security attribute based access control

FDP_ACF.1.3.A	Security attribute based access control
FDP_ACF.1.4.A	Security attribute based access control
FMT_MSA.1.1.A	Management of security attributes
FMT_MSA.2.1	Secure security attributes
FMT_MSA.3.1.A	Static attribute initialisation
FMT_MSA.3.2	Static attribute initialisation
FPT_STM.1.1	Reliable time stamps

Key Management

B.14 This TOE Security Function is achieved by the following functions:

FCS_CKM.1.1.A	Cryptographic key generation
FCS_CKM.1.1.B	Cryptographic key generation
FCS_CKM.1.1.C	Cryptographic key generation
FCS_CKM.2.1	Cryptographic key distribution
FCS_CKM.4.1	Cryptographic key destruction
FCS_COP.1.1.B	Cryptographic operation
FCS_COP.1.1.C	Cryptographic operation
FCS_COP.1.1.D	Cryptographic operation
FCS_COP.1.1.E	Cryptographic operation
FDP_DAU.1.1	Basic data authentication
FDP_DAU.1.2	Basic data authentication

Identification and Authentication

B.15 This TOE Security Function is achieved by the following functions:

FIA_UAU.2.1	User authentication before any action
FIA_UID.2.1	User identification before any action
FMT_MTD.1.1	Management of TSF data

Role Based Access

B.16 This TOE Security Function is achieved by the following functions:

FDP_ACC.1.1.B	Subset access control
FDP_ACC.1.1.C	Subset access control
FDP_ACF.1.1.B	Security attribute based access control
FDP_ACF.1.1.C	Security attribute based access control
FDP_ACF.1.2.B	Security attribute based access control
FDP_ACF.1.2.C	Security attribute based access control
FDP_ACF.1.3.B	Security attribute based access control
FDP_ACF.1.3.C	Security attribute based access control
FDP_ACF.1.4.B	Security attribute based access control
FDP_ACF.1.4.C	Security attribute based access control
FMT_MSA.1.1.B	Management of security attributes
FMT_MSA.1.1.C	Management of security attributes
FMT_MSA.2.1	Secure security attributes
FMT_MSA.3.1.B	Static attribute initialisation
FMT_MSA.3.1.C	Static attribute initialisation

FMT_MSA.3.2	Static attribute initialisation
FMT_MTD.1.1	Management of TSF data
FMT_SMR.1.1	Security roles
FMT_SMR.1.2	Security roles

SNMP

B.17 This TOE Security Function is achieved by the following functions:

FCS_COP.1.1.E	Cryptographic operation
FPT_ITT.1.1	Basic internal TSF data transfer protection

Encryption

B.18 This TOE Security Function is achieved by the following functions:

FCS_COP.1.1.A	Cryptographic operation
FDP_UCT.1.1	Basic data exchange confidentiality
FTP_ITC.1.1	Inter-TSF trusted channel
FTP_ITC.1.2	Inter-TSF trusted channel
FTP_ITC.1.3	Inter-TSF trusted channel

Audit

B.19 This TOE Security Function is achieved by the following functions:

FAU_GEN.1.1	Audit data generation
FAU_GEN.1.2	Audit data generation
FAU_SAR.1.1	Audit review
FAU_SAR.1.2	Audit review

FPT_STM.1.1	Reliable time stamps

Self Protect

B.20 This TOE Security Function is achieved by the following functions:

FCS_COP.1.1.E	Cryptographic operation
FPT_AMT.1.1	Abstract machine testing
FPT_PHP.3.1.A	Resistance to physical attack
FPT_PHP.3.1.B	Resistance to physical attack

Appendix C Evaluated Configuration

Configuration for Evaluation

C.1 The evaluation was conducted on the Cyphercell, Version 1.2.1 and CypherManager, Version 3.2.0. The evaluated software and hardware components of the Cyphercell and CypherManager have been identified below.

Software

C.2 The software elements of Cyphercell and CypherManager are as follows:

a) 1 x CDROM containing the **CypherManager Software, Version 3.2.0**, model number S1001A001.

b) The evaluated components of the **Cyphercell** are as follows.

i) **Cyphercell Software, Version 1.2.1**, for the following model numbers:

A1111A002	A1221A002	A1121A002	A1113A002	A1223A002	A1123A002
A1333A002	A1114A002	A1224A002	A1124A002	A1334A002	A1444A002
A1115A002	A1225A002	A1125A002	A1335A002	A1445A002	A1116A002
A1226A002	A1126A002	A1336A002	A1446A002	A1117A002	A1227A002
A1127A002	A1337A002	A1447A002	A1557A002	A1667A002	A1040A001

ii) **Cyphercell Software, Version 1.0**, for model number A1040A001.

Note: Users are advised that the developer prior to customer delivery installs the Cyphercell Software

Third Party Software

C.3 The third party software used in the evaluation of the CypherManager is as follows. Note, that the following software does not contribute to the security functionality implemented by the CypherManager:

a) Windows 95;

b) Windows 98;

c) Windows NT 4.0 with Service Pack 6a; or

d) Windows 2000 with Service Pack 1.

C.4 This evaluation is only valid for the above-mentioned version of CypherManager running on the above Windows operating systems, with the stated service pack applied. No other versions, operating systems or third party software are part of the evaluated configuration.

Hardware

C.5 A single configuration of the Cyphercell requires at least one of the following hardware platforms:

a) Model Number A1111A002, Cyphercell 155 ATM Encryptor, OC3/STM-1 Multimode Fibre Network Interface, DES Algorithm 155Mbps throughput, 1024 virtual circuits;

b) Model Number A1111A002, Cyphercell 155 ATM Encryptor, OC3/STM-1 Multimode Fibre Local Interface, DES Algorithm 155Mbps throughput, 1024 virtual circuits;

c) Model Number A1221A002, Cyphercell 155 ATM Encryptor, OC3/STM-1 Singlemode Fibre Network Interface, DES Algorithm 155Mbps throughput, 1024 virtual circuits;

d) Model Number A1221A002, Cyphercell 155 ATM Encryptor, OC3/STM-1 Singlemode Fibre Local Interface, DES Algorithm 155Mbps throughput, 1024 virtual circuits;

e) Model Number A1121A002, Cyphercell 155 ATM Encryptor, OC3/STM-1 Singlemode Fibre Network Interface, DES Algorithm 155Mbps throughput, 1024 virtual circuits;

f) Model Number A1121A002, Cyphercell 155 ATM Encryptor, OC3/STM-1 Multimode Fibre Local Interface, DES Algorithm 155Mbps throughput, 1024 virtual circuits;

g) Model Number A1113A002, Cyphercell 45 ATM Encryptor, OC3/STM-1 Multimode Fibre Network Interface, DES Algorithm 45Mbps throughput, 1024 virtual circuits;

h) Model Number A1113A002, Cyphercell 45 ATM Encryptor, OC3/STM-1 Multimode Fibre Local Interface, DES Algorithm 45Mbps throughput, 1024 virtual circuits;

i) Model Number A1223A002, Cyphercell 45 ATM Encryptor, OC3/STM-1 Singlemode Fibre Network Interface, DES Algorithm 45Mbps throughput, 1024 virtual circuits;

j) Model Number A1223A002, Cyphercell 45 ATM Encryptor, OC3/STM-1 Singlemode Fibre Local Interface, DES Algorithm 45Mbps throughput, 1024 virtual circuits;

k) Model Number A1123A002, Cyphercell 45 ATM Encryptor, OC3/STM-1 Multimode Fibre Network Interface, DES Algorithm 45Mbps throughput, 1024 virtual circuits;

l) Model Number A1123A002, Cyphercell 45 ATM Encryptor, OC3/STM-1 Multimode Fibre Network Interface, DES Algorithm 45Mbps throughput, 1024 virtual circuits;

m) Model Number A1333A002, Cyphercell 45 ATM Encryptor, T3 BNC Network Interface, DES Algorithm 45Mbps throughput, 1024 virtual circuits;

n) Model Number A1333A002, Cyphercell 45 ATM Encryptor, T3 BNC Local Interface, DES Algorithm 45Mbps throughput, 1024 virtual circuits;

o) Model Number A1114A002, Cyphercell 34 ATM Encryptor, OC3/STM-1 Multimode Fibre Network Interface, DES Algorithm 34Mbps throughput, 1024 virtual circuits;

p) Model Number A1114A002, Cyphercell 34 ATM Encryptor, OC3/STM-1 Multimode Fibre Local Interface, DES Algorithm 34Mbps throughput, 1024 virtual circuits;

q) Model Number A1224A002, Cyphercell 34 ATM Encryptor, OC3/STM-1 Singlemode Fibre Network Interface, DES Algorithm 34Mbps throughput, 1024 virtual circuits;

r) Model Number A1224A002, Cyphercell 34 ATM Encryptor, OC3/STM-1 Singlemode Fibre Local Interface, DES Algorithm 34Mbps throughput, 1024 virtual circuits;

s) Model Number A1124A002, Cyphercell 34 ATM Encryptor, OC3/STM-1 Singlemode Fibre Network Interface, DES Algorithm 34Mbps throughput, 1024 virtual circuits;

t) Model Number A1124A002, Cyphercell 34 ATM Encryptor, OC3/STM-1 Multimode Fibre Local Interface, DES Algorithm 34Mbps throughput, 1024 virtual circuits;

u) Model Number A1334A002, Cyphercell 34 ATM Encryptor, T3 BNC Network Interface, DES Algorithm 34Mbps throughput, 1024 virtual circuits;

v) Model Number A1334A002, Cyphercell 34 ATM Encryptor, T3 BNC Local Interface, DES Algorithm 34Mbps throughput, 1024 virtual circuits;

w) Model Number A1444A002, Cyphercell 34 ATM Encryptor, E3 BNC Network Interface, DES Algorithm 34Mbps throughput, 1024 virtual circuits;

x) Model Number A1444A002, Cyphercell 34 ATM Encryptor, E3 BNC Local Interface, DES Algorithm 34Mbps throughput, 1024 virtual circuits;

y) Model Number A1115A002, Cyphercell 25 ATM Encryptor, OC3/STM-1 Multimode Fibre Network Interface, DES Algorithm 25Mbps throughput, 1024 virtual circuits;

z) Model Number A1115A002, Cyphercell 25 ATM Encryptor, OC3/STM-1 Multimode Fibre Local Interface, DES Algorithm 25Mbps throughput, 1024 virtual circuits;

aa) Model Number A1225A002, Cyphercell 25 ATM Encryptor, OC3/STM-1 Singlemode Fibre Network Interface, DES Algorithm 25Mbps throughput, 1024 virtual circuits;

bb) Model Number A1225A002, Cyphercell 25 ATM Encryptor, OC3/STM-1 Singlemode Fibre Local Interface, DES Algorithm 25Mbps throughput, 1024 virtual circuits;

cc) Model Number A1125A002, Cyphercell 25 ATM Encryptor, OC3/STM-1 Singlemode Fibre Network Interface, DES Algorithm 25Mbps throughput, 1024 virtual circuits;

dd) Model Number A1125A002, Cyphercell 25 ATM Encryptor, OC3/STM-1 Multimode Fibre Local Interface, DES Algorithm 25Mbps throughput, 1024 virtual circuits;

ee) Model Number A1335A002, Cyphercell 25 ATM Encryptor, T3 BNC Network Interface, DES Algorithm 25Mbps throughput, 1024 virtual circuits;

ff) Model Number A1335A002, Cyphercell 25 ATM Encryptor, T3 BNC Local Interface, DES Algorithm 25Mbps throughput, 1024 virtual circuits;

gg) Model Number A1445A002, Cyphercell 25 ATM Encryptor, E3 BNC Network Interface, DES Algorithm 25Mbps throughput, 1024 virtual circuits;

hh) Model Number A1445A002, Cyphercell 25 ATM Encryptor, E3 BNC Local Interface, DES Algorithm 25Mbps throughput, 1024 virtual circuits;

ii) Model Number A1116A002, Cyphercell 8 ATM Encryptor, OC3/STM-1 Multimode Fibre Network Interface, DES Algorithm 8Mbps throughput, 1024 virtual circuits;

jj) Model Number A1116A002, Cyphercell 8 ATM Encryptor, OC3/STM-1 Multimode Fibre Local Interface, DES Algorithm 8Mbps throughput, 1024 virtual circuits;

kk) Model Number A1226A002, Cyphercell 8 ATM Encryptor, OC3/STM-1 Singlemode Fibre Network Interface, DES Algorithm 8Mbps throughput, 1024 virtual circuits;

ll) Model Number A1226A002, Cyphercell 8 ATM Encryptor, OC3/STM-1 Singlemode Fibre Local Interface, DES Algorithm 8Mbps throughput, 1024 virtual circuits;

mm) Model Number A1126A002, Cyphercell 8 ATM Encryptor, OC3/STM-1 Singlemode Fibre Network Interface, DES Algorithm 8Mbps throughput, 1024 virtual circuits;

nn) Model Number A1126A002, Cyphercell 8 ATM Encryptor, OC3/STM-1 Multimode Fibre Local Interface, DES Algorithm 8Mbps throughput, 1024 virtual circuits;

oo) Model Number A1336A002, Cyphercell 8 ATM Encryptor, T3 BNC Network Interface, DES Algorithm 8Mbps throughput, 1024 virtual circuits;

pp) Model Number A1336A002, Cyphercell 8 ATM Encryptor, T3 BNC Local Interface, DES Algorithm 8Mbps throughput, 1024 virtual circuits;

qq) Model Number A1446A002, Cyphercell 8 ATM Encryptor, E3 BNC Network Interface, DES Algorithm 8Mbps throughput, 1024 virtual circuits;

rr) Model Number A1446A002, Cyphercell 8 ATM Encryptor, E3 BNC Local Interface, DES Algorithm 8Mbps throughput, 1024 virtual circuits;

ss) Model Number A1117A002, Cyphercell 2 ATM Encryptor, OC3/STM-1 Multimode Fibre Network Interface, DES Algorithm 2Mbps throughput, 1024 virtual circuits;

tt) Model Number A1117A002, Cyphercell 2 ATM Encryptor, OC3/STM-1 Multimode Fibre Local Interface, DES Algorithm 2Mbps throughput, 1024 virtual circuits;

uu) Model Number A1227A002, Cyphercell 2 ATM Encryptor, OC3/STM-1 Singlemode Fibre Network Interface, DES Algorithm 2Mbps throughput, 1024 virtual circuits;

vv) Model Number A1227A002, Cyphercell 2 ATM Encryptor, OC3/STM-1 Singlemode Fibre Local Interface, DES Algorithm 2Mbps throughput, 1024 virtual circuits;

ww) Model Number A1127A002, Cyphercell 2 ATM Encryptor, OC3/STM-1 Singlemode Fibre Network Interface, DES Algorithm 2Mbps throughput, 1024 virtual circuits;

xx) Model Number A1127A002, Cyphercell 2 ATM Encryptor, OC3/STM-1 Multimode Fibre Local Interface, DES Algorithm 2Mbps throughput, 1024 virtual circuits;

yy) Model Number A1337A002, Cyphercell 2 ATM Encryptor, T3 BNC Network Interface, DES Algorithm 2Mbps throughput, 1024 virtual circuits;

zz) Model Number A1337A002, Cyphercell 2 ATM Encryptor, T3 BNC Local Interface, DES Algorithm 2Mbps throughput, 1024 virtual circuits;

aaa) Model Number A1447A002, Cyphercell 2 ATM Encryptor, E3 BNC Network

Interface, DES Algorithm 2Mbps throughput, 1024 virtual circuits;

bbb) Model Number A1447A002, Cyphercell 2 ATM Encryptor, E3 BNC Local Interface, DES Algorithm 2Mbps throughput, 1024 virtual circuits;

ccc) Model Number A1557A002, Cyphercell 2 ATM Encryptor, E1 BNC Network Interface, DES Algorithm 2Mbps throughput, 1024 virtual circuits;

ddd) Model Number A1557A002, Cyphercell 2 ATM Encryptor, E1 BNC Local Interface, DES Algorithm 2Mbps throughput, 1024 virtual circuits;

eee) Model Number A1667A002, Cyphercell 2 ATM Encryptor, T1 RJ45 Network Interface, DES Algorithm 2Mbps throughput, 1024 virtual circuits;

fff) Model Number A1667A002, Cyphercell 2 ATM Encryptor, T1 RJ45 Local Interface, DES Algorithm 2Mbps throughput, 1024 virtual circuits; and

ggg) Model Number A1040A001, which adds unlimited VPI/VCI mapping option, and a maximum of 65,536 virtual circuits.

C.6 Please note that the hardware identified above implements some of the security functionality offered by the Cyphercell. The minimum recommended hardware configurations for the above hardware platforms are located in section 1.1 of the Security Target (ref [9]).

Procedures for Determining Version of TOE

C.7 In order that an administrator can determine if a delivered product is in fact the evaluated product, the following procedures can be followed in making that determination.

Note: Potential Purchasers of the TOE should be aware that the Cyphercell product is sent independently of the CypherManager.

Procedures for Determining the Cyphercell

C.8 Once a copy of the Cyphercell has been received, the administrator should compare information on the label on the external packaging with the Order Acknowledgement form. This form is sent independently when the order is placed and includes the order number, model number, serial number and client's name.

C.9 The administrator should then check that the model number and the serial number labelled on the Cyphercell match the information provided on the Order Acknowledgement form.

C.10 The administrator should inspect the packaging for any signs of tampering. Once it has been determined that Cyphercell has been delivered intact, the Administrator should then check the tamper evident seals on the side and the base of the unit. Any indication of tampering should be reported immediately to CTAM Pty Ltd and the product returned.

Procedures for Determining the CypherManager

C.11 Once a copy of the CypherManager has been received, the administrator should compare information on the label on the external packaging with the Order Acknowledgement form. This form was sent when the order was placed and includes a random shipment number and client's name.

C.12 The administrator should inspect the packaging for any signs of tampering. Once it has been determined that the packaging of the CypherManager has been delivered intact, the Administrator should check the tamper seals on the envelope containing the CypherManager software. Any indication of tampering should be reported immediately to CTAM Pty Ltd and the product returned.

C.13 Operational documentation is delivered in hard and soft copy with the CD-ROM. Administrators of the CypherManager are advised to ensure that the soft copies of the operational documentation (refs [11] - [13]) are identical to the supplied hard copies. If not, the administrators should report the discrepancy back to CTAM immediately.