Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2008/47

11 August 2008

Version 1.0

Commonwealth of Australia 2008.

Reproduction is authorised provided
that the report is copied in its entirety.

Amendment Record

Version	Date	Description
0.1	09/07/2008	Internal release for review
0.2	01/08/2008	Extended review.
1.0	11/08/2008	Public release.

Executive Summary

1 SafeNet ProtectDrive v8.1.1 is a software product that is designed to provide protection of sensitive information on laptops and workstations. SafeNet ProtectDrive v8.1.1 is the Target of Evaluation (TOE).

2 This report describes the findings of the IT security evaluation of SafeNet Inc's SafeNet ProtectDrive v8.1.1, to the Common Criteria (CC) evaluation assurance level EAL 4. The report concludes that the product has met the target assurance level of EAL 4 and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by Logica and was completed in June 2008.

3 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that:

a) only use the TOE in its evaluated configuration (the default installation), ensuring that the assumptions concerning the TOE security environment are fulfilled;

b) apply encryption to all fixed media storage partitions;

c) configure the protected device BIOS to only boot from fixed media and apply a supervisor password to the BIOS;

d) enforce access controls over syskey.bin;

e) ensure TOE users are also removed from the preboot user database when the user's Windows account is disabled or removed;

f) if a TOE deployment is being managed from ActiveDirectory:

i) on the PDSettings\Authentication tab, disable Add Users to ProtectDrive on Successful Windows Logon – this will prevent users being added to the preboot user database that are not managed from ActiveDirectory; and

ii) optionally, the administrator may also disable Allow Local User Access on the PDSettings\Authentication tab – this will, however, prevent local recovery functionality if a network connection is not available;

iii) be aware of:

1. the hierarchy of various objects: policies set for an individual computer object will override default policies configured on the user objects; and

2. changes made to a logged on users access rights will not be enforced until that user logs off and on again;

g) restrict Windows user passwords to 20 characters; and

h) a list of tested removable storage media devices is provided in the supported devices section of the release notes.

4 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

5 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target at Ref [1], and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

6 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

7 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, SafeNet ProtectDrive v8.1.1, against the requirements of the Common Criteria (CC) evaluation assurance level EAL 4; and

b) provide a source of detailed security information about the TOE for any interested parties.

8 This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

9 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	SafeNet ProtectDrive v8.1.1
Software Version	V8.1.1
Security Target	Security Target for SafeNet ProtectDrive v8.1.1 dated August 2008
Evaluation Level	EAL 4
Evaluation Technical Report	Evaluation Technical Report for SafeNet ProtectDrive v8.1.1 dated May 2008
Criteria	CC Version 2.3, August 2005.
Methodology	CCMB-2005-08-004.
Conformance	CC Part 2 Conformant

	CC Part 3 Conformant
Sponsor	SafeNet Inc
Developer	SafeNet Inc
Evaluation Facility	Logica

Chapter 2 - Target of Evaluation

2.1 Overview

10 This chapter contains information about the Target of Evaluation (TOE), including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

11 The TOE is called SafeNet ProtectDrive v8.1.1 developed by SafeNet Inc. Its primary role is to provide protection through: encryption of storage devices; pre-boot authentication control; and access control over I/O devices (serial, parallel, floppy drives, CD/DVD drives and removable storage media) that may be attached to the machine on which it is operating.

12 The TOE is a software PC security product that protects the confidentiality of stored information (data at rest) by encrypting the information as it written to the computer's fixed and removable storage media.

13 The TOE is intended to be installed on machines using Microsoft Windows operating systems. The two operating systems within the scope of the TOE are Windows XP Professional SP2 and Windows 2000 Professional SP4. Additional components are provided to manage the TOE configuration from a Windows Active Directory service.

14 The TOE also provides identification and authentication services at boot that integrate with the underlying Windows identification and authentication services to control a user's ability to power on a protected device.

15 The main components that comprise the TOE are:

- a preboot application that extends the computer BIOS (VX BIOS);
- a preboot identification and authentication module (VROM);

- a transparent encryption driver (TED);
- an ActiveDirectory Management Console snap-in; and
- a Local Management Console.

16 The VX BIOS controls access to the device during startup and loads the VROM module.

17 The VROM provides a user identification and authentication interface. This interface allows both user name/password and hardware token/PIN to be used. This module can be configured to provide one time authentication (with administrator intervention) via challenge/response strings.

18 The VROM can be configured to block user input in the case of multiple failed authentication attempts – the time period for the lockout and the number of failed attempts that trigger the lockout can be configured by the TOE administrator.

19 On successful user identification and authentication the PC continues its boot sequence. When Windows is successfully loaded, the Windows GINA is replaced by a custom GINA (PDGINA) which can be configured for single sign-on (by using the authentication credentials obtained by the VROM).

20 The TED is loaded as a background service that intercepts input/output (I/O) calls to provide real time encryption and decryption of data as appropriate. The TED also provides administrator configurable access control over some of the PC's I/O devices and interfaces via the enforcement of read and write permissions (users may have full read/write, read only, or no access to a device).

21 The TOE can be managed locally (via Local Management Console) or remotely (via ActiveDirectory Management Console). This is configurable both during and after the TOE installation.

2.3 Security Policy

22 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The TSP is defined in the Security Target (Ref [1]).

23 A summary of the TOE security policy is as follows:

a) A user has no direct access to objects protected by the TOE, all access to protected objects is performed indirectly via the TOE;

b) Users can perform one of two operations on protected objects via the TOE: read from and write to; and

c) Access to protected objects (via the TOE) is granted only after a user has authenticated to the TOE.

24 Three sets of policy govern operations within the TOE:

1 Identification and Authentication Policy:

- The TOE Security Function (TSF) retrieves and updates attributes for each user from the same data store that contains the rules; some of these attributes may be changed by Administrators via the Secure Administration TSF;
- The TSF requires users to authenticate prior to making any requests;
- The TSF handles failed user authentications, based on administrator configured parameters;
- The TSF permits one time only user authentication with administrator intervention;
- The TSF permits multiple methods of authentication by users; and
- The TSF requires users to be identified prior to making any requests.

2 Default System Policy and Default User Policy:

- The TSF only accepts actions from a subject acting on behalf of an authenticated and authorised user;
- The TSF only accesses object stores that the user making the request is authorised to access;
- The TSF reads encrypted objects from an object store using a key for that object store known only to the TSF;
- The TSF writes encrypted objects to an object store using a key for that object store known only to the TSF;
- The TSF will encrypt an object store using a specified algorithm when required by an administrator;
- The TSF will decrypt an object store when required by an administrator; and
- The TSF will encrypt a removable object store as requested by an authorised user, using an algorithm preset by an administrator.

3 The following security policy set governs the configuration of the TOE:

- The TSF permits only administrative users to configure the rules;

- The TSF specifies most of the values that administrators can select in configuring the TOE; and
- The TSF permits administrators to set what is displayed at startup if the TOE is installed on a system that can run multiple operating systems.

2.4 TOE Architecture

25 The TOE consists of the following major architectural components:

a) User Interface Sub-system;

b) Remote Administrator Interface Sub-system;

c) Local Administrator Interface Sub-system;

d) Data Protection / Service Daemons Sub-system; and

e) Local Data Store Object (and optional Remote Data Store Object).

26 The Developer's Architectural Design identifies the 2 modes of the TOE:

a) Pre boot; and

b) Post boot.

27 The preboot mode of operation provides the preboot authentication and authentication failure lockout functionality. This mode also provides functionality to allow one time authentication in the case of new user introduction to the preboot environment or forgotten password/PIN. These functions generate a random challenge that requires an administrator to generate a valid response (using a supplied administrative tool).

28 In post boot mode, the TOE:

a) transparently (not visible to the user) encrypts and decrypts protected fixed media as required;

b) provides read and write access control over various classes of I/O device (removable media, floppy disk drive, CD/DVD drive, serial and parallel ports) based on administrator set permissions;

c) transparently encrypts and decrypts protected removable storage media as required in accordance with administrator set user permissions;

d) synchronises the local data store with the remote data store (if configured for remote configuration) – the data stores contain the

TOE user names and permissions and the TOE configuration settings; and

e) provides authenticated users with Windows administrator rights access to the administrative interface (if configured for local management) to change the TOE settings (grant/deny user permissions, set default encryption algorithm, set allowed encryption algorithms, configure user recovery options, add new users to preboot authentication database).

2.5 Clarification of Scope

29 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.5.1 Evaluated Functionality

30 The TOE provides the following evaluated security functionality:

a) Cryptographic Support;

b) User Data Protection;

c) Identification and Authentication; and

d) Security Management.

2.5.2 Non-evaluated Functionality

31 Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information and Technology Security Manual (ACSI 33) (Ref [1]) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

32 The functions and services that have not been included as part of the evaluation are provided below:

a) Multiple boot partitions;

b) Operating systems other than Windows XP Professional or Windows2000 Professional; and

c) Single DES CBC and IDEA encryption algorithms; and

d) Server edition components.

2.6 Usage

2.6.1 Evaluated Configuration

33 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in these defined evaluated configuration(s). Australian Government users should refer to ACSI 33 (Ref [1]) to ensure that configuration(s) meet the minimum Australian Government policy requirements. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

34 The TOE consists of SafeNet ProtectDrive v8.1.1. The 2 operating systems within the scope of the TOE for installing on client machines are Windows XP Professional SP2 (Build 5.1.2600) and Windows 2000 Professional SP4 (Build 5.00.2195).

35 Note: The default options install the TOE in an evaluated configuration.

2.6.2 Delivery procedures

36 When placing an order for the TOE the following process must be followed by a customer to receive the TOE in a secure manner:

a) Submit a purchase order to a SafeNet sales representative;

b) SafeNet delivers ProtectDrive v8.1.1 to the customer in tamper-evident shrink-wrapped packaging along with a shipping check-list that identifies the TOE serial number, the original customer purchase order number, and the vendor sales order number. The product is shipped using either a courier or postal service; and

a) A license key required to operate the TOE is emailed to the customer.

37 The customer should check that the shrink-wrapped packaging is intact and shows no sign of tampering to confirm secure delivery of the TOE.

38 Purchasers can verify that they have received the evaluated product by doing the following:

a) Confirm that the purchase order number and sales order number are consistent with the shipping check-list as well as with the customer's records; and

b) Confirm that the CD delivered is labelled as SafeNet ProtectDrive version 8.1.1.

39 If during delivery of the TOE there is any deviation in the above procedure, it is recommended that the customer contact the vendor for further advice.

2.6.3 Evaluated Product Identification and Verification

40 The certificate and signature details for the TOE installation are:

a) Filesize: 12,937,728 bytes - note this is the actual file size obtained from the file properties (i.e. not the size on disk or size reported by Windows explorer);

b) Certificate Serial Number: 46 27 a8 714b 22 b4 61 bd e6 7a de 02 e6 e2 ea;

c) Certificate Thumbprint (SHA1):ea bb a2 cc1e 61 86 9a f8 d1 e1 f0 0b a9 14 20 2a 4e 9f 80;

d) Message Digest (SHA1): 04 14 20 5c 4d 4d e8 f7 5f ad b2 1a 08 ce 67 2f 19 d3 50 cb 1b 05; and

e) Alternatively: Using the Microsoft File Checksum Integrity Verifier utility (http://support.microsoft.com/kb/841290).

2.6.4 Determining the Evaluated Configuration

41 The evaluated TOE configuration used for testing was an out of the box installation with the default settings (as per the Administration Guide (Ref [3]). An administrator can determine the evaluated configuration by physically verifying the settings against the default settings (as per the Administration Guide (Ref [3]).

2.6.5 Documentation

42 It is important that the TOE is used in accordance with guidance documentation in order to ensure the secure usage. The following documentation is provided with the TOE:

a) ProtectDrive Enterprise Version Administrator's Guide Chapter 5, Deploying ProtectDrive (Ref [3]); and

b) ProtectDrive Enterprise Version Administrator's Guide Appendix E, Additional Guidance Regarding Security (Ref [4]).

43 There are a number of configuration options available during the installation of the TOE.

44 The default options install the TOE in an evaluated configuration.

2.6.6 Secure Usage

45 The evaluation of the TOE accounted for certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

46 The following assumptions were made:

a) Administrators:

   i) are trusted not to compromise security;

   ii) are trusted not to abuse their authority;

   iii) are competent to manage the TOE and security of the information it protects;

   iv) follow the policies and procedures defined in the TOE documentation for the secure administration of the TOE; and

   v) follow password management policies to ensure users comply with password policies;

b) Authorised users:

   i) cooperate with those responsible for managing the TOE to maintain TOE security;

   ii) can be trusted and are not considered to be hostile; and

   iii) are fallible and can make errors or act in ways that may compromise security;

c) If the computer containing information protected by the TOE is connected to a network and an authorised user is authenticated to the TOE, then information protected by the TOE may be accessible from the network. To prevent compromise of protected information from a network connection the network must protect information to at least the same degree as that provided by the TOE;

d) It is assumed that:

   i) if the computer, on which the TOE is installed, is connected to a network that the network operates under the same security policy constraints as the TOE;

   ii) if the computer, on which the TOE is installed, is a part of a network domain then the domain operates under the same security policy constraints at the TOE; and

   iii) unauthorised physical tampering with the computer, on which the TOE is active, is clearly evident to users. e.g. the equipment is fitted with tamper evident seals (or similar devices) that provide a clear indication if the equipment has been physically tampered with.

47 The TOE is not designed to comply with any specific organisations security policies.

Chapter 3 - Evaluation

3.1 Overview

48 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

49 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [5], [6], [7]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [8]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [9], [10], [11], [12]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [13]) were also upheld.

3.3 Functional Testing

50 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

51 In addition, a number of independent tests were conducted by the evaluators. These were split into the following 3 categories:

a) Identification and Authentication

i) Confirm that a valid user with the associated valid password can be authenticated by the TOE. Also confirm that a valid user with a valid hardware token and PIN are authenticated.

ii) Confirm that a valid user presenting an invalid password is not authenticated by the TOE. Also confirm that a valid user with valid hardware token and invalid PIN are rejected.

iii) Confirm that an invalid user is not authenticated by the TOE.

iv) Confirm that a delay is invoked after a thresh-hold of failed authentication attempts is exceeded – this will be tested against multiple failed attempts against one user and also against multiple failed attempts with a series of user ids (valid and invalid).

v) Confirm that the delay introduced by the TOE is consistent with that specified in (Ref [1]).

vi) Confirm the operation of the password fallback/password recovery functionality.

b) Secure Administration

i) Confirm that a user without administrator rights cannot change the TOE configuration via the Windows Management Instrumentation (WMI – includes the AD snapin and the local management console).

ii) Determine if a user without administrator rights cannot change the TOE configuration via the supplied command line utilities.

iii) Confirm that a user with administrator rights can change the configuration of the TOE (including add/change rights/remove users, change encryption algorithms, encrypt and decrypt fixed storage media) using the WMI or command line utilities.

c) Data Protection

i) Confirm that the data at rest is obfuscated.

ii) Verify the correctness of encryption algorithms used (this was performed during the DEA visit under the supervision of the evaluators using NIST standard test vectors comprising sets of known plaintext, known key, expected cipher text).

iii) Confirm that an authenticated user can read from and write to the protected storage media.

iv) Confirm that an authenticated user can access removable storage and IO devices in accordance with the defined access permissions for that user. This will be performed by:

a. allowing read/write access;

b. allowing read/blocking writes;

c. blocking read/allowing writes; and

d. blocking read/write access.

v) These tests will be repeated for each of the objects that can be controlled i.e. CD/DVD drive, serial port, parallel port, removable media, floppy diskettes.

vi) Attempt to recover information from a protected device/medium.

3.4 Penetration Testing

52 The evaluators examined the developer's vulnerability analysis to verify that, for every identified vulnerability, a rationale was given why the vulnerability is not exploitable in the intended environment of the TOE. Based on the evaluators examination of the developer's vulnerability analysis, the evaluators developed penetration tests to:

a) disprove the developer's vulnerability analysis; and

b) determine the susceptibility of the TOE to vulnerabilities identified by the developer.

53 After the completion of testing, the evaluators were able to determine that the TOE, in its intended environment, has demonstrated resistance to low attack potential penetration attackers.

Chapter 4 - Certification

4.1 Overview

54 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

55 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [14]), the Australasian Certification Authority certifies the evaluation of SafeNet ProtectDrive v8.1.1 performed by the Australasian Information Security Evaluation Facility, Logica.

56 Logica has found that SafeNet ProtectDrive v8.1.1 upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL 4.

57 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

58 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 though an informal model of the TOE security policy.

59 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional

specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for obvious vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

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

4.4 Recommendations

61 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ACSI 33 (Ref [1]) and New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

62 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Refs [3], [4]), the ACA also recommends that users and administrators:

a) **Configure Hardware.**

i. Commercial off the shelf (COTS) tools are available that allow an attacker to boot into an environment where the TOE is not running. This would allow an attacker access to any unencrypted media on the protected device. To reduce the impact and likelihood of success for this type of attack, it is recommended that:

1. TOE administrators apply encryption to all fixed media storage partitions to reduce the impact of this type of attack; and

2. TOE administrators configure the protected device BIOS to only boot from fixed media and apply a supervisor password to the BIOS.

b) **Enforce access controls over syskey.bin.**

i. An organisation deploying the TOE must ensure that the file syskey.bin is included in the applicable key management plans and access to any copies of the file must be restricted (physically and logically). This file can optionally be encrypted using the TOE utilities to facilitate storage on a shared folder during remote installations; and

ii. The TOE may be installed on multiple hosts using the same syskey.bin/syskey.ske. This advantages of this approach are to

reduce the key management effort (by reducing the amount of key material to manage) and to allow sharing of encrypted removable media between hosts (see Controlling Removable Storage Media below). The risk with this approach is that all hosts installed using a single syskey.bin will affected in the event of this file being compromised.

c) **Disable/Remove TOE Users**.

i. TOE administrators ensure that TOE users are also removed from the preboot user database when the user's Windows account is disabled or removed.

d) **Manage TOE users from a server.**

i. If a TOE deployment is being managed from ActiveDirectory, the following settings should be applied:

1. On the PDSettings\Authentication tab, disable Add Users to ProtectDrive on Successful Windows Logon – this will prevent users being added to the preboot user database that are not managed from ActiveDirectory; and

2. Optionally, the administrator may also disable Allow Local User Access on the PDSettings\Authentication tab – this will, however, prevent local recovery functionality if a network connection is not available.

ii. When managing users from ActiveDirectory – be aware of the hierarchy of the various objects: policies set for an individual computer object will override default policies configured on the user objects; and

iii. Changes made to a logged on user's access rights will not be enforced until that user logs off and on again (even if periodic configuration updates are set in ActiveDirectory). The local management console will display the new rights and permissions for the user when the configuration update is applied, but the user will need to logoff and logon again before those configuration changes are enforced.

e) **Control Removable Storage Media**.

i. Only devices listed in the supported devices section of the release notes (available on the installation CD delivered to the customer) are used within the environment, or configure the TOE to deny access to unencrypted media – dependent on a risk assessment.

f) **Restrict Windows User Passwords to 20 Characters.**

i. ProtectDrive only allows a maximum of 20 character passwords. Therefore to ensure synchronisation with Windows allow a maximum password length of 20 characters for users; This advice is repeated in the Administrator Guide and release notes for v8.2.1 of ProtectDrive but due to the timing of the discovery, is not present in the guidance for v8.1.1 (the TOE).

g) **Use only in its evaluated configuration**.

i. Ensure that the assumptions concerning the TOE security environment, and organisational security policies (Ref [1]) are fulfilled.

Annex A - References and Abbreviations

A.1 References

[1] Security Target for SafeNet ProtectDrive v8.1.1 dated August 2008

[2] Australian Government Information and Communications Technology Security Manual (ACSI 33), March 2005, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] ProtectDrive Enterprise Version Administrator's Guide Chapter 5, Deploying ProtectDrive User Documentation.

[4] ProtectDrive Enterprise Version Administrator's Guide Appendix E, Additional Guidance Regarding Security

[5] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 2.3, August 2005, CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC), Version 2.3, August 2005, CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 2.3, August 2005, CCMB-2005-08-003

[8] Common Methodology for Information Technology Security Evaluation (CEM), Version 1.0, August 2005, CCMB-2005-08-004

[9] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[10] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.0, 21 February 2006, Defence Signals Directorate.

[11] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate

[12] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September 2006, Defence Signals Directorate

[13] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[14] Evaluator Technical Report for SafeNet ProtectDrive v8.1.1 dated 20 June 2008, Logica

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy