Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 36/2005

September 2005

Version 1.0

Amendment Record

Version	Date	Description
1.0	20/9/2005	Public release.

Executive Summary

1 ProtectDrive Version 7.0.3 is a product that is designed to protect the confidentiality of information stored on computer laptops and workstations by encrypting the information as it is written to the computer's hard disk drive. ProtectDrive Version 7.0.3 is the Target of Evaluation (TOE).

2 This report describes the findings of the IT security evaluation of Eracom Technologies Australia Pty Ltd's ProtectDrive Version 7.0.3, to the Common Criteria (CC) evaluation assurance level EAL 2. The report concludes that the product has met the target assurance level of EAL 2 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 LogicaCMG and was completed in August 2005.

3 With regard to the secure operation of the TOE, it is important to ensure that the assumptions concerning the operational environment are fulfilled and the guidance documentation is followed.

4 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 [2]) and New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

5 The Australasian Certification Authority (ACA) also recommends that users and administrators:

a) Disable *Automatic Pre-boot Authentication*;

b) Fully encrypt hard disks;

c) Use the Triple-DES encryption algorithm;

d) Enable the *Show disk not fully encrypted* warning;

e) Lock their computer screens when unattended;

f) Use RSA token keys of size 1024 bits; and

g) Use New Technology File System (NTFS).

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

7 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.

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

Table of Contents

Chapter 1 - Introduction

1.1 Overview

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

1.2 Purpose

10 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, ProtectDrive Version 7.0.3, against the requirements of the Common Criteria (CC) EAL 2 (Evaluation Assurance Level); and

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

11 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

12 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	ProtectDrive Version 7.0.3
Operating System	Microsoft Windows 2000 Professional 5.00.2195 Service Pack 4 and Microsoft Windows XP Professional 5.1.2600 Service Pack 2 Build 2600
Security Target	ProtectDrive Evaluation Security Target Revision: B12
Evaluation Level	EAL 2
Evaluation Technical Report	Eracom ProtectDrive v 7.0.3 Evaluation Technical Report, Issue 1.1, August 2005, ECF8406/T8/1.
Criteria	CC Version 2.1, August 1999, with interpretations as of 24 June 2003
Methodology	CEM-99/045 Version 1.0, August 1999, with interpretations as of 24 June 2003
Conformance	CC Part 2 Conformant CC Part 3 Conformant
Developer	Eracom Technologies Australia Pty Ltd
Evaluation Facility	LogicaCMG

Chapter 2 - Target of Evaluation

2.1 Overview

13 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

14 The TOE is ProtectDrive Version 7.0.3, developed by Eracom Technologies Australia Pty Ltd.

15 ProtectDrive is a software product that provides protection of sensitive information on laptops and workstations. Protection is provided through pre-boot authentication and access control of peripheral devices combined with hard disk encryption.

16 ProtectDrive uses a modified Master Boot Record (MBR) to load its own security functions as the computer is initialising. ProtectDrive's security functions ensure that users are identified and authenticated before access to sensitive information is permitted and before the operating system is loaded. Access control is implemented with User ID and password or Token and PIN.

17 After the initial boot process ProtectDrive provides continued protection by monitoring access through its extensions to the Windows graphical identification and authentication (GINA) library and its Transparent Encryption Driver (TED).

18 ProtectDrive security features also include:

a) Unauthorised sign-on protection activation after three failed sign-on attempts;

b) Previous sign-on display showing the date and time of previous successful sign-on and the details of any unsuccessful attempts since that time when using a User ID and password; and

c) Control of booting from floppy disk after pre-boot authentication occurs.

2.3 Security Policy

19 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]). A summary of the TSP is provided below:

a) **Cryptographic Support**: The TOE provides the ability to generate and destroy cryptographic keys. The TOE can also encrypt and decrypt data using the DES and Triple-DES algorithms. The cryptographic key sizes used are 56 and 112 bits respectively.

b) **User Data Protection**: The TOE enforces a number of access control policies relating to hard disk access, user attributes, and TOE configuration. A user can access protected disk data only if they have successfully authenticated. An authenticated user may also modify their password. An authenticated administrator may modify users' attributes and modify any system configuration properties.

c) **Identification and Authentication**: The TOE requires that users successfully authenticate prior to any other action. If three unsuccessful authentication attempts are made in succession then the TOE will prevent any further authentication attempts for one minute.

d) **Security Management**: The TOE maintains two roles: the Administrator and User. The TOE provides the following security management functions: logon control; authentication options; disk encryption display; and default user permissions.

e) **TOE Access**: Upon successful session establishment, the TOE will display the date and time of the last successful session establishment. The TOE will also provide a history of failed authentication attempts since the last successful authentication.

2.4 TOE Architecture

20 The TOE consists of the following major architectural components:

a) User Interface subsystem; and

b) Data Protection subsystem.

21 The User Interface subsystem consists of the following components:

a) Pre-Boot Authentication: ensures that the user is successfully authenticated prior to starting the operating system, and enforces the access control policy for controlled resources. It also enables the ProtectDrive Transparent Encryption Driver by making available the necessary encryption key.

b) GINA Extension Authentication: displays to the user the time and date of the last successful log on. This component monitors the operating system authentication of a new or the same user after a user has logged off from the operating system. It also synchronises the pre-boot user authentication information when a user's password is changed through the operating system management facilities.

c) Secure Admin: provides tools for administrators to manage user accounts and access attributes. It also manages the TOE configuration by setting the area of the hard disk that will be protected.

22 The Data Protection subsystem encrypts and decrypts data as it is being written to or being read from the hard disk drive. It also enforces the access control policy to the floppy disk, serial and parallel ports.

2.5 Clarification of Scope

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

2.5.1 Evaluated Functionality

24 The TOE provides the following evaluated security functionality:

a) Identification and Authentication – is implemented in the TOE pre-boot module and the GINA extension.

b) Secure Administration – an authenticated administrator can manage user accounts and privileges, and the TOE configuration.

c) Protection of Data – encrypts and decrypts data from the hard drive.

2.5.2 Non-evaluated Functionality

25 Potential users of the TOE are advised that some functions and services in the product 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 the Australian Government Information and Technology Security Manual (ACSI 33) (Ref [2]) 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).

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

a) Server Edition of ProtectDrive;

b) Multiple Boot Manager;

c) Network Installation;

d) IDEA Encryption Algorithms;

e) Password Fallback;

f) Password Recovery; and

g) New User Introduction.

27 Access control to the TOE may be performed using a suitable token for authentication. While the security of a specific token was not part of the evaluation, the Security Target (Ref [1]) describes the requirements that must be provided by a token. These requirements are summarised in Section 2.6.5.

2.6 Usage

2.6.1 Evaluated Configuration

28 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 [2]) to ensure that configuration(s) meet the minimum Australian Government policy requirements. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

29 The TOE is implemented entirely in software and is identified as ProtectDrive 7.0.3. The TOE runs on the following Microsoft operating systems:

a) Windows 2000 Professional, 5.00.2195 Service Pack 4; and

b) Windows XP Professional 5.1.2600 Service Pack 2 Build 2600.

30 The User Guidance (Ref [3]) provides guidance to administrators on configuring the underlying operating system and the installation of the TOE. To summarise, the underlying operating system must be configured as follows:

a) System Password Policy:

i) *Enforce Password History*: 7 passwords.

ii) *Maximum Password Age*: set in accordance with organisational policy.

iii) *Minimum Password Age*: 1 day or greater.

iv) *Minimum Password Length*: 6 characters or greater.

v) *Password Complexity Requirements*: enabled.

vi) *Store Password using Reversible Encryption*: disabled.

b) Screen Lock Feature must be enabled and configured according to organisational policy.

31 The TOE must be configured as follows:

a) *Show Unsuccessful Logon Warnings* must be enabled.

b) Only *DES* and *Triple-DES* encryption algorithms are to be enabled.

c) *Password Fallback* must not be used.

d) *Allow Password Recovery* must not be used.

e) *Allow New User Introduction* must not be used.

32 Note that there are other TOE configuration options that are recommended, but are not required. For more details on configuring the TOE, administrators should refer to the guidance documentation (Ref [3]).

2.6.2 Delivery procedures

33 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated version.

34 The TOE is delivered in shrink-wrapped packaging containing a CD ROM. Purchasers should ensure that:

a) the name and version on the CD-ROM and its packaging match the version of the evaluated product.

b) there is no evidence of tampering.

35 If these conditions are not met, then the product should be returned to the developer without being used.

2.6.3 Determining the Evaluated Configuration

36 Prior to installation, the administrator should ensure that that the CD volume label correctly identifies the version of the TOE and shows *PD_7_00_03*. Both the *Readme.txt* and the release note, *PD_Release_Note_7_00_03.pdf*, should correspond to the version of the TOE.

37 The purchaser should download the Eracom FileVerify utility (www.eracom-tech.com/resources/fileverify.htm) and verify the cryptographic signatures for each of the files included in the installation package. The digital certificate for Eracom Technologies is embedded in this utility, but may be downloaded separately from their website.

38 After installation, the administrator should check that the installed version matches the evaluated version of the product. This can be determined by running the *ProtectDrive About* application.

39 If there are problems with either of the above steps, then the developer should be contacted for further information.

2.6.4 Documentation

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

a) Protect Drive User Manual, Version B00 (Ref [3]).

2.6.5 Secure Usage

41 The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met. The following assumptions were made:

a) A.Administrator:

i) Administrators are trusted not to compromise security.

ii) Administrators are trusted not to abuse their authority.

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

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

v) Administrators follow password management policies to ensure users comply with password policies.

b) A.Attacker:

i) Attackers have a layman level of expertise and have access to public information concerning the TOE.

ii) Attackers use standard, non-specialised, equipment with which to attempt to exploit the TOE.

c) A.Authorised_User:

i) Authorised users cooperate with those responsible for managing the TOE to maintain TOE security.

ii) Authorised users can be trusted and are not considered to be hostile.

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

d) A.Peer:

i) 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 the information to at least the same degree as that provided by the TOE.

ii) It is assumed that 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.

iii) It is assumed that 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 as the TOE.

e) A.Tamper_Id:

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

42 Access control to the TOE may be implemented using a token and PIN. Any tokens used with the TOE must provide the same level of security. This may be achieved through an equivalent level of evaluation assurance or other security measures.

43 The Security Target (Ref [1]) lists the required security functionality that a token must provide to operate with the TOE. The expected security functionality of the token is:

a) **Cryptographic Support**: The token shall perform asymmetric decryption of data in accordance with the RSA cryptographic algorithm with 512 and 1024 bit key sizes.

b) **User Data Protection**: The token shall only allow access to the protected token data after successful authentication.

c) **Identification and Authentication**: The token will require a user to be successfully authenticated before allowing any other actions to take place.

Chapter 3 - Evaluation

3.1 Overview

44 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

45 The criteria against which the Target of Evaluation (TOE) has been evaluated are expressed in the Common Criteria for Information Technology Security Evaluation (Refs [4], [5], [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [7]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [8], [9]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [10]) were also upheld.

3.3 Functional Testing

46 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 and repeated all of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

47 The evaluators also performed a number of independent functional tests to complement the developer's tests. This testing demonstrated that the TOE security functions have been fully implemented.

3.4 Penetration Testing

48 The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE.

49 Based on the information given in the developer's vulnerability analysis, the evaluators were able to devise a penetration test. After the completion of testing, the evaluators were able to determine that the TOE, in its intended configuration and environment, has no obvious exploitable vulnerabilities.

Chapter 4 - Certification

4.1 Overview

50 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

51 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [11]), the Australasian Certification Authority certifies the evaluation of ProtectDrive Version 7.0.3 performed by the Australasian Information Security Evaluation Facility, LogicaCMG.

52 LogicaCMG has found that ProtectDrive Version 7.0.3 upholds the claims made in the Security Target (Ref[1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL 2.

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

4.3 Assurance Level Information

54 EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behaviour.

55 The analysis is supported by: independent testing of the TOE security functions; evidence of developer testing based on the functional specification; selective independent confirmation of the developer test results; strength of function analysis; and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

56 EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

4.4 Recommendations

57 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 [2]) and New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

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

a) **Disable *Automatic Pre-boot Authentication***: The TOE requires users to authenticate prior to the operating system loading. Enabling this option circumvents this security mechanism. Furthermore, the password for a valid TOE user account is stored in clear text in the registry while this feature is used.

b) **Use Triple-DES algorithm for encryption:** The TOE also allows the use of DES algorithm for encryption. However, due to short key lengths used with DES (56 bit), key exhaustion is a viable attack against this encryption.

c) **Fully encrypt hard disks**: The TOE only provides full security when all the hard drives and partitions have been fully encrypted.

d) **Enable the *Show disk not fully encrypted* warning**: This TOE option should be enabled during installation to ensure that users are aware that in the event that the hard disk is not fully encrypted that their data may not be encrypted.

e) **Lock their computer screens when unattended**: If a user leaves the computer unattended and logged in, then the TOE security properties can be easily bypassed.

f) **Use RSA token keys that are 1024 bits long**: The TOE also supports RSA token keys of 512-bit length. However, this key length is no longer considered to be secure against factoring attacks.

g) **Use New Technology File System (NTFS)**: The TOE will also work with a FAT-32 file system. However, NTFS provides security features such as access control that are not available with FAT-32.

Annex A - References and Abbreviations

A.1 References

[1] ProtectDrive Evaluation Security Target, Eracom Technologies, Revision B12, August 2005.

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

[3] ProtectDrive User Manual, Eracom Technologies, Version B00, March 2005.

[4] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 2.1, August 1999, CCIMB-99-031, Incorporated with interpretations as of 2003-12-31.

[5] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC), Version 2.1, August 1999, CCIMB-99-032, Incorporate with interpretations as of 2003-12-31.

[6] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 2.1, August 1999, CCIMB-99-033, Incorporate with interpretations as of 2003-12-31.

[7] Common Methodology for Information Technology Security Evaluation (CEM), Version 1.0, August 1999, CEM-99/045, Incorporated with interpretations as of 2003-12-31.

[8] AISEP Publication No. 1 – Description of the AISEP, AP 1, Version 2.0, February 2001, Defence Signals Directorate.

[9] AISEP Publication No. 2 – The Licensing of the AISEFs, AP 2. Version 2.1, February 2001, Defence Signals Directorate.

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

[11] EFAT029 Eracom ProtectDrive v 7.0.3 Evaluation Technical Report, Issue 1.1, Reference ECF8406/T8/1, August 2005.

A.2 Acronyms and Abbreviations

ACA	Australasian Certification Authority
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
DES	Data Encryption Standard
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FAT	File Allocation Table
GCSB	Government Communications Security Bureau
GINA	Graphical Identification and Authentication
ID	Identification
MBR	Master Boot Record
NTFS	New Technology File System
PIN	Personal Identification Number
PP	Protection Profile
RSA	Rivest Shamir Adleman public key algorithm
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TED	Transparent Encryption Driver
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy