ProtectDrive

Evaluation Security Target

Revision: B12

eracom TECHNOLOGIES

THIS PAGE INTENTIONALLY LEFT BLANK

Preface

Copyright

Eracom Technologies
28 Greg Chappell Drive
Burleigh Heads, Queensland 4220
AUSTRALIA

	National	International
Voice:	(07) 5593 4911	+ 61 7 5593 4911
Fax:	(07) 5593 4388	+ 61 7 5593 4388

Website: www.eracom-tech.com

Disclaimer

Eracom makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Eracom reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon Eracom to notify any person or organisation of any such revisions or changes.

Publication Improvements

Eracom invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be dispatched to the above address.

THIS PAGE INTENTIONALLY LEFT BLANK

Revision History

No	Date	Reason
B0	12 May 2003	Initial Issue
B1	2 July 2003	Incorporation of AISEP comments
B2	29 September 2003	EOR 1 to 11 and RFC 1 to 10
B3	January 2004	Removal of SC8, Update to PD version 7.0.1, EOR 9,EOR 12 to 14.
B4	February 2004	Update to Version 7.0.2, EOR 9_2, EOR13_2
B5	June 2004	EOR 26
B6	July 2004	Clarify token assumptions; Session definition
B7	August 2004	Update to Version 7.0.3, Fix logon fail details
B8	March 2005	Operating system service pack updates
B9	March 2005	Correct GINA extension description in SF1
B10	May 2005	Change token to an Environmental SFR
B11	May 2005	Environments SFR suitability added, minor typographical errors corrected
B12	August 2005	Correct installation inconsistency

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

CHAPTER 1 Introduction

1.1 Identification

This document is the Security Target (ST) for the Eracom Technologies ProtectDrive version 7.0.3

The TOE is identified as:

ProtectDrive Version 7.0.3**.**

For Microsoft Windows 2000 Professional, 5.00.2195 Service Pack 4; and

Microsoft Windows XP Professional 5.1.2600 Service Pack 2 Build 2600.

This ST has been prepared in accordance with the Common Criteria for Information Technology Security Evaluation (CC), version 2.1, August 1999.

1.2 Overview

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.

ProtectDrive provides strong security while being easy to install and manage and after initial authentication is transparent in operation.

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.

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).

ProtectDrive security features also include:

- Unauthorised sign-on protection activation after three failed sign-on attempts;
- Previous sign-on display showing date and time of previous successful sign-on and details of any unsuccessful attempts since that time;
- Control of booting from floppy disk.

If a PC or laptop computer, with ProtectDrive installed and configured correctly, is stolen, lost or left in an insecure area the confidentiality of information stored on the hard disk is protected by ProtectDrive encryption against attempts, by unauthorised people or hackers, to access the information.

1.3 CC Conformance

The Target of Evaluation (TOE) for this ST is conformant with the functional requirements specified in Part 2 of the CC, and the assurance requirements for Evaluation Assurance Level (EAL) 2, as specified in Part 3 of the CC.

CHAPTER 2
Description

2.1 Product Type

The Target of Evaluation (TOE) is ProtectDrive version 7.0.3.

ProtectDrive is a software based PC security product that protects the confidentiality of information stored on a PC or Laptop computer by encrypting the information as it is written to the computer's Hard Disk Drive.

ProtectDrive permits access to the protected information by authorised users while preventing access by unauthorised users.

ProtectDrive authenticates users through the use of a User Id and Password or Token and PIN. If a Token and PIN is used to authenticate, then ProtectDrive authenticates and identifies users on the basis of the provision of a recognised certificate by the Token.

ProtectDrive also provides configurable control of computer input and output devices (including floppy disk and serial and parallel ports) to prevent inadvertent release of protected information by authorised users.

2.2 TOE Description

The main components of the TOE are:

1. An application that extends the computer BIOS (VX BIOS);
2. a pre-boot identification and authentication module (VROM);
3. a Transparent Encryption Driver (TED);
4. an operating system Graphical Identification and Authentication library (GINA) extension; and
5. a ProtectDrive administration program.

ProtectDrive extends the existing computer BIOS with an application (VX BIOS) that controls access to the computer during initial start up. The BIOS extension controls access to the computer's physical resources and loads the ProtectDrive Pre-Boot identification and authentication module (VROM). After a successful user log on, via the VROM, the BIOS extension allows the operating system to load by decrypting the relevant disk information as it is read from the hard disk drive.

The ProtectDrive pre-boot identification and authentication module (VROM) performs initial user identification and authentication before the operating system is loaded. On completion of the boot process the ProtectDrive identification and authentication module passes the validated user credentials to the operating system.

ProtectDrive adds, as a part of the operating system, a TED between the operating system and the computer input and output system. The TED controls encryption and decryption of information as it is being written to and read from the hard disk drive and provides access control to the computers input and output devices.

ProtectDrive extends the operating system GINA with an authentication monitoring function. This enables ProtectDrive to control user permissions after the operating system has been loaded. (e.g. when a user logs out of the operating system and another user attempts to log on).

A ProtectDrive administration module is provided which allows users with ProtectDrive administration rights to configure individual user access rights and to administer the ProtectDrive configuration.

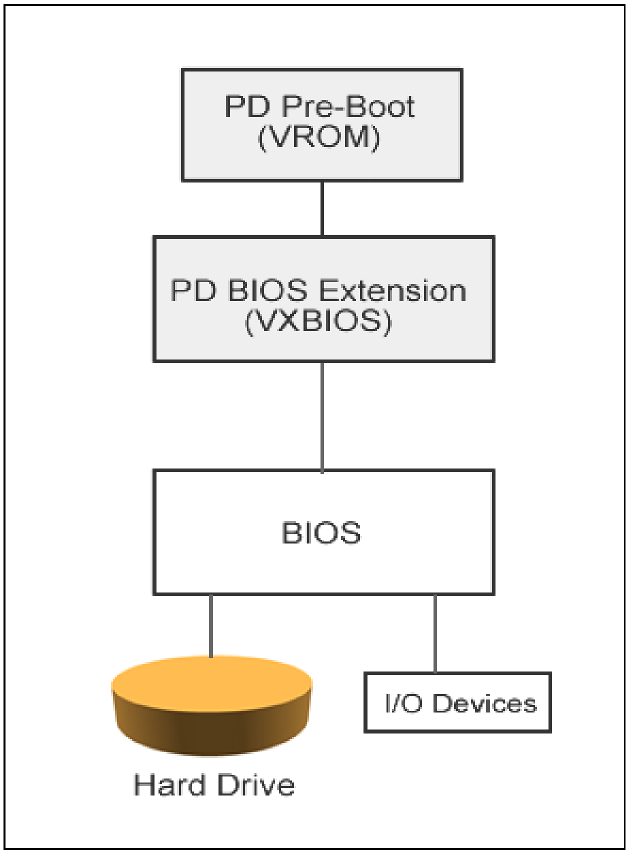

Figure 1 - ProtectDrive Pre-Boot Scope

Figure 1 above pictorially represents the TOE and computer being protected by the TOE in the pre-boot condition. In this condition the scope and boundary of the TOE are the "VROM" and the "VXBIOS" modules.

Figure 2 below pictorially represents the TOE and computer being protected by the TOE in the post-boot condition. In this condition the scope and boundary of the TOE are the "PD Gina Extension", the "PD TED" and the "PD Administration" modules.

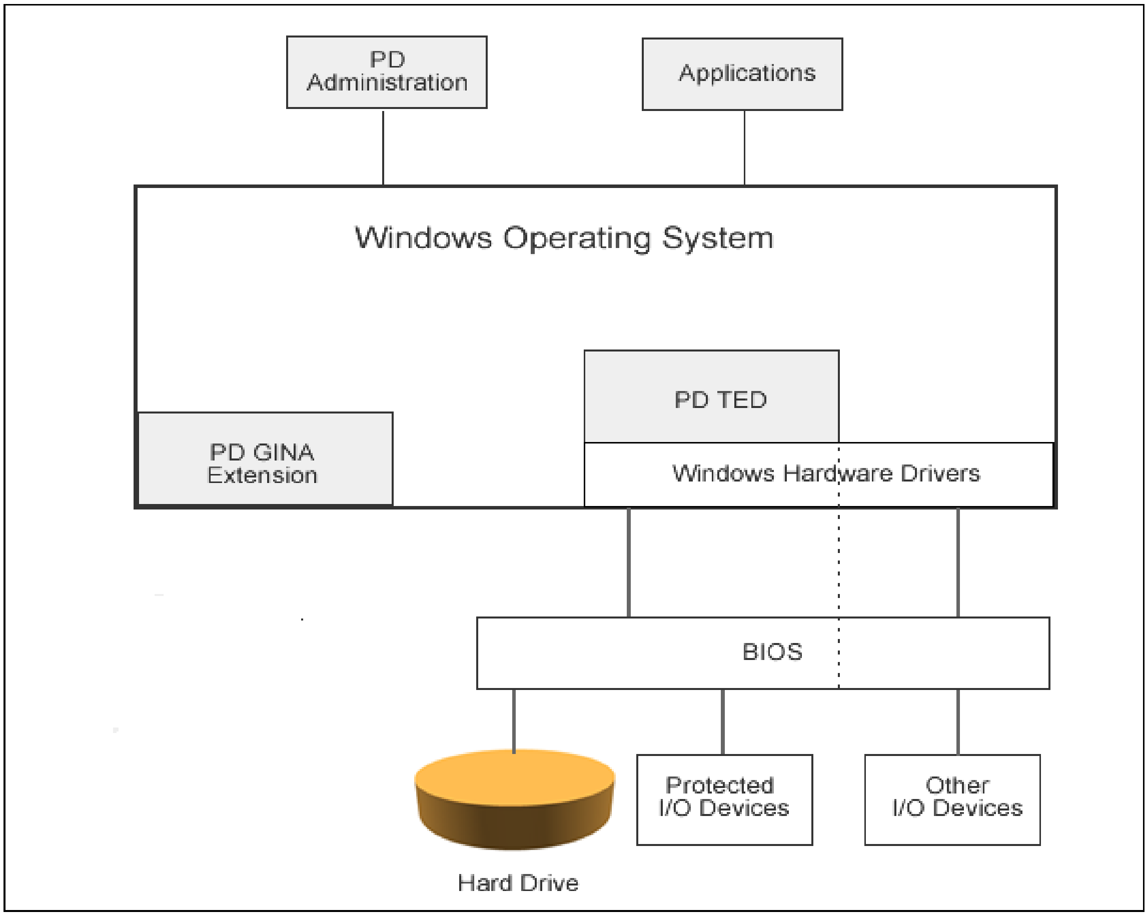

Figure 2 - PD Post Boot Scope

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 3
TOE Security Environment

3.1 Introduction

This section identifies the security issues that form the basis for the choice of the TOE security requirements. It identifies assumptions about the physical, personal and other aspects of the environment of the TOE, the organisational security policies for which the TOE is appropriate, and the threats to information confidentiality that the TOE is intended to counter.

3.2 Assumptions

The following conditions are assumed to exist in the environment in which the TOE will be used.

Identification	Description
A.Administrator	Administrators are trusted not to compromise security. Administrators are trusted not to abuse their authority. Administrators are competent to manage the TOE and security of the information it protects. Administrators follow the policies and procedures defined in the TOE documentation for the secure administration of the TOE. Administrators follow password management policies to ensure users comply with password policies.
A.Attacker	Attackers have a layman level of expertise and have access to public information concerning the TOE. Attackers use standard, non-specialised, equipment with which to attempt to exploit the TOE.
A.Authorised_User	Authorised users cooperate with those responsible for managing the TOE to maintain TOE security. Authorised users can be trusted and are not considered to be hostile. Authorised users are fallible and can make errors or act in ways that may compromise security.

Identification	Description
A.Peer	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. 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. 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 at the TOE.
A.Tamper_Id	It is assumed that 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.

Table 3.1 - Assumptions

3.3 Threats

The following threats are addressed either by the TOE or the environment.

Identification	Description
T.Hack_AC_Weak	An attacker may exploit weak system access control mechanism(s) or user attributes that can be broken or weak implementation methods of the system access control, to gain access to information protected by the TOE, resulting in a compromise of protected information.
T.Hack_Disk	An attacker may physically access a disk drive and use hardware and/or software tools to gain access to information protected by the TOE resulting in a compromise of protected information

Identification	Description
T.Hack_Spoof_Login	An attacker may simulate the system's log on program in order to capture a legitimate user's authentication data and use the captured authentication data to impersonate the user and access information protected by the TOE resulting in a compromise of protected information. This attack requires that an attacker physically access and modify the system protected by the TOE to enable capture of data and then at a later time to again access the system to retrieve and use the captured data.
T.User_Err_Res	An authorised user of the TOE, may accidentally transmit via a serial or parallel port or to floppy disk drive, sensitive information which may be accessed by an attacker resulting in a compromise of protected information.

Table 3.2 - Threats

3.4 Organisational Security Policies

The TOE is intended for general use by organisations, including governmental, commercial and private and for use in various countries, which may have differing organisational and national policies relating to the protection of information. There are no generic organisational security policies with which the TOE is intended to comply.

Organisations intending to use the TOE for protection of information should consider their organisational and national security policies in the selection of a product.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4
Security Objectives

4.1 Introduction

This section defines the security objectives to be satisfied by the TOE and the security objectives to be satisfied by IT and non-IT measures within the TOE environment. It addresses all of the identified aspects of the security environment.

4.2 Security Objectives for the TOE

This section defines the security objectives that will be satisfied by the TOE.

Identification	Description
O.Access_History	The TOE will provide facilities to display information related to the most recent successful and unsuccessful attempts to establish a user session, once a user successfully establishes a user session.
O.Encrypt_Data	The TOE will provide the means of protecting the confidentiality of information stored on the system hard disk drive.
O.Export_Prevention	The TOE will provide a means of preventing unauthorised export of protected information by use of a floppy disk, serial port or parallel port.
O.I&A_User	The TOE will uniquely identify all users, and will authenticate the claimed identity before granting a user access to the TOE facilities.

Table 4.1 - Security Objectives for the TOE

4.3 Security Objectives for the Environment

This paragraph defines the security objectives to be satisfied by IT and non-IT measures within the TOE environment.

Identification	Description
OE.Connect	Those responsible for the TOE must ensure that no connections are provided to outside systems that would undermine security features of the TOE.
OE.Guidance	Those responsible for the TOE must ensure that the TOE is delivered, installed, configured, administered and operated in a manner that maintains its security.

OE.Token	Those responsible for the TOE must ensure that any Tokens used with the TOE provide the same level of security as the TOE. This may be achieved though an equivalent level of evaluation assurance or a combination of evaluation assurance and organisational security measures.
OE.Tamper_ID	Those responsible for the TOE must ensure that the system on which the TOE is installed has features that detect physical tampering to the system and that they provide a clear indication to users that tampering has occurred.
OE.Training	Those responsible for the TOE must ensure that all personnel given administrator privileges are given training sufficient to fulfil their duties.
OE.User_Guidance	Those responsible for the TOE must provide documentation for general users containing information sufficient to fulfil their duties.

Table 4.2 - Security Objectives for the Environment

CHAPTER 5
IT Security Requirements

This section defines IT Security requirements and is divided into the following sections:

1. TOE security functional requirements;
2. TOE assurance requirements;
3. Security requirements for the IT environment; and
4. Security requirements for the Non-IT environment.

5.1 TOE Security Functional Requirements

This section defines the security functional requirements (SFRs) of the TOE as functional components, TOE Security Functions (TSF) drawn from the Common Criteria (CC) Part 2 and through Security Function Policies (SFP).

5.1.1 Cryptographic Support (FCS)

5.1.1.1 Cryptographic key generation (FCS_CKM.1)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [DEA*, Triple DES*] and specified cryptographic key sizes [*56 bit, 112 bit*] that meet the following: [*DES [DES_STD], Triple DES [3DES_STD]*].$^{\text{FCS\_CKM.1.1}}$

5.1.1.2 Cryptographic key destruction (FCS_CKM.4)

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwriting with a standard pattern] that meet the following: [*no defined standard*].$^{\text{FCS\_CKM.4.1}}$

5.1.1.3 Cryptographic operation (FCS_COP.1)

The TSF shall perform [

a. *symmetric encryption and decryption of disk data;*

b. *symmetric encryption and decryption of disk data;*

] in accordance with a specified cryptographic algorithm [

a. *DES* ;

b. *Triple DES.*

] and cryptographic key sizes [

a. *56 bits;*

b. *112 bits;*

] that meet the following: [

a. *DES [DES_STD];*

b. *Triple DES [3DES_STD];*

].FCS_COP.1.1

5.1.2 User Data Protection (FDP)

5.1.2.1 Complete access control (FDP_ACC.2)

The TSF shall enforce the [

a. *Disk Access Control SFP;*

b. *User Attribute Control SFP;*

c. *TOE Configuration Control SFP;*

] on [

a. *Authorised User, Administrator and Protected Disk Data;*

b. *Authorised User, Administrator and User Attribute data;*

c. *Authorised User, Administrator and TOE Configuration Data;*

] and all operations among subjects and objects covered by the SFP.FDP_ACC.2.1

The TSF shall ensure that all operations between any subject in the TOE Scope of Control (TSC) and any object within the TSC are covered by an access control SFP.FDP_ACC.2.2

5.1.2.2 Security attribute based access control (FDP_ACF.1)

The TSF shall enforce the [

a. *Disk Access Control SFP,*

b. *User Attribute Control SFP,*

c. *TOE Configuration Control SFP,*

] to objects based on [

a. *User authentication.*

b. *User Properties, User Permissions, User accounts.*

c. *System Configuration Properties.*

].FDP_ACF.1.1

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a. *If a user is successfully authenticated, then access to Protected Disk Data granted; If a user is not successfully authenticated, then access to Protected Disk Data denied.*

b. *An authenticated user may modify his password, an authenticated Administrator may modify any user's attributes.*

c. *An authenticated administrator may modify any system configuration properties.*

].FDP_ACF.1.2

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [

a. *no rules.*

b. *no rules.*

c. *no rules.*

].FDP_ACF.1.3

The TSF shall explicitly deny access of subjects to objects based on the [

a. *no rules.*

b. *an Administrator shall not remove the default administrator account.*

c. *no rules.*

].FDP_ACF.1.4

5.1.3 Identification and Authentication (FIA)

5.1.3.1 Authentication failure handling (FIA_AFL.1)

The TSF shall detect when [*three*] unsuccessful authentication attempts occur related to [*authenticating to the TOE*].FIA_AFL.1.1

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [for each subsequent authentication attempt prevent an authentication attempt for a time period of one minute].FIA_AFL.1.2

5.1.3.2 User attribute definition (FIA_ATD.1)

The TSF shall maintain the following list of security attributes belonging to individual users: [*role, resource access control list]*. FIA_ATD.1.1

5.1.3.3 User authentication before any action (FIA_UAU.2)

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.FIA_UAU.2.1

5.1.3.4 Protected authentication feedback (FIA_UAU.7)

The TSF shall provide only [*an indication that authentication is in progress*] to the user while the authentication is in progress.FIA_UAU.7.1

5.1.3.5 User identification before any action (FIA_UID.2)

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user. FIA_UID.2.1

5.1.4 Security Management (FMT)

5.1.4.1 Management of security attributes (FMT_MSA.1)

The TSF shall enforce the [

a. *User Attribute Control SFP;*

b. *TOE Configuration Control SFP;*

] to restrict the ability to [

a. *modify;*

b. *modify;*

] the security attributes [

a. *User Properties, User Permissions;*

b. *Configuration Data;*

] to [

a. *Administrators.*

b. *Administrators.*

].FMT_MSA.1.1

5.1.4.2 Secure security attributes (FMT_MSA.2)

The TSF shall ensure that only secure values are accepted for security attributes.FMT_MSA.2.1

5.1.4.3 Specification of Management Functions (FMT_SMF.1

The TSF shall be capable of performing the following security management functions: [Logon Control, Authentication Options, Disk Encryption display, Default User Permissions]$^{FMT\_SMF.1.1}$

5.1.4.4 Security roles (FMT_SMR.1)

The TSF shall maintain the roles [*Administrator, User*].$^{FMT\_SMR.1.1}$

The TSF shall be able to associate users with roles.$^{FMT\_SMR.1.2}$

5.1.5 TOE Access (FTA)

5.1.5.1 TOE access history (FTA_TAH.1)

Upon successful session establishment, the TSF shall display the [*date, time*] of the last successful session establishment to the user. $^{FTA\_TAH.1.1}$

Upon successful session establishment, the TSF shall display the [*date, time*] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment. $^{FTA\_TAH.1.2}$

The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.$^{FTA\_TAH.1.3}$

5.2 TOE Security Assurance Requirements

The TOE security assurance requirements are identical to those defined by the Evaluation Assurance Level 2 (EAL2) of the CC. These requirements are detailed below.

5.2.1 Configuration Management (ACM)

5.2.1.1 Configuration items (ACM_CAP.2)

The reference for the TOE shall be unique to each version of the TOE.$^{ACM\_CAP.2.1C}$

The developer shall provide a reference for the TOE.$^{ACM\_CAP.2.1D}$

The TOE shall be labelled with its reference.$^{ACM\_CAP.2.2C}$

The developer shall use a CM system.$^{ACM\_CAP.2.2D}$

The CM documentation shall include a configuration list.$^{ACM\_CAP.2.3C}$

The configuration list shall uniquely identify all configuration items that comprise the TOE. $^{ACM\_CAP.2.3C[Int\_003]}$

The developer shall provide CM documentation.$^{ACM\_CAP.2.3D}$

The configuration list shall describe the configuration items that comprise the TOE.$^{ACM\_CAP.2.4C}$

The CM documentation shall describe the method used to uniquely identify the configuration items. [ACM_CAP.2.5C]

The CM system shall uniquely identify all configuration items. [ACM_CAP.2.6C]

5.2.2 Delivery and Operation (ADO)

5.2.2.1 Delivery procedures (ADO_DEL.1)

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site. [ADO_DEL.1.1C]

The developer shall document procedures for delivery of the TOE or parts of it to the user. [ADO_DEL.1.1D]

The developer shall use the delivery procedures. [ADO_DEL.1.2D]

5.2.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.[ADO_IGS.1.1C] [Int_051]

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.[ADO_IGS.1.1D]

5.2.3 Development (ADV)

5.2.3.1 Informal functional specification (ADV_FSP.1)

The functional specification shall describe the TSF and its external interfaces using an informal style. [ADV_FSP.1.1C]

The developer shall provide a functional specification. [ADV_FSP.1.1D]

The functional specification shall be internally consistent. [ADV_FSP.1.2C]

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate. [ADV_FSP.1.3C]

The functional specification shall completely represent the TSF.[ADV_FSP.1.4C]

5.2.3.2 Descriptive high-level design (ADV_HLD.1)

The presentation of the high-level design shall be informal. [ADV_HLD.1.1C]

The developer shall provide the high-level design of the TSF.[ADV_HLD.1.1D]

The high-level design shall be internally consistent. [ADV_HLD.1.2C]

The high-level design shall describe the structure of the TSF in terms of sub-systems. [ADV_HLD.1.3C]

The high-level design shall describe the security functionality provided by each subsystem of the TSF.[ADV_HLD.1.4C]

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software. $^{\mathrm{ADV\_HLD.1.5C}}$

The high-level design shall identify all interfaces to the subsystems of the TSF.$^{\mathrm{ADV\_HLD.1.6C}}$

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible. $^{\mathrm{ADV\_HLD.1.7C}}$

5.2.3.3 Informal correspondence demonstration (ADV_RCR.1)

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation. $^{\mathrm{ADV\_RCR.1.1C}}$

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided. $^{\mathrm{ADV\_RCR.1.1D}}$

5.2.4 Guidance Documents (AGD)

5.2.4.1 Administrator guidance (AGD_ADM.1)

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.$^{\mathrm{AGD\_ADM.1.1C}}$

The developer shall provide administrator guidance addressed to system administrative personnel. $^{\mathrm{AGD\_ADM.1.1D}}$

The administrator guidance shall describe how to administer the TOE in a secure manner. $^{\mathrm{AGD\_ADM.1.2C}}$

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment. $^{\mathrm{AGD\_ADM.1.3C}}$

The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.$^{\mathrm{AGD\_ADM.1.4C}}$

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate. $^{\mathrm{AGD\_ADM.1.5C}}$

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.$^{\mathrm{AGD\_ADM.1.6C}}$

The administrator guidance shall be consistent with all other documentation supplied for evaluation. $^{\mathrm{AGD\_ADM.1.7C}}$

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator. $^{\mathrm{AGD\_ADM.1.8C}}$

5.2.4.2 User guidance (AGD_USR.1)

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE. AGD_USR.1.1C

The developer shall provide user guidance. AGD_USR.1.1D

The user guidance shall describe the use of user-accessible security functions provided by the TOE. AGD_USR.1.2C

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment. AGD_USR.1.3C

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment. AGD_USR.1.4C

The user guidance shall be consistent with all other documentation supplied for evaluation. AGD_USR.1.5C

The user guidance shall describe all security requirements for the IT environment that are relevant to the user. AGD_USR.1.6C

5.2.5 Tests (ATE)

5.2.5.1 Evidence of coverage (ATE_COV.1)

The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. ATE_COV.1.1C

The developer shall provide evidence of the test coverage. ATE_COV.1.1D

5.2.5.2 Functional testing (ATE_FUN.1)

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results. ATE_FUN.1.1C

The developer shall test the TSF and document the results. ATE_FUN.1.1D

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed. ATE_FUN.1.2C

The developer shall provide test documentation. ATE_FUN.1.2D

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests. ATE_FUN.1.3C

The expected test results shall show the anticipated outputs from a successful execution of the tests. ATE_FUN.1.4C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified. ATE_FUN.1.5C

5.2.5.3 Independent testing - sample (ATE_IND.2)

The TOE shall be suitable for testing.$^{ATE\_IND.2.1C}$

The developer shall provide the TOE for testing.$^{ATE\_IND.2.1D}$

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF. $^{ATE\_IND.2.2C}$

5.2.6 Vulnerability Assessment (AVA)

5.2.6.1 Strength of TOE security function evaluation (AVA_SOF.1)

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the Protection Profile (PP)/Security Target (ST).$^{AVA\_SOF.1.1C}$

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.$^{AVA\_SOF.1.1D}$

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.$^{AVA\_SOF.1.2C}$

5.2.6.2 Developer vulnerability analysis (AVA_VLA.1)

The developer shall perform a vulnerability analysis. $^{AVA\_VLA.1.1D[Int\_051]}$

The developer shall provide vulnerability analysis documentation. $^{AVA\_VLA.1.2D[Int\_051]}$

The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP. $^{AVA\_VLA.1.1C[Int\_051]}$

The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities. $^{AVA\_VLA.1.2C[Int\_051]}$

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. $_{AVA\_VLA.1.3C[Int\_051]}$

5.3 Security Requirements for the IT Environment

5.3.1 IT Environment

The IT environment security requirements define functional and/or assurance requirements to be satisfied by the IT environment. The requirements are satisfied hardware, firmware and/or software external to the TOE needed in order to ensure that the security objectives for the TOE are achieved.

5.3.2 Cryptographic Support (FCS)

5.3.2.1 Cryptographic operation (OE.FCS_COP.1)

The TSF shall perform [a*symmetric decryption of data]*

in accordance with a specified cryptographic algorithm [RSA]

and cryptographic key sizes [*512 bit, 1024 bit*]

that meet the following: [RSA STD].FCS_COP.1.1

5.3.3 User Data Protection (FDP)

5.3.3.1 Complete access control (OE.FDP_ACC.2)

The TSF shall enforce the [*Token Access Control SFP*]

on [*Authorised User and Protected Token Data*]

and all operations among subjects and objects covered by the SFP.FDP_ACC.2.1

The TSF shall ensure that all operations between any subject in the TOE Scope of Control (TSC) and any object within the TSC are covered by an access control SFP.FDP_ACC.2.2

5.3.3.2 Security attribute based access control (OE.FDP_ACF.1)

The TSF shall enforce the [*Token Access Control SFP*]

to objects based on [*User authentication*].FDP_ACF.1.1

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*If a user is successfully authenticated, then access to Protected Token Data granted; If a user is not successfully authenticated, then access to Protected Token Data denied*].FDP_ACF.1.2

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no rules*].FDP_ACF.1.3

The TSF shall explicitly deny access of subjects to objects based on [*no rules*].FDP_ACF.1.4

5.3.4 Identification and Authentication (FIA)

5.3.4.1 User authentication before any action (OE.FIA_UAU.2)

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.FIA_UAU.2.1

CHAPTER 6
TOE Summary Specification

6.1 Introduction

This section defines the instantiation of the security requirements of the TOE. This specification describes the security functions and assurance measures of the TOE that meet the TOE security requirements.

6.2 TOE Security Functions

This describes the IT security functions provided by the TOE and details how these functions satisfy the TOE security functional requirements. It includes a bi-directional mapping between functions and requirements that shows which functions satisfy which requirements and that all requirements are met.

6.2.1 Identification and Authentication(Ident_Auth) <SF1>

Identification and Authentication security functionality is implemented in the ProtectDrive pre-boot module and in the ProtectDrive GINA extension.

The identification and authentication function (uid and password version) is a probabilistic mechanism that has a Strength of Function (SOF) of SOF ~~-basic~~Basic.

6.2.1.1 Pre-Boot Authentication

This function:

1. Displays a log on window whilst blocking all other screen output and keyboard input until the user has successfully been identified and authenticated.

2. In the event of a failed authentication attempt, creates an audit event in the user's login history and then returns to the initial log on window.

3. In the event of three or more unsuccessful authentication attempts has been met or surpassed, the TSF shall for each subsequent authentication attempt, restart the computer and prevent an authentication attempt for a time period of one minute

4. In the event of a successful authentication; creates an audit event in the user's log on history.

5. Permits user access to controlled resources, based on the user's access attributes.

6. Boots the operating system (which includes the PD GINA extension and the PD TED) by reading and decrypting information from the hard disk drive through the PD BIOS Extension.

7. Enables the ProtectDrive Transparent Encryption driver by making available the necessary encryption key.

8. Passes system Authentication control to the PD GINA Extension.

6.2.1.2 GINA Extension Authentication

This function:

1. Displays to the user the time and date of the last successful log on.
2. Monitors the operating system authentication of a new or the same user after a user has logged off from the operating system. This is to control user based access control to resources.
3. Synchronises the pre-boot user Authentication information when a user's password is changed through the operating system management facilities.

6.2.2 Secure Administration (Secure_Admin)<SF2>

This function allows an authenticated Administrator to:

1. Manage user accounts by adding or removing users and resetting user passwords.
2. Manage user access attributes by granting or removing access to serial or parallel input/output devices and by enabling or disabling user access to floppy disk drives.
3. Manage the TOE configuration by setting the area of the hard disk that is to be protected. This may include "No encryption", "Protect System areas" or "Protect Full Drive".

6.2.3 Protection of Data (Data_Protection) <SF3>

This function:

1. Encrypts and decrypts data, as it is being written to or read from the hard disk drive, in accordance with the TOE configuration, and

Controls access to the computer input and output devices, in accordance with the user access control attributes.

The encryption and decryption functions are realised by permutational (cryptographic) means. It is not appropriate to make a SOF claim for cryptographic mechanisms.

6.3 Assurance Measures

This section specifies the Security Assurance Requirements described in section 5.2.

The TOE itself does not provide any measure or mechanism to satisfy the assurance requirements. Assurance is guaranteed by the development process and by users observing the corresponding directions.

Table 6.3 associates the measures and the documents describing them with the assurance requirements of CC EAL2:

EAL2 Requirement	Assurance Measures	Describing Document
ACM_CAP.2	Use a documented CM system that includes: A unique TOE reference number; A description of the method used to uniquely identify configuration items. Configuration lists that uniquely identify and describe the configuration items that comprise the TOE.	ProtectDrive Configuration Management Document, Rev [B9].
ADO_DEL.1	Document procedures necessary to maintain security of the TOE when distributing the TOE to a user's site.	ProtectDrive Ver [7.0.3], User Manual, Rev [A11].
ADO_IGS.1	Document procedures necessary for the secure installation, generation and start-up of the TOE.	ProtectDrive Ver [7.0.3], User Manual, Rev [A11].
ADV_FSP.1	Provide an informal functional specification of the TOE.	ProtectDrive Functional Specification, Rev [B3].
ADV_HLD.1	Provide a descriptive High Level Design of the TOE.	ProtectDrive High Level Design, Rev [B1]
ADV_RCR.1	Provide an informal analysis of correspondence between adjacent TSF representations.	Informal correspondence analysis is documented in the Functional specification and the High level design documents.
AGD_ADM.1	Provide administrator guidance documentation.	ProtectDrive Ver [7.0.3], User Manual, Rev [A11].
ADG_USR.1	Provide user guidance documentation.	ProtectDrive Ver [7.0.3], User Manual, Rev [A11].
ATE_COV.1	Provide evidence that testing covers the TSFs.	ProtectDrive Ver [7.0.3], Test Plan, Ver [B2].
ATE_FUN.1	Provide test documentation	ProtectDrive Ver [7.0.3], Test Plan, Ver [B2].
ATE_IND.2	Provide the TOE for testing.	TOE; ProtectDrive Ver [7.0.3], User Manual, Rev [A9]; ProtectDrive Ver [7.0.3], Test Plan, Ver [B2].

EAL2 Requirement	Assurance Measures	Describing Document
AVA_SOF.1	Perform a Strength of Function analysis for each identified security function that has a SOF claim.	ProtectDrive Strength of Function Analysis, Rev [B1].
AVA_VLA.1	Perform and document an analysis of obvious ways in which a user can violate the TSP.	ProtectDrive Vulnerability Analysis, Rev [B2].

Table 6.3 - Assurance Measures

CHAPTER 7
Protection Profile Claims

This Security Target does not make any claim that the TOE conforms with the requirements of a Protection Profile. As a consequence, sections "PP Reference", "PP Refinement" and PP Additions" are omitted.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 8
Rationale

8.1 Introduction

The purpose of this chapter is to demonstrate that all aspects of the identified security needs (as defined in the TOE security environment) are suitably addressed by the security objectives, and that the security objectives for the TOE are suitably met by the identified IT security requirements, which in turn are suitably met by the IT security functions and assurance measures. This chapter would also demonstrate compliance with a Protection Profile if it was claimed that the TOE complied with a PP.

8.2 Security Objectives Rationale

This section demonstrates that all identified security needs are suitably addressed by security objectives.

Table 8.1 cross-references the Threats, Organisational Security Policies (OSP) (none in this instance) and Assumptions against the TOE security objectives which are intended to address them.

Table 8.2 cross-references the Threats, Organisational Security Policies (none in this instance) and Assumptions against the Environmental security objectives which are intended to address them.

8.2.1 Objectives

It is evident from the tables that each security objective covers at least one threat, OSP or assumption and that each threat, OSP and assumption is covered by at least one security objective.

Objective	Threat or Assumption
O.Access_History	T.Hack_Spoof_Login, T.Hack_AC_Weak
O.Encrypt_Data	T.Hack_Disk, A.Attacker
O.Export_Prevention	T.User_Err_Res
O.I&A_User	T.Hack_AC_Weak, A.Attacker

Table 8.1 - TOE Security Objectives

Objective	Threat or Assumption
OE.Connect	A.Peer
OE.Guidance	A.Administator
OE.Token	T.Hack_AC_Weak, A.Attacker

Objective	Threat or Assumption
OE.Tamper_ID	A.Tamper_ID, T.Hack_Spoof_Login
OE.Training	A.Administrator
OE.User_Guidance	A.Authorised_User

Table 8.2 - Environmental Security Objectives

8.2.2 Assumptions

The following sections demonstrate that the security objectives are sufficient to meet the security needs of the TOE. Each assumption and threat is considered in turn.

Assumption	Rationale
A.Administrator	OE.Training and OE.Guidance address the Administrator assumption by ensuring that administrators have sufficient training and guidance to competently manage the TOE and comply with the policies and procedures required to maintain the security of the TOE.
A.Attacker	O.EncryptData, O.I&A_User and OE.Token address the Attacker assumption by providing protection to a sufficient level to counter an attempt by an Attacker to access protected information.
A.Authorised_User	OE.User_Guidance addresses the Authorised User assumption by providing sufficient guidance to enable a user to correctly use the TOE.
A.Peer	OE.Connect addresses the Peer assumption by ensuring that any connected networks are protected to at least the same level as the TOE.
A.Tamper_Id	OE.Tamper_ID addresses the Tamper Id assumption by providing adequate evidence of tampering that can be readily seen by a user.

Table 8.3 - Assumptions

8.2.3 Threats

Threat	Rationale
T.Hack_AC_Weak	O.I&A_User, O.Access_History and OE.Token address the threat of a hacker gaining access through weak access controls by Identifying and Authenticating authorised users and by alerting users of unauthorised attempts to use their Identification and Authentication.

Threat	Rationale
T.Hack_Disk	O.Encrypt_Data addresses the Disk Hacking threat by encrypting data before it is written to the disk, making the data unreadable to the hacker.
T.Hack_Spoof_Login	OE.Tamper_ID and O.Access_History address the Spoof Login threat by altering a user that a system has been tampered which in turn alerts the user to the possibility of a spoof login attack.
T.User_Err_Res	O.Export_Prevention addresses the User Resource Error Threat by working together to provide control over access to input and output facilities based on user roles and attributes.

Table 8.4 - Threats

8.3 Security Requirements Rationale

This section shows that the identified IT security requirements (and the SFRs in particular) are suitable to meet and traceable to the identified security objectives and thereby address the security needs of the TOE.

8.3.1 Security Requirement Suitability

Table 8.5 and Table 8.6 cross-reference each security objective for the TOE and the TOE environment with the SFR or SFRs that satisfies it.

It is evident from table 8.5 and table 8.6 that each SFR addresses at least one security objective and that each security objective is addressed by at least one SFR.

Objective	SFR
O.Access_History	FTA_TAH.1
O.Encrypt_Data	FCS_CKM.1 FCS_CKM.4 FCS_COP.1 FDP_ACC.2
O.Export_Prevention	FDP_ACF.1 FIA_ATD.1 FMT_MSA.1 FMT_MSA.2 FMT_SMF.1 FMT_SMR.1
O.I&A_User	FIA_AFL.1

Objective	SFR
	FIA_UAU.2 FIA_UAU.7 FIA_UID.2

Table 8.5 - TOE Security objectives - SFRs

Objective	SFR
OE.Connect	None
OE.Guidance	None
OE.~~Smart_Card~~Token	OE.FCS_COP.1 OE.FDP_ACC.2 OE.FDP_ACF.1 OE.FIA_UAU.2
OE.Tamper_ID	None
OE.Training	None
OE.User_Guidance	None

Table 8.6 - Environmental Security objectives - SFRs

Table 8.7 provides an informal argument for each security objective asserting how the identified SFRs are suitable and sufficient to satisfy the security objective.

Security Objective	Why the SFRs are sufficient
O.Access_History	FTA_TAH.1 displays the users access history to the user after authentication. This requirement ensures that users are provided with details of previous successful and unsuccessful access attempts when they authenticate to the system.
O.Encrypt_Data	FCS_CKM.1 provides a cryptographic key to enable operation of cryptographic operations. FCS_CKM.4 ensures that cryptographic keys are destroyed when no longer required. FCS_COP.1 provides cryptographic operations to encrypt data. FDP_ACC.2 enforces that only authorised users can access decrypted data. OE.FCS_COP.1provides cryptographic operations to decrypt data OE.FDP_ACC.2 enforces that only authorised users can access Token data that is used to decrypt data.

Security Objective	Why the SFRs are sufficient
	These requirements work together to ensure that only authenticated users can access decrypted data.
O.Export_Prevention	FDP_ACF.1 restricts access to resources to authenticated users with resource access rights. FIA_ATD.1 requires that a list of access rights be maintained for users. FMT_MSA.1 restricts the right to change access rights to the administrator. FMT_MSA.2 ensures that only secure values are accepted for rights. FMT_SMF.1 specifies the management functions provided. FMT_SMR.1 requires the creation of administrator and user roles. These requirements work together to control access to resources to authenticated users who have been granted explicate access rights and to restrict control of rights management to administrators.
O.I&A_User	FIA_AFL.1 restricts access attempts after sequential authentication failures. FIA_UAU.2 requires that users be authenticated before allowing access to protected resources. FIA_UAU.7 specifies that only authentication progress information is provided during authentication. FIA_UID.2 requires that users be identified before allowing any other actions. OE.FDP_ACF.1 ensures that only an authenticated user can access the protected Token data. OE.FIA_UAU.2 requires that a user be authenticated before accessing protected Token data These requirements work together to ensure that a user must be identified and authenticated before being permitted to access any resources or information that is protected by the TOE.

Table 8.7 - Suitability of SFRs Satisfy Security Objectives

Table 8.8 provides an informal argument for the environmental security objective that has Environmental SFRs, asserting how the identified environmental SFRs are suitable and sufficient to satisfy the environmental security objective.

Security Objective	Why the SFRs are sufficient

Security Objective	Why the SFRs are sufficient
OE.Token	OE.FCS_COP.1provides cryptographic operations to decrypt data. OE.FDP_ACC.2 enforces that only authorised users can access decrypted data. OE.FDP_ACF.1 ensures that only an authenticated user can access the protected Token data. OE.FIA_UAU.2 requires that a user be authenticated before accessing protected Token data These requirements work together to ensure that the only authenticated users can access Token functionality and decrypted Token data.

Table 8.8 - Suitability of Environmental SFRs to Satisfy Environmental Security Objectives

8.3.2 Security Assurance Requirements

The target evaluation level of CC EAL 2 provides a “low to moderate level of assurance” ([CC]). This is sufficiently high given the identified threats and security objectives, and the assumed environment in which the TOE will operate.

The TOE Assurance Requirements (Section 5.2) cover all aspects to ensure that the security functions provided by the TOE are actually able to respond to the security problems in the form of TOE Security Objectives (Section 4.2). The assurance requirements are exactly those defined for the Evaluation Assurance Level 2. The documentation provided by the developer as listed in Table 6.3 describes that the assurance requirements are properly fulfilled.

The TOE itself does not provide any measure or mechanism to satisfy the assurance requirements.

8.3.3 Functional Requirements Dependencies

Table 8.9 displays all functional dependencies required by the TOE and the IT Environment.

Table 8.9 is constructed with:

1. The first column is a unique row identifier.

2. The second column identifying the component;

3. The third column identifying the dependencies; and

4. The fourth column showing where the dependency is fulfilled.

Id	Component	Dependencies	Dependency fulfilled by

	TOE Security Functional Components		
1	FCS_CKM.1	FCS_COP.1 FCS_CKM.4 FMT_MSA.2	FCS_COP.1 (3) FCS_CKM.4 (2) FMT_MSA.2 (12)
2	FCS_CKM.4	FCS_CKM.1 FMT_MSA.2	FCS_CKM.1 (1) FMT_MSA.2 (12)
3	FCS_COP.1	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	FCS_CKM.1 (1) FCS_CKM.4 (2) FMT_MSA.2 (12)
4	FDP_ACC.2	FDP_ACF.1	FDP_ACF.1 (5)
5	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 (4) See note below (FMT_MSA.3)
6	FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 (8)
7	FIA_ATD.1	No dependency	
8	FIA_UAU.2	FIA_UID.1	FIA_UID.2 (10)
9	FIA_UAU.7	FIA_UAU.1	FIA_UAU.2 (8)
10	FIA_UID.2	No Dependency	
11	FMT_MSA.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	FDP_ACC.2 (4) FMT_SMF.1 (13) FMT_SMR.1 (14)
12	FMT_MSA.2	FDP_ACC.1 FMT_MSA.1 FMT_SMR.1 ADV_SPM.1	FDP_ACC.2 (4) FMT_MSA.1 (11) FMT_SMR.1 (14) See note below (ADV_SPM.1)
13	FMT_SMF.1	No Dependency	
14	FMT_SMR.1	FIA_UID.1	FIA_UID.2 (10)
17	FTA_TAH.1	No Dependency	
	IT Environment Security Functional Components		
18	OE.FCS_COP.1	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	OE fulfilment (see note below) OE fulfilment (see note below) OE fulfilment (see note below)
19	OE.FDP_ACC.2	FDP_ACF.1	OE.FDP_ACF.1 (20)
20	OE.FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	OE.FDP_ACC.2 (19) OE fulfilment (see note below)

21	OE.FIA_UAU.2	FIA_UID.1	See note below (FIA_UID.1)

Table 8.9 - SFR Dependency Analysis

OE Fulfilment. These dependency functions are considered to be fulfilled by the Organisational Environment. The dependencies are not directly required by the TOE and are considered to be beyond the scope of the TOE evaluation.

Several dependencies are not directly satisfied, as shown in Table 8.9. These are satisfied as follows:

FMT_MSA.3 Dependencies of FDP_ACF.1. FDP_ACF.1 is dependent on FMT_MSA.3, Static attribute initialisation, which requires that the TSF allow specified roles to set alternative default values for security attributes that are used to enforce the SFP. ProtectDrive does not provide this functionality. The default values for security attributes used to enforce the SFP are always the same, being set by the TSF itself. As the initial values are secure, the dependency is satisfied

ADV_SPM.1 Dependencies of FMT_MSA.2. FMT_MSA.2 is dependent on ADV_SPM.1, Informal TOE security policy model. Assumption A.Administrator and environment objective OE.Training ensure that Administrators are trained and apply suitable management of security attributes such as passwords. As the attributes are competently managed by trained administrators this dependency is considered to be satisfied.

FIA_UID.1 Dependency of OE.FIA_UAU.2. OE.FIA_UAU.2 is dependent on FIA_UID.1, timing of identification. In this instance identification is achieved by possession and presentation of a Token. The Token (though data contained on the Token) is the identification

8.3.4 Mutually Supportive Security Requirements Rationale

The security requirements are mutually supporting as all requirements are based purely on the CC part 2 and all dependencies have been addressed. The set of SFRs are internally consistent and include SFRs that defend other SFRs against attacks such as bypassing or tampering.

The internal consistency of the security requirements is demonstrated by considering how they work together to satisfy the TOE security objectives as detailed in Table 8.7. The informal arguments in Table 8.7 also demonstrate that in meeting the TOE security objectives there is no inconsistency or conflict amongst the SFRs.

8.3.5 Strength of Function Level Rationale

The TOE Identification and Authentication function (when using user ID and password) has a strength of function of SOF–-Basic. The Strength of function claim is demonstrated in the document ProtectDrive Strength of Function Analysis Document, Rev [B0].

No claim as to the SOF of cryptographic algorithms is made as these are outside the scope of the CC. $^{\text{ASE\_REQ.1-15}}$

The SOF of Basic for the TOE Identification and Authentication function is consistent with identified threats to the TOE, the A.Attacker assumption and the countering objectives O.Encrypt_Data and O.I&A_User.

8.4 TOE Summary Specification Rationale

8.4.1 Satisfaction of Functional Requirements

Table 8.10 demonstrates that the IT Security Functions are suitable to meet to meet all of the TOE SFRs. It is also self-evident from the mapping in Table 8.10 and the Security Function descriptions in section 6.2 how each SFR is satisfied.

SFR	<SF1>	<SF2>	<SF3>
FCS_CKM.1			X
FCS_CKM.4			X
FCS_COP.1			X
FDP_ACC.2			X
FDP_ACF.1			X
FIA_AFL.1	X		
FIA_ATD.1		X	
FIA_UAU.2	X		
FIA_UAU.7	X		
FIA_UID.2	X		
FMT_MSA.1		X	
FMT_MSA.2		X	
FMT_SMF.1		X	
FMT_SMR.1		X	
FTA_TAH.1	X		
OE.FCS_COP.1			X
OE.FDP_ACC.2			X
OE.FDP_ACF.1			X
OE.FIA_UAU.2	X		

Table 8.10 - SFR and Security Function Correspondence

8.4.2 Mutually Supportive IT Security Functions

The TOE Summary Specification does not introduce any changes to the dependency and mutual support argument presented for SFRs.

8.4.3 Security Assurance Measures

The security assurance requirements of EAL 2 is achievable for the following reasons:

1. all documentation and other resources required by this assurance level as shown in Table 6.3 will be made available,

2. the documents have been produced to fulfil the criteria of this assurance level,

3. the TOE has been developed to achieve a high degree of security, and

4. the TOE was developed in a secure manner.

As shown in the Security Assurance Requirements Rationale, the Security assurance level of EAL2 is suitable for this TOE.

8.5 PP Claims Rationale

This Security Target does not make any claim that the TOE conforms to the requirements of a Protection Profile (PP). As a consequence the chapter PP Claims Rationale is omitted.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A
Glossary

Boot Record	See Master Boot Record
DEA	Data Encryption Algorithm (another name for DES)
DES	Data Encryption Standard (also see DEA)
EAL	Evaluation Assurance Level
IPL	Initial Program Load - this component of the BIOS runs after Power On Self Test (POST). It loads the MBR into memory and executes the first instruction. Also known as the Master Boot Loader.
KEK	Key encryption key
Master Boot Record	This is the sector loaded and executed by the IPL. Traditionally it is the first sector on the first mass storage device detected by the BIOS.
MBR	See Master Boot Record
PC	Personal Computer
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RSA	RSA (Rivest, Shamir, Adleman) public key algorithm
System key	The System Key is a KEK used by ProtectDrive.
TED	Transparent Encryption Driver. The TED is a Windows Device Driver module which interfaces directly with the operating system to perform all disk read and write operations, and also manages all other ProtectDrive functions that require such an interface.
User	Any person (authorised or unauthorised) attempting to use a machine that the TOE is installed on.
VROM	VROM is the user authentication module of ProtectDrive that is invoked during the boot process..
VXBIOS	Virtual eXtended BIOS. Is a BIOS extension used by ProtectDrive.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix B References

The following documents were referenced in the preparation of this Security Target:

Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), version 2.1, Parts 1, 2 and 3 [CC]

Guide for Production of Protection Profiles and Security Targets, Version 0.9, ISO/IEC WD 15446, M. Donaldson, January 2000 [GPPPST]

NBS FIPS PUB 46 Data Encryption Standard, National Bureau of Standards, US Department of Commerce, Jan 1977 [DES_STD]

END OF DOCUMENT