ProtectDrive 8.1.1
Common Criteria EAL 4
Security Target

DOCUMENT NUMBER:	CR-2627
AUTHOR:	David Pitard / Iain Holness
DEPARTMENT:	Enterprise Engineering
LOCATION OF ISSUE:	Belcamp
DATE ORIGINATED:	April 2005
REVISION LEVEL:	B10
REVISION DATE:	August 5, 2008
SUPERSESSION DATA:	B09
SECURITY LEVEL:	

DOCUMENT CHANGE HISTORY

Revision	Date	Author	Reason for Change	Sections Affected
A00	April 2005		Initial Issue	
A01	June 2005		Update to Token environmental SFR	
A02	June 2005		Update to SFR dependencies (EOR001).	
A03	July 2005		Product Version change 7.02.01 to 7.02.02	
A04	August 2005		T.User_Err_Res satisfaction and scope diagram	
B00	May 2006		Product Version Change 7.02.02 to 8.00.00	
B01	August 2006		Company name change	
B02	January 2006	David Pitard	Update to product features	
B03	March 08, 2007	Iain Holness	• EOR 02 Response • Removed FMT_SMR.1 as part of a development review of product features • Product version change 8.0.0 to 8.1.1 • Reformatted to common SafeNet template • Updated 5.1.2.2 (FDP_ACF.1.4) as part of development review of product features – no more admin accounts in TOE, only user accounts • Minor corrections to 5.2.2.1, 6.2.5 on Mar 22	all
B04	March 28, 2007	Iain Holness	Minor update to 5.1.3.5: added text at end of FIA_UAU.5.1	5.1.3.5
B05	October 16, 2007	Iain Holness	Response to EORs ▪ Reintroduced FMT_SMR.1 ▪ Added Security Objective for OpEnv to identify users ▪ Add in FMT_MSA.3 based on Admin Guide	4.3, 5.1, 8.2.1, 8.3.1, 8.3.3, 8.4.1
B06	November 21, 2007	Iain Holness	Updates as per discussion from site visit	5.1.4.3, 5.1.4.1, 5.1.5, 6.2.3
B07	March 6, 2008	Iain Holness	Minor corrections noted from evaluators	8.2.2.2, 8.3.1
B08	April 23, 2008	Iain Holness	Correction as per independent testing • lockout is at preboot only • FTA_TAH.1.1 and related text removed	1.2, 4.2, 5.1.6, 8.2.1, 8.2.2.2, 8.3.1, 8.3.3, 8.4.1
B09	July 8, 2008	Iain Holness	• Minor corrections noted from certifier • Removal of Company Confidential text	1.2
B10	August 5, 2008	Iain Holness	Minor tweaks from certifier	1.2, 6.2.2

TABLE OF CONTENTS

Section **Title** **Page**

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

1.1 Identification

This document is the Security Target (ST) for the SafeNet Inc. ProtectDrive version 8.1.1

The TOE is identified as:

ProtectDrive Version 8.1.1.

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 2.3, August 2005.

1.2 Overview

ProtectDrive is a software product that provides protection of sensitive information on laptops and workstations. Protection is provided through encryption of storage devices and pre-boot authentication control.

ProtectDrive provides the benefit of strong security while being easy to install and manage and transparent in operation.

ProtectDrive security features include:

- Unauthorized sign-on protection activation after a configurable number of failed pre-boot sign-on attempts;
- Controlled access to device classes[1] such as storage devices, printers, modems, digital cameras and scanners etc.

ProtectDrive may be deployed to multiple clients using a Windows Installer (MSI) package over a network or individual clients by personal installation.

If a PC or laptop computer protected by ProtectDrive is stolen, lost or left in an insecure area the confidentiality of information protected by ProtectDrive encryption is secured against attempts, by unauthorized people or hackers, to access the information.

ProtectDrive supports most removable storage media devices, with a list of tested devices provided in the product documentation.

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) 4, as specified in Part 3 of the CC.

[1] See definition of ProtectDrive Device Classes in Appendix A.

1.4 References

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

- Common Criteria for Information Technology Security Evaluation, version 2.3, Parts 1, 2 and 3 [CC]
- National Institute of Standards and Technology, Federal Information Processing Standards Publication 46-3 - Data Encryption Standard (DES) (FIPS PUB 46-3), 25 October 1999. [TDEA_STD]
- National Institute of Standards and Technology, Federal Information Processing Standards Publication 197 - Advanced Encryption Standard (AES) (FIPS PUB 197), 26 November 2001. [AES_STD]

2. DESCRIPTION

2.1 Production Type

The Target of Evaluation (TOE) is ProtectDrive version 8.1.1.

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 Storage Media.

2.2 TOE Description

The main components of the TOE are:

1. a pre-boot 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 Active Directory Management Console Snap-in; and
5. a Local Management Console.

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 logon via the VROM, the BIOS extension allows the operating system to load by decrypting the relevant data as it is read from the storage device.

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 storage devices and provides access control to the computers’ input and output devices through control of device classes.

ProtectDrive adds an extension to the Windows Local and Group Management Console with an authentication monitoring function. This enables ProtectDrive to control user permissions after the operating system has been loaded and for users to update their password.

ProtectDrive adds an Active Directory Management Console Snap-in that enables an administrator to centrally manage ProtectDrive installations.

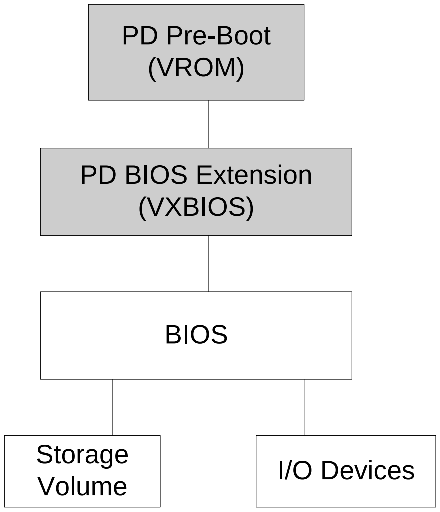

Figure 2.1 – ProtectDrive Pre-Boot Scope

Figure 2.1 above depicts the TOE and computer being protected by the TOE in the pre-boot state. In this state the scope and boundary of the TOE are the "VROM" and the "VXBIOS" modules.

Figure 2.2 below depicts the TOE and computer being protected by the TOE in the post-boot state. In this state the scope and boundary of the TOE are the "PD GINA Extension", the “Service Daemons / Shell Extensions”, the "PD TED" and the "PD Admin Utility" modules.

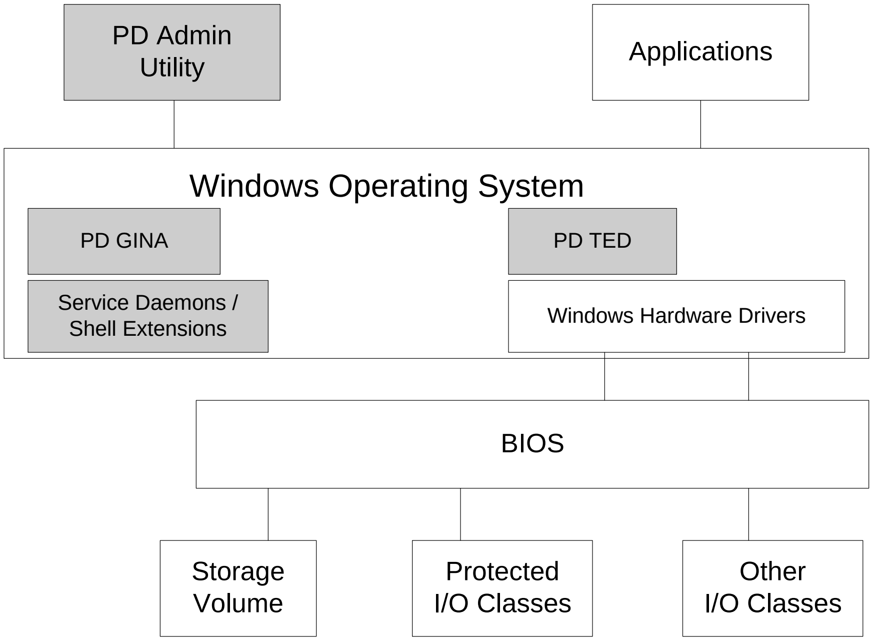

Figure 2.2 – ProtectDrive Post-Boot Scope

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 organizational 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.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.
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 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_Storage	An attacker may physically access a storage device and use hardware and/or software tools to gain access to information protected by the TOE resulting in a compromise of protected information
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 direct protected information to a device that is connected to a physical interface on the computer. This may allow the protected information to be accessed by an attacker resulting in a compromise of protected information.

Table 3.2 - Threats

3.4 Organizational Security Policies

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

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

ProtectDrive is intended primarily as a pre-boot protection program. Once a system has booted and is under control of the operating system the user has access to protected information. Organizations should implement suitable policies controlling the use and export of protected information while a system is active; e.g. use of e-mail, file sharing, network drives, network printers and FTP etc.

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.Encrypt_Data	The TOE will provide the means of protecting the confidentiality of information stored on the system storage devices.
O.Interface_Protection	The TOE will provide a means of controlling access to computer connections through control of device classes.
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 section 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.Tamper_ID	Those responsible for the TOE must ensure that the system on which the TOE is installed provides a clear indication of any tampering to the system.
OE.Training	Those responsible for the TOE must ensure that all personnel given TOE administrator privileges have the required competencies to fulfil their duties.
OE.Token	Those responsible for the TOE must ensure that 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.

Identification	Description
OE.User_Guidance	Those responsible for the TOE must ensure that all users of the TOE have the required competencies to fulfil their duties.
OE.User_Identification	The Operating Environment in which the TOE is installed must differentiate between administrative users and regular users, ensuring that only administrative users can make modifications using the TOE’s administrative functions.

Table 4.2 - Security Objectives for the Environment

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).

Assignments, Selections and Refinements are indicated in italics within brackets, with tables included where appropriate.

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 specified cryptographic key generation algorithms and specified cryptographic key sizes that meet known standards, as indicated in Table 5.1 below. $^{\text{FCS\_CKM.1.1}}$

Algorithm	Key Sizes	Standard
Triple DES	112 bits	Triple DES [FIPS PUB 46-3]
AES	128 bits or 192 bits or 256 bits	AES [FIPS PUB 197]

Table 5.1 – Cryptographic Key Generation

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 meets the following: [*no defined standard*]. $^{\text{FCS\_CKM.4.1}}$

5.1.1.3. Cryptographic Operation (FCS_COP.1)

The TSF shall perform [*symmetric encryption and decryption of Storage data*] in accordance with specified cryptographic algorithms and specified cryptographic key sizes that meet known standards, as indicated in Table 5.2 below. $^{\text{FCS\_COP.1.1}}$

Algorithm	Key Sizes	Standard
Triple DES	112 bits	Triple DES [FIPS PUB 46-3]
AES	128 bits or 192 bits or 256 bits	AES [FIPS PUB 197]

Table 5.2 – Cryptographic Operation

5.1.2 User Data Protection (FDP)

5.1.2.1. Complete Access Control (FDP_ACC.2)

The TSF shall enforce [*specified access control SFPs*] on [*specified objects*] and all operations among subjects and objects covered by the SFP, as indicated in Table 5.3 below. FDP_ACC.2.1

Access Control	Object
Storage Access Control SFP	Authorized User, Administrator and Protected Storage Data
User Attribute Control SFP	Authorized User, Administrator and User Attribute data
TOE Configuration Control SFP	Authorized User, Administrator and TOE Configuration Data

Table 5.3 – Complete Access Control

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 [*specified access control SFPs*] to objects based on [*specified criteria*], as indicated in Table 5.4 below. FDP_ACF.1.1

Access Control	Access Control Criteria
Storage Access Control SFP	User authentication
User Attribute Control SFP	User Properties, User Permissions, User accounts
TOE Configuration Control SFP	System Configuration Properties

Table 5.4 – Access Control Criteria

The TSF shall enforce [*specific rules*] to determine if an operation among controlled subjects and controlled objects is allowed, as indicated in Table 5.5 below. FDP_ACF.1.2

Access Control	Access Control Rule(s)
Storage Access Control SFP	If a user is successfully authenticated, then access to Protected Storage Data granted; If a user is not successfully authenticated, then access to Protected Storage Data denied.
User Attribute Control SFP	An authenticated user may modify his password; an authenticated Administrator may modify any user's attributes.
TOE Configuration Control SFP	An authenticated administrator may modify system configuration properties.

Table 5.5 – Access Control Rules

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules shown in Table 5.6 below. FDP_ACF.1.3

Access Control	Additional Access Control Rule(s)
Storage Access Control SFP	None
User Attribute Control SFP	None
TOE Configuration Control SFP	none

Table 5.6 – Additional Access Control Rules

The TSF shall explicitly deny access of subjects to objects based on the rules shown in Table 5.7 below. FDP_ACF.1.4

Access Control	Subjects Access to Objects Control Rule(s)
Storage Access Control SFP	none
User Attribute Control SFP	none
TOE Configuration Control SFP	none

Table 5.7 – Additional Access Control Rules

5.1.3 Identification and Authentication (FIA)

5.1.3.1. Authentication Failure Handling (FIA_AFL.1)

The TSF shall detect when [*a configurable number of*] 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 configurable time period*]. 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, device class 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. Single-Use Authentication Mechanisms (FIA_UAU.4)

The TSF shall prevent reuse of authentication data related to [*Token fall back mechanism, User Key Recovery mechanism, and New User Introduction mechanism*]. FIA_UAU.4.1

5.1.3.5. Multiple Authentication Mechanisms (FIA_UAU.5)

The TOE shall provide [

a. User ID and Password mechanism;

b. Token (including smartcard) authentication mechanism;

c. Token fall back authentication mechanism, with Windows log-on recovery;

d. User key recovery authentication mechanism, with Windows log-on recovery;

e. New User Introduction authentication mechanism, with Windows log-on recovery.

] to support user authentication. FIA_UAU.5.1

The TSF shall identify user's claimed identify according to the [authentication mechanism specified by an authorized administrator]. FIA_UAU.5.2

5.1.3.6. 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

5.1.3.7. 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 [*specified access control SFP*] to restrict the ability to [*specific actions*] the security attributes [*specific security attributes*] to [*specific users*], as shown in Table 5.8 below. FMT_MSA.1.1

Access Control	Specific Action(s)	Specific Security Attributes	Specific Users
User Attribute Control SFP	Modify	User Properties User Permissions	OE Administrators
TOE Configuration Control SFP	Modify	Configuration Data	OE Administrators

Table 5.8 – Access Restrictions on Security Attributes

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. Static Attribute Initialisation (FMT_MSA.3)

The TSF shall enforce the [*access control SFPs*] to provide [*restrictive, permissive*] default values for security attributes that are used to enforce the SFP. FMT_MSA.3.1

The TSF shall allow the [*OE Administrators*] to specify alternative initial values to override the default values when an object or information is created. FMT_MSA.3.2

5.1.4.4. Specification of Management Functions (FMT_SMF.1)

The TSF shall be capable of performing the following security management functions: [*user accounts (create, delete and modify), User Permissions, Password recovery, Storage Encryption*]. FMT_SMF.1.1

5.1.5 Security Roles (FMT_SMR.1)

The TSF shall maintain the roles [*authenticated OE user*, *authenticated OE administrator*]. FMT_SMR.1.1

The TSF shall be able to associate users with roles. FMT_SMR.1.2

5.2 TOE Assurance Requirements

The TOE security assurance requirements are identical to those defined by the Evaluation Assurance Level 4 (EAL 4) of the CC. These requirements are detailed below.

5.2.1 Configuration Management (ACM)

5.2.1.1. Partial CM Automation (ACM_AUT.1)

The developer shall use a CM system. ACM_AUT1.1D

The developer shall provide a CM plan. ACM_CAP.1.2D

The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation. ACM_AUT.1.1C

The CM system shall provide an automated means to support the generation of the TOE. ACM_AUT.1.2C

The CM plan shall describe the automated tools used in the CM system. ACM_AUT.1.3C

The CM plan shall describe how the automated tools are used in the CM system. ACM_AUT.1.4C

5.2.1.2. Generation, Support and Acceptance Procedures (ACM_CAP.4)

The developer shall provide a reference for the TOE. ACM_CAP.4.1D

The developer shall use a CM system. ACM_CAP.4.2D

The developer shall provide CM documentation. ACM_CAP.4.3D

The reference for the TOE shall be unique to each version of the TOE. ACM_CAP.4.1C

The TOE shall be labeled with its reference. ACM_CAP.4.2C

The CM documentation shall include a configuration list, a CM plan, and an acceptance plan. ACM_CAP.4.3C

The configuration list shall uniquely identify all configuration items that comprise the TOE. ACM_CAP.4.4C

The configuration list shall describe the configuration items that comprise the TOE. ACM_CAP.4.5C

The CM documentation shall describe the method used to uniquely identify the configuration items. ACM_CAP.2.6C

The CM system shall uniquely identify all configuration items. ACM_CAP.2.7C

The CM plan shall describe how the CM system is used. ACM_CAP.2.8C

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan. ACM_CAP.2.9C

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system. ACM_CAP.2.10C

The CM system shall provide measures such that only authorized changes are made to the configuration items. ACM_CAP.2.11C

The CM system shall support generation of the TOE. ACM_CAP.2.12C

The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE. ACM_CAP.2.13C

5.2.1.3. Problem Tracking CM Coverage (ACM_SCP.2)

The developer shall provide a list of configuration items for the TOE. ACM_SCP.2.1D

The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST. ACM_SCP.2.1C

5.2.2 Delivery and Operation (ADO)

5.2.2.1. Detection of Modification (ADO_DEL.2)

The developer shall document procedures for delivery of the TOE or parts of it to the user. ADO_DEL.2.1D

The developer shall use the delivery procedures. ADO_DEL.2.2D

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.2.1C

The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between developer’s master copy and the version received at the user site. ADO_DEL.2.2C

The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user’s site. ADO_DEL.2.3C

5.2.2.2. Installation, Generation, and Start-up Procedures (ADO_IGS.1)

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

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

5.2.3 Development (ADV)

5.2.3.1. Fully-defined External Interfaces (ADV_FSP.2)

The developer shall provide a functional specification. ADV_FSP.2.1D

The functional specification shall describe the TSF and its external interfaces using an informal style. ADV_FSP.2.1C

The functional specification shall be internally consistent. ADV_FSP.2.2C

The functional specification shall describe the purpose and method of use of all external TSF interfaces; provide complete details of effects, exceptions and error messages. ADV_FSP.2.3C

The functional specification shall completely represent the TSF. ADV_FSP.2.4C

The functional specification shall include rationale that the TSF is completely represented. ADV_FSP.2.4C

5.2.3.2. Security Enforcing High-level Design (ADV_HLD.2)

The developer shall provide the high-level design of the TSF. ADV_HLD.2.1D

The presentation of the high-level design shall be informal. ADV_HLD.2.1C

The high-level design shall be internally consistent. ADV_HLD.2.2C

The high-level design shall describe the structure of the TSF in terms of sub-systems. ADV_HLD.2.3C

The high-level design shall describe the security functionality provided by each subsystem of the TSF. ADV_HLD.2.4C

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. ADV_HLD.2.5C

The high-level design shall identify all interfaces to the subsystems of the TSF. ADV_HLD.2.6C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible. ADV_HLD.2.7C

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages as appropriate. ADV_HLD.2.8C

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems. ADV_HLD.2.9C

5.2.3.3. Subset of the Implementation of the TSF (ADV_IMP.1)

The developer shall provide the implementation representation for a selected subset of the TSF. ADV_IMP1.1D

The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions. ADV_IMP1.1C

The implementation representation shall be internally consistent. ADV_IMP1.2C

5.2.3.4. Descriptive Low-level Design (ADV_LLD.1)

The developer shall provide the low-level design of the TSF. ADV_LLD.1.1D

The presentation of the low-level design shall be informal. ADV_LLD.1.1C

The low-level design shall be internally consistent. ADV_LLD.1.2C

The low-level design shall describe the TSF in terms of modules. ADV_LLD.1.3C

The low-level design shall describe the purpose of each module. ADV_LLD.1.4C

The low-level design shall define the interrelationships between modules in terms of provided security functionality and dependencies on other modules. ADV_LLD.1.5C

The low-level design shall describe how each TSP-enforcing function is provided. ADV_LLD.1.6C

The low-level design shall identify all interfaces to the modules of the TSF. ADV_LLD.1.7C

The low-level deign shall identify which of the of the interfaces to he modules of the TSF are externally visible. ADV_LLD.1.8C

The low-level design shall describe purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate. ADV_LLD.1.9C

The low-level deign shall describe the separation of the TOE into TSP-enforcing and other modules. ADV_LLD.1.10C

5.2.3.5. Informal Correspondence Demonstration (ADV_RCR.1)

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided. ADV_RCR.1.1D

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. ADV_RCR.1.1C

5.2.3.6. Informal TOE Security Policy Model (ADV_SPM.1)

The developer shall provide a TSP model. ADV_SPM.1.1D

The developer shall demonstrate correspondence between the functional specification and the TSP model. ADV_SPM.1.2D

The TSP model shall be informal. ADV_SPM.1.1C

The TSP model shall describe the rules and characteristic of all policies of the TSP that can be modeled. ADV_SPM.1.2C

The TSP model shall describe the rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled. ADV_SPM.1.3C

The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model. ADV_SPM.1.4C

5.2.4 Guidance Documents (AGD)

5.2.4.1. Administrator Guidance (AGD_ADM.1)

The developer shall provide administrator guidance addressed to system administrative personnel. AGD_ADM.1.1D

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE. AGD_ADM.1.1C

The administrator guidance shall describe how to administer the TOE in a secure manner. AGD_ADM.1.2C

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment. AGD_ADM.1.3C

The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE. AGD_ADM.1.4C

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate. 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. AGD_ADM.1.6C

The administrator guidance shall be consistent with all other documentation supplied for evaluation. AGD_ADM.1.7C

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator. AGD_ADM.1.8C

5.2.4.2. User Guidance (AGD_USR.1)

The developer shall provide user guidance. AGD_USR.1.1D

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

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 behavior 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 Life Cycle Support (ALC)

5.2.5.1. Identification of Security Measures (ALC_DVS.1)

The developer shall produce development security documentation. ALC_DVS.1.1D

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. ALC_DVS.1.1C

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.1.2C

5.2.5.2. Developer-defined Life-cycle Model (ALC_LCD.1)

The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE. [ALC_LCD.1.1D]

The developer shall provide life-cycle definition documentation. [ALC_LCD.1.2D]

The life-cycle definition documentation shall describe the model used to develop and maintain the TOE. [ALC_LCD.1.1C]

The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE. [ALC_LCD.1.2C]

5.2.5.3. Well-defined Developer Tools (ALC_TAT.1)

The developer shall identify the development tools being used for the TOE. [ALC_TAT.1.1D]

The developer shall document the selected implementation-dependent options of the development tools. [ALC_TAT.1.2D]

All development tools used for implementation shall be well defined. [ALC_TAT.1.1C]

The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation. [ALC_TAT.1.2C]

The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options. [ALC_TAT.1.3C]

5.2.6 Tests (ATE)

5.2.6.1. Analysis of Coverage (ATE_COV.2)

The developer shall provide evidence of the test coverage. [ATE_COV.2.1D]

The analysis 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.2.1C]

The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete. [ATE_COV.2.2C]

5.2.6.2. Testing: High-level Design (ATE_DPT.1)

The developer shall provide the analysis of the depth of testing. [ATE_DPT.1.1D]

The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design. [ATE_DPT.1.12C]

5.2.6.3. Functional Testing (ATE_FUN.1)

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

The developer shall provide test documentation. [ATE_FUN.1.2D]

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

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 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]

5.2.6.4. Independent Testing - Sample (ATE_IND.2)

The developer shall provide the TOE for testing. [ATE_IND.2.1D]

The TOE shall be suitable for testing. [ATE_IND.2.1C]

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]

5.2.7 Vulnerability Assessment (AVA)

5.2.7.1. Validation of Analysis (AVA_MSU.2)

The developer shall provide guidance documentation. [AVA_MSU.2.1D]

The developer shall document an analysis of the guidance documentation. [AVA_MSU.2.2D]

The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation. [AVA_MSU.2.1C]

The guidance documentation shall be complete, clear, consistent and reasonable. [AVA_MSU.2.2C]

The guidance documentation shall list all assumptions about the intended environment. [AVA_MSU.2.3C]

The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls). [AVA_MSU.2.4C]

The analysis documentation shall demonstrate that the guidance documentation is complete. [AVA_MSU.2.5C]

5.2.7.2. Strength of TOE Security Function Evaluation (AVA_SOF.1)

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 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]

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]

5.2.7.3. Independent Vulnerability Analysis (AVA_VLA.2)

The developer shall perform a vulnerability analysis. [AVA_VLA.2.1D]

The developer shall provide vulnerability analysis documentation. [AVA_VLA.2.2D]

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. $^{\text{AVA\_VLA.2.1C}}$

The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities. $^{\text{AVA\_VLA.2.2C}}$

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. $^{\text{AVA\_VLA.2.3C}}$

The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks. $^{\text{AVA\_VLA.2.4C}}$

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 [*asymmetric 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 [*Authorized 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 is granted; If a user is not successfully authenticated, then access to Protected Token Data is denied*]. FDP_ACF.1.2

The TSF shall explicitly authorize 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

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 Statement of 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.

Configurable items are indicated in italics within brackets.

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.

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 [*a configurable number of*] 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 [*a configurable period of time*].
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 Storage 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.

6.2.2 Windows Local User and Group Management Extension Authentication

This function:

1. 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.
2. Synchronizes the pre-boot user Authentication information when a user’s password is changed

through the user and group management facility.

6.2.3 Secure Administration (Secure_Admin) <SF2>

This function allows an authenticated OE 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 Storage that is to be protected. This may include "No encryption" or "Protect Full Drive".

6.2.4 Protection of Data (Data_Protection) <SF3>

This function:

1. Encrypts and decrypts data, as it is being written to or read from a storage device, in accordance with the TOE configuration, and
2. Controls access to the computer input and output devices, in accordance with the user access control attributes.

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

6.2.5 Statement of Assurance Measures

This section specifies the assurance measures of the TOE which are claimed to satisfy the assurance measures stated in section 5.2 TOE Security Assurance Requirements.

Table 6.1 below associates assurance requirements to the measures that contribute to the satisfaction of the requirements and provides references to relevant supporting documents.

EAL4 Assurance Measure	How Assurance Measure is Satisfied	Describing Document
ACM_AUT.1	SafeNet uses a combination of tools to automate control of changes to the TOE during development and maintenance.	ProtectDrive Configuration Management Plan
ACM_CAP.4	SafeNet uses a controlled system of unique identifiers to label the TOE and its associated configuration items. The referenced CM plan describes how the CM system is used, how identifiers are used and managed, how the CM system supports generation of the TOE and how acceptance of a new version of the TOE is managed.	ProtectDrive Configuration Management Plan
ACM_SCP.2	Coverage of SafeNet’s change control tools includes the TOE, TOE flaw management and control of assurance components.	ProtectDrive Configuration Management Plan
ADO_DEL.2	The Delivery Procedures describes procedures for validation of TOE integrity, though use of a cryptographic process, against substitution or modification during distribution to a user’s site.	ProtectDrive Delivery Procedures

EAL4 Assurance Measure	How Assurance Measure is Satisfied	Describing Document
ADO_IGS.1	The TOE user manual documents procedures and steps for secure installation of the TOE.	ProtectDrive User Manual
ADV_FSP.2	The TOE functional specification provides a complete informal description of the TOE security functions through a description of the purpose and method of use of all TSF interfaces and details of effects, exceptions and errors.	ProtectDrive Functional Specification
ADV_HLD.2	The TOE high-level design document describes the TOE in terms of subsystems and provides a description of the security functionally of each subsystem. The descriptions identify all hardware, software and firmware required by the security functions and any supporting functions provided by underlying hardware, firmware or software.	ProtectDrive High-Level Design
ADV_IMP.1	The TOE source code, when considered with the TOE development tools, provides an unambiguous representation of the TOE without further design decisions.	ProtectDrive Source code ProtectDrive Life-Cycle Management Plan
ADV_LLD.1	The TOE low-level design document describes the TOE in terms of modules that are a refinement of the high-level design. The description includes the inter-relationship between modules and how each TSP-enforcing function is provided.	ProtectDrive Low-Level Design
ADV_RCR.1	Each of the TOE design documents includes a section that describes the correspondence between adjacent design documents.	ProtectDrive Security Target (this document) ProtectDrive Functional Specification ProtectDrive High-Level Design ProtectDrive Low-Level Design ProtectDrive Source code
ADV_SPM.1	The TOE Security Policy model describes the rules and characteristics of all TOE security policies that can be modelled and related these to the TOE Functional Specification	ProtectDrive Security Policy Model
AGD_ADM.1	The TOE user manual includes sufficient information to allow an administrator to securely administer the TOE.	ProtectDrive User Manual
ADG_USR.1	The TOE user manual includes sufficient guidance to enable users to securely use the TOE.	ProtectDrive User Manual
ALC_DVS.1	The TOE Life-Cycle Management Plan describes the security measures implemented to provide adequate confidentiality and integrity of the TOE development environment	ProtectDrive Life-Cycle Management Plan

EAL4 Assurance Measure	How Assurance Measure is Satisfied	Describing Document
ALC_LCD.1	The TOE Life-Cycle Management Plan describes the development approach used for the TOE and includes use of procedures, tools and techniques.	ProtectDrive Life-Cycle Management Plan
ALC_TAT.1	The TOE Life-Cycle Management Plan includes well defined details of all development tools and their implementation as used with the TOE development	ProtectDrive Life-Cycle Management Plan
ATE_COV.2	The TOE test plan provides tests that adequately test all TOE security functions.	ProtectDrive Test Plan
ATE_DPT.1	The TOE test plan provides tests that adequately and completely test the interfaces and functionally describes in the TOE High-Level Design	ProtectDrive Test Plan
ATE_FUN.1	The TOE test plan includes test plans, test procedures, expected test results and actual test results. The test plan provides correspondence between the functions being tested and the tests used.	ProtectDrive Test Plan
ATE_IND.2	Provide the TOE for testing.	TOE ProtectDrive User Manual ProtectDrive Test Plan
AVA.MSU.2	The TOE user manual provides comprehensive guidance for the secure operation of the TOE in all modes of operation.	ProtectDrive User Manual ProtectDrive Misuse Analysis
AVA_SOF.1	The TOE SOF analysis verifies that the strength of TOE mechanisms (that are subject to SOF analysis) meet or exceed the specific SOF defined in the TOE Security Target.	ProtectDrive Strength of Function Analysis
AVA_VLA.2	The TOE Vulnerability analysis is an analysis of the TOE and associated documentation to demonstrate that there are no obvious way to violate the TSP.	ProtectDrive Vulnerability Analysis

Table 6.1 – Assurance Measures

7. PROTECTION PROFILE CLAIMS

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

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, Organizational Security Policies (OSPs) (none in this instance) and Assumptions against the TOE security objectives which are intended to address them.

Table 8.2 cross-references the Threats, OSPs (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 following 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.Encrypt_Data	T.Hack_Storage
O.Interface_Protection	T.User_Err_Res
O.I&A_User	T.Hack_AC_Weak

Table 8.1 – TOE Security Objectives

Objective	Threat or Assumption
OE.Connect	A.Peer
OE.Guidance	A.Administator, T.User_Err_Res
OE.Tamper_ID	A.Tamper_ID, T.Hack_Spoof_Login
OE.Training	A.Administrator, T.User_err_Res
OE.Token	T.Hack_AC_Weak
OE.User_Guidance	A.Authorized_User, T.User_Err_res
OE.User_Identification	A.Administrator, A.Authorized_User

Table 8.2 – Environmental Security Objectives

8.2.2 Assumptions and Threats

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.

8.2.2.1. Assumptions

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.Authorized_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 and identifying that sending protected information over a connected network will not compromise the information.
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

8.2.2.2. Threats

Threat	Rationale
T.Hack_AC_Weak	O.I&A_User and OE.Token address the threat of a hacker gaining access through weak access controls by Identifying and Authenticating authorized users.
T.Hack_Storage	O.Encrypt_Data addresses the Storage Hacking threat by encrypting data before it is written to the Storage, making the data unreadable to a hacker.
T.Hack_Spoof_Login	OE.Tamper_ID addresses the Spoof Login threat by alerting 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.Interface_Protection, OE.Guidance and OE.Training address the User Resource Error Threat by allowing controlled access to selected physical interfaces while permitting other interfaces to be locked out entirely though the operating system or organizational policy.

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

Tables 8.6 and 8.7 cross-reference each security objective for the TOE and the TOE environment with the SFR or SFRs that satisfies it.

It is evident from these two tables that each SFR addresses at least one security objective and that each security objective is addressed by at least one SFR.

Objective	SFR
O.Encrypt_Data	FCS_CKM.1 FCS_CKM.4 FCS_COP.1 FDP_ACC.2
O.Interface_Protection	FDP_ACF.1 FIA_ATD.1 FMT_MSA.1 FMT_MSA.2 FMT_MSA.3 FMT_SMF.1
O.I&A_User	FIA_AFL.1 FIA_UAU.2 FIA_UAU.4 FIA_UAU.5 FIA_UAU.7 FIA_UID.2

Table 8.5 – TOE Security objectives – SFRs

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

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.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 encrypted data. These requirements work together to ensure that only authenticated users can access encrypted data.
O.Interface_Protection	FDP_ACF.1 restricts access to resources to authenticated users with resource access attributes. FIA_ATD.1 requires that a list of access attributes be maintained for users. FMT_MSA.1 restricts the right to change access attributes to the administrator. FMT_MSA.2 ensures that only secure values are accepted for attributes. FMT_MSA.3 ensures that secure values accepted for attributes are either permissive or restrictive in nature. FMT_SMF.1 requires the capability for management of user and system security related attributes. These requirements work together to control access to resources to authenticated users who have been granted explicate access attribute and to restrict control of attributes management to administrators.
O.I&A_User	FIA_AFL.1 restricts access attempts after sequential authentication failures. FIA_UAU.2 requires that a user be authenticated before the TOE allows any further TSF-mediated actions on behalf of the user. FIA_UAU.4 prevents reuse of information that is intended for single use authentication purposes. FIA_UAU.5 provides multiple ways for the TOE to identify a user's claimed identity. 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. 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
OE.Token	OE.FCS_COP.1 provides cryptographic operations to decrypt data. OE.FDP_ACC.2 enforces that only authorized 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 only authenticated users can access Token functionality and decrypted Token data.

Table 8.8 – Suitability of Environmental SFRs Satisfy Environmental Security Objectives

8.3.2 Security Assurance Requirements

The target evaluation level of CC EAL 4 provides a “moderate to high 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 4. The documentation provided by the developer as listed in Table 6.1 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 below displays all functional dependencies required by the TOE and the IT Environment.

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 (14)
2	FCS_CKM.4	FCS_CKM.1 FMT_MSA.2	FCS_CKM.1 (1) FMT_MSA.2 (14)
3	FCS_COP.1	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	FCS_CKM.1 (1) FCS_CKM.4 (2) FMT_MSA.2 (14)
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) FMT_MSA.3 (15)

Id	**Component**	**Dependencies**	**Dependency fulfilled by**
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 (12)
9	FIA_UAU.4	No Dependency	
10	FIA_UAU.5	No Dependency	
11	FIA_UAU.7	FIA_UAU.1	FIA_UAU.2 (8)
12	FIA_UID.2	No Dependency	
13	FMT_MSA.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	FDP_ACC.2 (4) FMT_SMF.1 (17) FMT_SMR.1 (16)
14	FMT_MSA.2	FDP_ACC.1 FMT_MSA.1 FMT_SMR.1 ADV_SPM.1	FDP_ACC.2 (4) FMT_MSA.1 (13) FMT_SMR.1 (16) (ADV_SPM.1)
15	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 (13) FMT_SMR.1 (16)
16	FMT_SMR.1	FIA_UID.1	FIA_UID.2 (12)
17	FMT_SMF.1	No Dependency	
IT Environment Security Functional Components			
19	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)
20	OE.FDP_ACC.2	FDP_ACF.1	OE.FDP_ACF.1 (21)
21	OE.FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	OE.FDP_ACC.2 (20) OE fulfilment (see note below)
22	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 Organizational 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:

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 is internally consistent and includes 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.

No claim as to the SOF of cryptographic algorithms is made as these are outside the scope of the CC. [ASE_REQ.1-15]

The SOF of Basic for the TOE Identification and Authentication function is consistent with identified threats to the TOE 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.4	X		
FIA_UAU.5	X		
FIA_UAU.7	X		
FIA_UID.2	X		
FMT_MSA.1		X	
FMT_MSA.2		X	

SFR	<SF1>	<SF2>	<SF3>
FMT_MSA.3		X	
FMT_SMF.1		X	
FMT_SMR.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 4 are 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 fulfill 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 EAL 4 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.

9. APPENDIX A: GLOSSARY

Boot Record	See Master Boot Record
AES	Advanced Encryption Standard
DEA	Data Encryption Algorithm (another name for DES)
DES	Data Encryption Standard (also see DEA)
Device Class	Microsoft Windows© device classes. Management of device class access in ProtectDrive is through the ProtectDrive management console. The devices controlled are: CD ROM; Diskettes; Removable Media; Scanners; Printers; Modems; Parallel ports; Serial Ports; Tape Drives and Smart Cards.
EAL	Evaluation Assurance Level
GINA	Microsoft Windows© Graphical Identification and Authentication library
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 Storage read and write operations, and also manages all other ProtectDrive functions that require such an interface.
TDEA	Triple DES algorithm (also see DEA)
User	Any person (authorised or unauthorised) attempting to use a machine on which the TOE is installed.
VROM	VROM is the user authentication module of ProtectDrive that is invoked during the boot process.
VXBIOS	Virtual eXtended BIOS. A BIOS extension used by ProtectDrive.