Security Target

for

Reflex Magnetics Disknet Pro

version 4.50.1

Author	Reflex Magnetics Limited
Valid on	25th April 2005
Status	12th DRAFT
Deliverability	EXTERNAL
File number	REFLEX.DN.PRO
Issue Number	2.6
Page Count	49

Signed (Author)

Authorised

(this page is intentionally left blank)

DOCUMENT CONTROL

Document Title	Reflex Magnetics Disknet Pro Version 4.50.1 Security Target

VERSION	DATE	DESCRIPTION
0.A	3rd August 2004	First draft for EDS review
0.B	24th September 2004	Various updates from EDS meeting
0.C	13th October 2004	Fine tuning after second EDS review
1.0	15th October 2004	First version release to EDS
1.1	20th October 2004	Second release to EDS
2.0	22nd October 2004	First release to evaluators and Certification Body
2.1	21st January 2005	TSM and L3OR-01 amendments
2.2	7th February 2005	Further L3OR-01 amendments
2.3	18th March 2005	Final EDS review amendments
2.4	24th March 2005	Added Assumption E-EnhancedMode and Objective OE-EnhancedMode for new Disknet Pro client version 4.50.1 and reflected this change in the overall master version throughout the ST
2.5	31st March 2005	New security function tag [F8.4] for RMM's Enhanced Mode. Previous [F8.4] blended into [F8.3]. Updated version of Admin. Help
2.6	25th April 2005	Implemented the omitted SFR FMT_MSA.1

TABLE OF CONTENTS

REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation Parts 1-3, Version 2.2, January 2004.

[Admin] Reflex Disknet Pro4, Reflex Disknet Pro Administrator Guide, Version 1.9, Reflex Magnetics Ltd, January 2005. Available in hardcopy or by pressing F1 where RDP Server is installed.

GLOSSARY AND TERMS

AD	Active Directory
Assets	Information (data) or resources to be protected by the countermeasures of a TOE.
ATA	Advanced Technology Attachment, a disk drive implementation that integrates the controller on the disk drive itself.
Authorisation	The process through which a removable media device is passed in order to be allowed for use.
Authorised Administrator	A user or subset of authorised users who have authority to administer all aspects of the TOE relative to installation, configuration and use. An Administrator also has the authority to maintain the system, including access to a system's components.
Authorised User	A legitimate user who has been granted physical access to the TOE.
CC	Common Criteria
CM	Configuration Management
DAC	Discretionary Access Control (as implemented by the MS Windows operating system (in the case of this TOE).
Data Scanner	An intelligent scanner which examines removable media devices for executable code. Used in the authorisation process.
EAL	Evaluation Assurance Level
Executable Code	A file in a format that the computer can directly execute. Unlike source files, executable files cannot be read by humans. To transform a source file into an executable file, you need to pass it through a compiler or assembler.
FIPS	Federal Information Processing Standard
HD(D)	Hard Disk (Drive)
IE	Internet Explorer
IT	Information Technology
LAN	Local Area Network
MBR	Master Boot Record
MMC	Microsoft Management Console
MS	Microsoft
MySQL	(My) Structured Query Language, an open-source RDBMS that relies on SQL for processing the data in a database.
OS	Operating System

PG	Port Guard
PP	Protection Profile
Product	The RMM, PSG, PG and DataScan software components of the Reflex Disknet Pro Client product and the Reflex Disknet Pro Server product.
PSG	Program Security Guard
RDBMS	Relational Database Management System
RDP	Reflex Disknet Pro
REFLEX-PROGRAM-PORT-MEDIA-SFP	This security functional policy defines what a user within the TOE domain can and cannot do as regards the import (and execution) of executable and\or viral code to a client machine, access to the devices attached to a client machine and import of removable media to a client machine (specifically, the data held on this media, i.e. is it safe data or executable\viral code).
Removable Media Device	Any device capable of maintaining a file system in which data or resources could be stored.
Resources	All programs or program code installed on the machine housing the TOE.
RMM	Removable Media Manager
SARs	Security Assurance Requirements
Security Policy	The set of rules and practices that regulate what a user is allowed to have access to and will further define what functions a user can accomplish.
Server Software	The Reflex Disknet Pro Enterprise Server, which is controlled via a MS Management Console (MMC) by the Administrator used to configure Security Profiles (SP) for users and user groups.
SFP	Security Functional Policy
SFRs	Security Functional Requirements
Signature	A hash value combined with a unique ID, which RDP uses to mark authorised removable media devices.
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function
SP	Security Profile
SQL	A standardised Structured Query Language for requesting information from a database.
SSPI	Security Support Provider Interface. SSPI is a functionality provided by MS Windows to protect the TOE network connections.
ST	Security Target

SyOPs	Security Operating Procedures
System	A specific environment, which includes an installation of the TOE, together with appropriate operating software.
TOE	Target of Evaluation
TSC	TSFs' Scope of Control
TSF	TOE Security Functions
UDF	Universal Disk Format

1.0 INTRODUCTION TO THE SECURITY TARGET

1.1 ST Identification

Document Title: Security Target for Reflex Magnetics Disknet Pro v4.50.1

Product: Reflex Disknet Pro

Version: 4.50.1

Developer: Reflex Magnetics Ltd.

Components: Reflex Disknet Pro Enterprise Client, version 4.50.1
Reflex Disknet Pro Enterprise Server, version 4.50

Platform: Microsoft Windows XP Professional (Service Packs 1 and 2), for this evaluation.

Evaluation Assurance Level (EAL):
This TOE is CC Part 3, for a product with a target evaluation level of EAL2.

Common Criteria Identification:
Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004.

1.2 ST Overview

(1) Reflex Disknet Pro (RDP) is a unique corporate solution that provides a policy driven mechanism of securing an organisation's information and ensures data integrity.

(2) Each client machine within the RDP domain houses software components that handle specific areas of system security. These components can be controlled remotely by authorised Administrators from Disknet Pro Server or Disknet Pro Administration Console machines, upon which all client activity is selectively recorded for auditing.

(3) Specifically, the RDP product is intended to perform the following functions:

- To ensure that the appropriate Security Profile (SP) is applied to a user at logon.
- To control access to I\O Ports by providing no access, read-only access and full-access options.
- To ensure that only authorised removable media devices can be accessed by authorised users. Whereby every item of removable media in the RDP-protected environment has to be scanned and signatured before a user can access it (optical media is an exception where access is either 'no access', 'read-only' or 'full' whereupon all file transfers can be audited). When authorised removable media has had files modified or written to it outside of the RDP protected environment, the device signature will be invalidated and will need to be re-authorised before access is permitted again.
- To ensure that any user cannot modify or delete resident programs on the machine executing the TOE.
- To prevent new executable code or specific file types from being written to the hard drive or any connected drive unless via an authorised deployment tool. This may include malicious software, or other non-malicious software, which, for example, comes from other departments of the organisation or external third party contacts.

1.3 CC Conformance Claim

(4) This ST is CC Part 2 and CC Part 3 conformant and the assurance level is EAL2.

2.0 TOE DESCRIPTION

2.1 TOE Functionality

(5) Reflex Disknet Pro provides security functionality that allows the peripherals, media and files that can be attached or introduced onto users' workstation to be controlled and monitored on a per user basis via a centrally maintained policy. More detailed information on the controls provided by the product is given in section six of this ST and in [Admin]. Via these means various threats to the integrity of a system and its data may be countered, usually by being directly prevented or in some cases by being reported as audit events.

(6) Reflex Disknet Pro is based upon a client\server model of service. With security policies being defined and monitored at a central server and enforced at the distributed clients.

(7) The Reflex Disknet Pro Server software will be hosted upon a machine(s) (running either a Microsoft Windows Server or Workstation operating system) that can be generally accessed within a Microsoft Windows Domain.

(8) The Reflex Disknet Pro Server provides the capability for:

- Maintaining Disknet Pro security profiles co-ordinated with the users and groups established within the Windows Domain.
- Serving profiles to Reflex Disknet Pro clients as users logon to the network.
- Monitoring the status of Disknet usage throughout the network.
- A central repository for audit records raised by the Disknet clients.
- Tools for searching and maintaining the audit log.
- Forwarding alarms as emails to selected Administrators.

(9) The Reflex Disknet Pro Server consists of 3 components:

- The Disknet Pro Server itself that communicates with the Reflex clients and integrates the other server components.
- The Disknet Pro Administration Console (the Administrative user interface) provided by a standard plug-in to the Microsoft Management Console.
- A MySQL relational database server for the recording and maintenance of profile data and for the storage and review of audit (accounting) records.

These components can be installed upon the same host or upon communicating machines within the same domain.

(10) The Reflex Disknet Pro client software will be installed upon the end user workstations within the domain. The Reflex Disknet Pro client will be started as a service when the workstation is booted up and will perform the following activities:

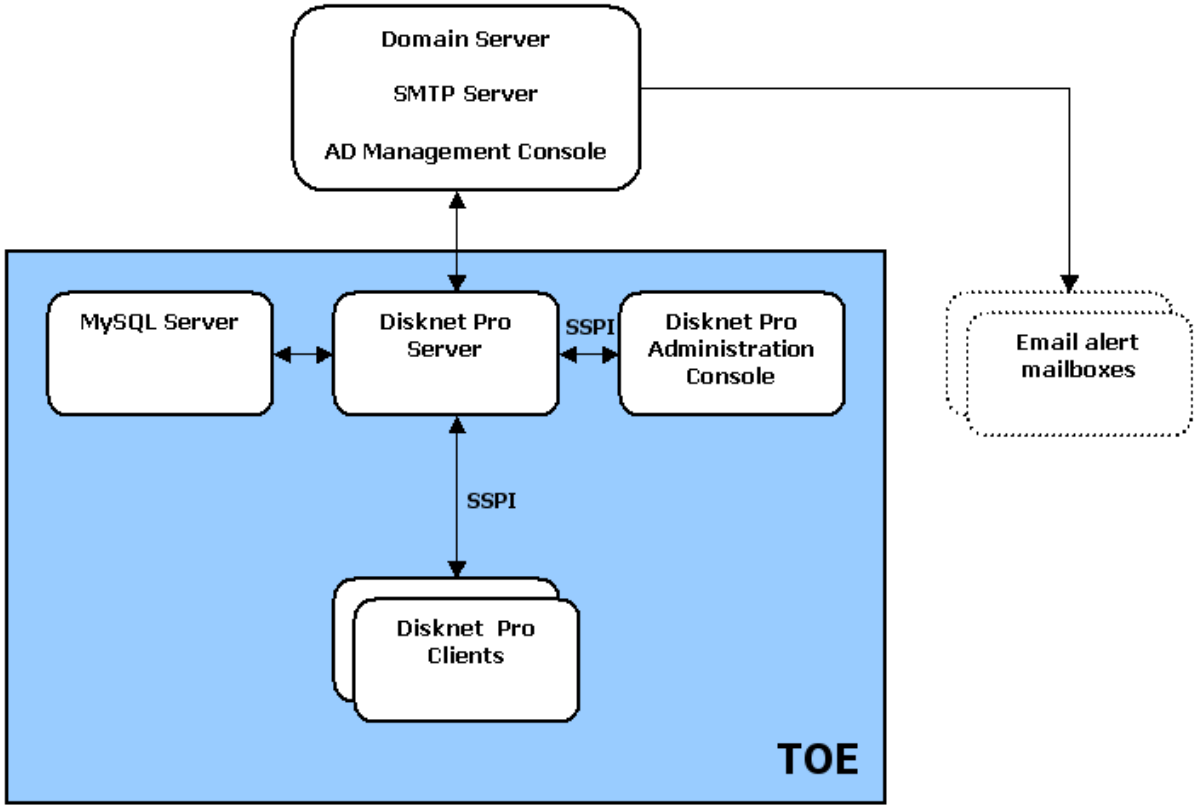
- Provide default protection where a user has no profile or a current profile could not be downloaded.
- Will download the Disknet policy associated with the user, when a user logs at a workstation.
- Will enforce the policy specified by the downloaded policy controlling:
    - access to the I\O ports on the workstation,
    - the file types that can be written to file systems, either local to the machine or upon mapped network drives;
    - how the user can interact with media, authorised for use within the domain.
- Will create audit records of events as specified by the policy and forward audit records to the server at the frequency defined by the policy.
- Will respond to communications originated by the Reflex Disknet Pro server, including status requests and forced downloads of new profiles.

2.2 TOE Architecture

(11) There are numerous server configurations to consider when deploying Reflex Disknet Pro, which one to adopt will normally be dictated by the existing domain setup.

(12) For this evaluation, the TOE will comprise the components as detailed in the blue shaded area in the diagram below. The scope does not include configurations where there are multiple instances of MySQL servers, Disknet Pro servers or Disknet Pro Administration Consoles.

(13) The Domain, MySQL, SMTP and Disknet Pro Server components may be on the same or separate machines. This also holds true for the Disknet Pro Administration Console(s), which can reside on one or more machines for authorised Administrator use.



(14) This simple LAN diagram shows that the Domain Server will also house the SMTP Server and the AD Management Console for this evaluation.

(15) The interactions between the shown components are as follows:

1. The Disknet Pro Server (under authorised Administrator direction) requests domain users and groups from the Domain Server to furnish its user base. This request will be synchronised at regular intervals to keep the RDP Server in line with the Domain Server.

2. The Disknet Pro Console will perform server tasks throughout the evaluation. These requests will be carried via the secure SSPI connection to the Disknet Pro Server and be deployed to the connected Disknet Pro Clients in the form of a security profile.

3. The Disknet Pro Client machines will enforce Disknet Pro policy as governed by their respective security profiles and communicate details of user activity to the Disknet Pro Server. The Disknet Pro Server will audit (policy specific) events for monitoring purposes.

4. The MySQL Server holds the MySQL database that stores user, group, profile and auditing data as fed from and updated by the Disknet Pro Server. (The only exception to this is the auditing of optical media when it is recording data; these traces are stored on the Disknet Pro Server machine in XML file format.)

5. Specified user events will instigate Disknet Pro Client(s) to relate these actions to the Disknet Pro Server, which directs (optional) email alerts to pre-determined email accounts via the SMTP Server.

2.3 TOE Installation Requirements

(16) This section defines the configuration environment for the TOE. The evaluation configuration comprises:

2.3.1 Software Requirements

(17) The Reflex Disknet Pro Server, version 4.50, and Client software, version 4.50.1. MySQL, version 4.0.20. The MySQL database software and license is included with the RDP software package.

(18) For this evaluation, the RDP Server will be executing on the MS Windows XP Professional platform, (including both Service Packs 1 and 2). The RDP Client machines will also be using the Windows XP Professional platform, (including Service Packs 1 and 2).

(19) The network requirements dictate that a (Primary) Domain Controller or Active Directory host be available for furnishing the RDP Server with group \ client account information. Additionally, if RDP alert functionality is utilised, an SMTP server is also a network requirement for handling the alert messaging.

(20) In all instances it is recommended that the latest Microsoft operating system patches are applied and that the system BIOS is set to prevent booting from floppy disk and CD-ROM.

2.3.2 Hardware Requirements

(21) These are the requirements of the operating systems on which the RDP server suite and RDP client machines will run.

- The RDP Server host machine and any server (MySQL) within the configuration will run the MS Windows XP Professional platform with supporting devices including a Network Interface Card. 256MB+ of RAM is recommended for each server with at least 1GB free HD space per server.

- The RDP Client host machines will run the MS Windows XP Professional platform with supporting devices including a Network Interface Card. 128MB+ of RAM is recommended for each client machine with at least 2MB free HD space. The client hardware must include a non-removable hard disk drive, containing a single partitioned & NTFS formatted hard drive, a CD-ROM drive, a 3.5 inch 1.44 Mb diskette drive and USB Ports.

- Each system must be Pentium class or compatible.

- The system BIOS set-up facilities must be configured to permit booting only from the hard disk drive, and to support password control for System set-up access.

- TCP\IP connectivity.

2.3.3 TOE Features

(22) The TOE features included within the evaluated configuration are:

- **Removable Media Manager (RMM)**
- **Program Security Guard (PSG)**
- **Port Guard (PG)**
- **Data Authorisation Module (DataScan)**
- **Auditing & Monitoring (Disknet Pro Server)**

(23) The following features of the RDP product are not included in the TOE:

- **Encryption Policy Manager (EPM):** this is an optional component that supports encryption of removal media in a manner that is transparent to system users but that protects media should they be lost or stolen. This functionality is excluded from the evaluation, but the AES algorithm is FIPS 197 certified and a full FIPS 140 evaluation of EPM is planned for the first half of 2005.
- **Reflex ScreenMail:** this is a high-security plug-in designed to work with MS Outlook and MS Outlook Express. It provides integrated anti-virus and active code protection for both inbound and outbound e-mails.

2.3.4 Scope of Evaluation

(24) The TOE will be comprised of the Disknet Pro Server, version 4.50, and Disknet Pro Client, version 4.50.1, software executing on machines as detailed above. There will be an additional machine housing the Disknet Pro (Administration) Console and one another with the MySQL server software.

(25) The network environment of the TOE is described in sections 2.3.1\2 and will include an SMTP server and an AD server. For this evaluation, the AD server will reside on the Domain Server, as shown in the above diagram. These environmental components are not considered as part of the TOE. Also, the TOE does not specifically include the underlying operating systems, hardware, SSPI connectivity, SMTP server or MMC software.

3.0 SECURITY ENVIRONMENT

3.1 Assumptions

(26) This section contains the assumptions regarding the security environment and the intended usage of the TOE.

ASSUMPTIONS	
E-Network	The server or workstation hardware and the network that hosts the product components, are protected physically, technically and procedurally in a manner commensurate with their role and the data they hold.
E-OSInstall	That the Microsoft Windows OS for the host platforms has been accurately installed at the versions and patch levels recommended by [Admin].
E-UserAccounts	The user accounts etc. for the network domain within which the product operates have been accurately and appropriately configured, in particular users without system administration responsibilities should not be granted local administration rights to their workstations.
E-Boot	That the BIOS boot protection has been configured for hardware hosting the product components so that it will boot solely from its local internal hard drive. This is particularly true for the Reflex Disknet Pro clients, which are required to start the Disknet service at boot to place the workstation in a protected state. It is recommended that this control be put in place to prevent tampering with the BIOS.
E-Install	The product, for both its server and client components, is installed upon the host server or workstation platforms in accordance with the manufactures guidance. This will ensure that the host OS accounts and DAC will be configured to protect the product and an accurate and secure initial configuration of the product component will be achieved.
E-Admin	That Administrators of the product operate it in accordance with the manufacturer's guidance and local SyOPs in order to maintain the efficient operation of the product and the security functions it provides (e.g. policies should be kept current, audit logs reviewed and regular housekeeping activities performed.)
E-Users	That users, whose policies provide them with more privileges in respect to the operation of the product, such as the ability to authorise media, use the product appropriately and do not abuse the trust and responsibilities associated with these privileges.
E-EnhancedMode	That Administrators leave the Removable Media Manager component's Enhanced Mode operational (as is the default) to ensure maximum security when importing and re-importing media.

Table 3-1

3.2 Threats

(27) This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment.

3.2.1 Assets

- (Sensitive) data held on a TOE machine or held on a removable media device used within the TOE.
- The software configuration, e.g. the operating system, application software and file systems on or accessible from the machines hosting the client component of the TOE.
- The hardware configuration, in terms of the allowed peripherals, of the machines hosting the client component of the TOE.

3.2.2 Threat agent

(28) The following are threat agents for the TOE:

- An attacker who has been granted access to the TOE. In this case, the threat would come from an authenticated user attempting access not granted to them.
- Non-TOE Software, which may introduce threats such as viruses.

3.2.3 Threats countered by the TOE

(29) The Reflex Disknet Pro product is primarily aimed to protect a system from threats arising from the activities of its authorised users within its domain. The activities are those that would result in unauthorised modifications of the configuration of the system which could be incompatible with the security of the system, such as attaching a modem to a workstation or introducing an unwanted executable into the system. The specific threats countered by the TOE are identified in the table below.

THREAT	DESCRIPTION
T-UnAuthorised-Peripherals	That an authorised user will attempt to attach to their workstation an unauthorised peripheral, such as a modem, a printer, a removable storage devices and media etc. in a manner that could compromise the integrity of the system or its data.
T-UnAuthorised-FileTypes	That an authorised user could introduce files of an unauthorised type that would be incompatible with the intended usage policy for the system and which could compromise the security of the system. The most damaging case being that of an executable file whose subsequent execution would compromise the system or its data.
T-UnAuthorised-Media	That an authorised user could exploit access to removable storage devices and media, whose legitimate use is required for the operation of a system, to compromise the system or its data by the introduction or removal of data.

Table 3-2

3.3 Organisational Security Policies

(30) The RDP product is not designed to meet or address any specific organisational security policies.

4.0 SECURITY OBJECTIVES

(31) The security objectives define conditions that must be met to counter threats and cover assumptions and organisational security policies. Threats can be directed against the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the TOE IT Environment

4.1 Security Objectives for the TOE

(32) The security objectives for the RDP product, when it is installed and operated in accordance with the security requirements for the environment, are that it directly addresses the threats previously enumerated. This leads to the following objectives as detailed in the table below.

TOE SECURITY OBJECTIVE	DESCRIPTION
O-Policy-controlled-Port-Access	An authorised user's access to available ports, and thereby their ability to attach peripherals on a workstation, will be subject to a policy assigned specifically to that user.
O-Policy-controlled-File-Types	An authorised user's ability to introduce files of specific types into any file systems within the domain, either local to the workstation or mapped within the domain, will be subject to a policy assigned specifically to that user.
O-Policy-controlled-Media-Access	An authorised user's ability to use removable media, e.g. open, read, write, authorise for use within the system will be subject to a policy assigned specifically to that user.
O-Monitoring-of-Policy-Enforcement	Operation of the controls will be monitored and attempts to violate policy will be subject to audit and detection.

Table 4-1: TOE Security Objectives

4.2 Security Objectives for the Environment

(33) The TOE operating environment must satisfy the following objectives. These objectives are satisfied by procedural or administrative measures:

ENVIRONMENT SECURITY OBJECTIVE	DESCRIPTION
OE-Network	Those responsible for the TOE must ensure that it is protected physically, technically and procedurally in a manner consistent with IT security policy.
OE-OSInstall	Those responsible for the TOE must ensure that the MS Windows OS for the host platforms has been accurately installed at the versions and patch levels recommended by [Admin].
OE-UserAccounts	Those responsible for the TOE must ensure that the user accounts etc. for the network domain within which the product operates have been accurately and appropriately configured, in particular users without system administration responsibilities should not be granted local administration rights to their workstations.
OE-Boot	Those responsible for the TOE must ensure that the BIOS boot protection has been configured for hardware hosting the product components so that it will boot solely from its local internal hard drive.
OE-Install	Those responsible for the TOE must ensure that the product, for both its server and client components, is installed upon the host server or workstation platforms in accordance with the manufacturer's guidance.
OE-Admin	Administrators of the TOE must operate it in accordance with the manufacturer's guidance.
OE-Users	Privileged users, whose policies provide them with more privileges in respect to the operation of the product must use the product appropriately and must not abuse the trust and responsibilities associated with these privileges.
OE-EnhancedMode	Those responsible for the TOE must

	ensure that the product, for its client component, that the Removable Media Manager's Enhanced Mode remains in force (as is the default).

Table 4-2: Security Objectives for the Environment

5.0 IT SECURITY REQUIREMENTS

5.1 TOE Security Functional Requirements

(34) Compliant with [CC] Part 2.

Component	Description
FDP_ACC.1	Subset access control (Reflex Security Policy)
FDP_ACF.1	Security attribute based access control (Reflex Security Policy)
FMT_MSA.1	Management of security attributes (Reflex Security Policy)
FMT_MSA.3	Static attribute initialisation (Reflex Security Policy)
FAU_GEN.1	Audit data generation
FAU_ARP.1	Security Alarms
FAU_SAA.1	Potential violation analysis
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions

Table 5-1: TOE Security Functional Requirements

Please note that text shown below within square brackets represents RDP specialization of the CC SFR statement in which it appears.

(35) FDP_ACC.1 Subset access control (Reflex Security Policy)

FDP_ACC.1.1 The TSF shall enforce the [REFLEX-PROGRAM-PORT-MEDIA-SFP] on:

a) [subjects: processes acting on behalf of an authorised user;

b) objects: file systems (for Program Security Guard);

peripheral ports local to a workstation (for Port Guard), and

removable media (for Removable Media Manager).

c) operations: modify the content of a file system (for Program Security Guard);

access to peripheral port for read and\or write (for Port Guard), and

access to files contained within removable media (for Removable Media Manager).

(36) **FDP_ACF.1 Security attribute based access control (Reflex Security Policy)**

FDP_ACF.1.1 The TSF shall enforce the [REFLEX-PROGRAM-PORT-MEDIA-SFP] to objects based on:

a) [subject security attributes: Reflex Profile appropriate to the authorised user,

b) object security attributes: the removable media, a cryptographic checksum derived from a Media ID key and a digest of the media's content].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[In case of:

Program Security Guard: named processes (subjects) will only be allowed unrestricted access to file systems when they have been explicitly exempted within the currently applied Reflex Profile,

Port Guard: the peripheral ports may be accessed with the level of access, None, Read or Read\Write, explicitly specified within the currently applied Reflex Profile.

Removable Media Manager: Port Guard allows access to the ports associated with the removable media and one of the following holds:

a) The TSF can verify the checksum bound to the removable media.

b) The currently applied Reflex Profile grants the authorised user the privilege to authorise removable media and no anomalies are detected in the scanning of the media.

c) The currently applied Reflex Profile grants the authorised user the privilege to authorise removable media and to bypass media scanning.

]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rule:

[In case of:

Program Security Guard, Port Guard and Removable Media Manager: there is a profile option for each of these components to allow each policy to be disabled as granted by the authorised Administrator.

]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on

[In the case of:

Program Security Guard: subjects attempt to modify files within a file system where the file type (as identified by its file name extension) has been explicitly protected within the currently applied Reflex Profile.

]

(37) **FMT_MSA.1 Management of security attributes**
FMT_MSA.1.1 The TSF shall enforce the [REFLEX-PROGRAM-PORT-MEDIA-SFP] to restrict the ability to [change_default, modify, delete] the security attributes [

a) the Reflex Profiles definitions (this configures policy and audit of policy)]

to [an authorised Administrator].

(38) **FMT_MSA.3 Static attribute initialisation (Reflex Security Policy)**
FMT_MSA.3.1 The TSF shall enforce the [REFLEX-PROGRAM-PORT-MEDIA-SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

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

(39) **FAU_GEN.1 Audit data generation**

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Startup and shutdown of the audit function.

b) all auditable events for the [not specified] level of audit: and

c) [For:

Program Security Guard, blocked file system access attempts,

Port Guard, blocked port access attempts,

RMM,

- attempts to introduce unauthorised media;
- successful media authentication;
- unsuccessful media authentication;
- file system access events for the file systems hosted upon authorised media, and
- CD\DVD Audit.]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity, outcome (success or failure) of the event; and

b. For each audit event type, based upon the auditable event definitions of the functional components included in the ST, [the following details are recorded:

- Date and time of the event
- Type of event
- Subject identity
- The outcome (success or failure) of the event
- The unique ID of the event
- The event source (i.e. from which RDP component)
- Domain\user name
- Host name
- Alert status
- File name(s) written to optical media (for CD\DVD Audit only)]

(40) **FAU_ARP.1 Security Alarms**

FAU_ARP.1.1 The TSF shall [forward an alert via email to specified email addresses] upon detection of a potential violation.

(41) **FAU_SAA.1 Potential violation analysis**

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring the audited events:

a) Accumulation or combination of [no such events specified] known to indicate a potential security violation.

b) [Audit events which have been specified as giving rise to an alert.]

(42) **FAU_SAR.1 Audit review**
FAU_SAR.1.1 The TSF shall provide [an authorised Administrator] with the capability to read [all audit trail data] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

(43) **FAU_SAR.3 Selectable audit review**
FAU_SAR.3.1 The TSF shall provide the ability to perform [searches] of audit data based on:
[rules that select audit records based upon logical combinations ("AND" or "OR") of conditions applied to the different data field provided within a record].

(44) **FAU_SEL.1 Selective audit**
FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [event type]

b) [in the case of events associated file access by RMM, user identity, host identity and type of file access event.].

(45) **FMT_MTD.1 Management of TSF data**
FMT_MTD.1.1 The TSF shall restrict the ability to [change_default, query, modify, delete and archive] the:[

b) Media ID key

c) the Reflex Profiles definitions (this configures policy and audit of policy),

d) the Reflex Group definitions,

e) the Alert definitions, and

f) Audit Log (for this item only archiving allowed)]

to [an authorised Administrator].

(46) **FMT_SMF.1 Specification of Management Functions**
FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

a) Specifying the content of Reflex profiles and their allocation to user groups;

b) Monitoring the operation of Reflex profiles at host platforms;

c) Reviewing and maintaining the audit log, and

d) Specifying alerts.

]

5.2 TOE Security Assurance Requirements

(47) The table below defines the assurance requirements for the TOE. Assurance requirement components are Evaluation Assurance Level (EAL) 2, with no augmentation, from part 3 of the CC me.

Assurance Class	Assurance Components	
Configuration Management	ACM_CAP.2	Configuration items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation and start- up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high- level design
	ADV_RCR.1	Informal correspondence Demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 5-2: TOE SARs

5.3 IT Environment Security Functional Requirements

Component	Description
FPT_STM.1	Reliable Time Stamps
FPT_SEP.1	Domain Separation
FMT_SMR.1	Security Role
FIA_UID.1	User Identification
FPT_ITT.1	Basic internal TSF data transfer protection

Table 5-3: Environmental Security Functional Requirements

(48) **FPT_STM.1 Reliable Time Stamps**

FPT_STM.1.1 The IT environment of TSF shall be able to provide reliable time stamps for its own use.

Application Note: The TOE will use the clock function provided by the platform OS in generating time stamps.

(49) **FPT_SEP.1 Domain Separation**

FPT_SEP.1.1 The IT environment of TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The IT environment of TSF shall enforce separation between the security domains of subjects in the TSC.

Application Note: The TOE will use the DAC and process separation provided by platform OS in addressing this requirement.

(50) **FMT_SMR.1 Security Role**

FMT_SMR.1.1 The IT environment of TSF shall maintain the roles of [authorised Administrator, and authorised users]

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

Application Note: The TOE will employ user accounts and other aspects of the configuration associated with the use of the Windows XP OS to establish its distinguished role.

(51) **FIA_UID.1 User Identification**

FIA_UID.1.1 The IT environment of TSF shall allow [no TSF mediated actions] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The IT environment of TSF shall require each user to be identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note: The TOE user identification will make use of the OS user identification and authentication applied by the Windows XP OS when users log on to a domain.

(52) **FPT_ITT.1 Basic internal TSF data transfer protection**

FPT_ITT.1.1 The IT environment of TSF shall protect TSF data from [modification] when it is transmitted between separate parts of the TOE.

Application Note: The TOE will make use of the SSPI functionality of the Windows XP OS to establish secure communication between its components.

5.4 Strength of Function Claim

(53) A strength of function claim of BASIC is made for the TOE as it includes one directly attackable combinatorial mechanism in the form of a SHA1 digital cryptographic checksum, created by Disknet Pro's RMM component when authenticating media. This checksum is as noted in the TOE Security Functional Requirement, FDP_ACF.1.1.

6.0 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functions

(54) This section describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in Section 5.1.

(55) Individual testable functions are labeled as '[core function.sub-function]' in the left margin. For example, [F2.3]. These sub-functions will provide the traceability for the rationale.

6.1.2 Reflex Disknet Pro Server

[F1.1] This provides the capability for:

a) central definition of the security profiles that describe the specific policy which shall be enforced at a user's workstation.

b) central collection of accounting, in product terminology audit, records and tools for selective inspection of these records. Furthermore, at the server it is possible to identify the workstations and users that are currently connected and, if required, force the occurrence of a refresh of the Disknet Pro security profile at a selected workstation.

(56) The Reflex Disknet Pro server runs as a service on its host, its functionality has been built around a database, implemented using the MySQL relational database server that provides the repository for the structured policy and audit data. The graphical user interface for administering the Reflex Disknet Pro Server and thereby the product is provided by a plug-in for the Microsoft Management Console. The MMC can be collocated with the Reflex Disknet Pro Server or can be installed upon another workstation within the domain.

(57) The Administration Console makes use of the standard MMC conventions for displaying and interacting with the objects that are subject to administration, so for instance properties are set by checking and selecting controls within standard forms. Detailed descriptions of the various displays and menus may be found in the Disknet Administrator's Guide (in hardcopy or by pressing F1); a summary of the functionality supported by the Reflex Disknet Pro Server follows.

6.1.2.1 Profile Definition

(58) The security policy in respect to port, file and media access that should apply to a user is defined and recorded in a profile. A profile will be associated with a named group of users and specific Windows domain users may be associated with Disknet groups in a number of ways:

[F2.1] a) There is a Default group associated with the Default profile, any user who logs on to a Disknet protected client and who has not been assigned a group will be subject to this profile.

[F2.2] b) Users from the Windows domain may be individually assigned to a group.

[F2.3] c) A Disknet group may be explicitly synchronised with a security group specified within the Windows domain. This is the recommended way of assigning groups for the majority of users. The Reflex Disknet Pro server will synchronise with the domain controller at start-up and after a specified interval and, if required, an immediate synchronisation can be forced.

[F2.4] d) A profile may be individually assigned to a specific user, in which case the user will be assigned to the Disknet group of special users.

(59) The policies which will be configured within a profile for a group or a user are the:

- Port Guard Policy
- Program Security Guard Policy
- Removable Media Manager Policy

(60) Descriptions of the controls provided by and configurable for these policies are given in the description of Reflex Disknet Pro Client, below, which is where enforcement of the policy occurs.

6.1.2.2 Audit (accounting)

(61) A set of security audit events is identified in relation to the various Reflex Disknet Pro policies. A Reflex Disknet Pro profile will include an identification of the set of events which are selected for reporting as part of a policy, the set of events which should be reported and the urgency with which they should be reported.

(62) There are two log files:

[F3.1] 1) The Administrator's log records events specifically associated with the Reflex Disknet Pro product.

[F3.2] 2) The RMM Audit log records media access events associated with file systems (opening of files, renaming of files, deletion of files) being monitored by the RMM policy enforcement component.

[F3.3] The selection of media access events for reporting may be further refined via a rule (identifying users, machines, type of access etc.) relevant for reported events.

[F3.4] Audit events are generated at a client and are forwarded, at an interval configurable within the profile, to the server where the log file is stored as a database. The Administration Console provides screens that enable rule-directed searches to be carried out on the audit event logs.

[F3.5] DVD\CDROM auditing is a sub-section of the auditing component whereby all files written to optical media are optionally logged for Administrator review. Optical media auditing is initiated by creating a rule within the 'RMM Audit' tab of the RDP Server console to record these entries in the RMM log when data is written to such media. Most disc burning software is supported, however 'packet write' software isn't currently supported. Therefore, packet write software can be blocked by RDP to prevent the UDF format from working since we cannot audit this format at present. RDP blocks packet write software from working by either:

[F3.6] a) setting PG DVD\CDROM access to RO or

[F3.7] b) setting PG DVD\CDROM access to full access, but with the DVD \ CDROM auditing set on, (i.e. by creating a RMM Audit rule).

[F3.8] In addition, the Reflex Disknet Pro product allows for alarms to be configured, so that selected types of audit event will be forwarded by the server on receipt to selected email addresses.

[F3.9] The Administration Console also supports the management of the log files i.e. the archiving and creation of new logs.

[F3.10] The following information is audited for all events:

- Incremental Log ID (for searching)
- Unique ID
- Date \ Time
- Event Type
- Alert (Yes \ No)
- User ID (within the RDP user database)
- User Name (Windows)
- Hostname (machine)
- Source (from which RDP component)
- Message (other relevant information)

6.1.2.3 Monitoring

[F4.1] The Administration Console provides a list of the machines within the domain where a Reflex Disknet Pro client is active, and identifies if a user is logged on and which user is logged on.

[F4.2] This screen also enables a refresh of the profile applied at the machine.

6.1.3 Reflex Disknet Pro Client

(63) This implements:

a) The mechanisms that perform the enforcement of the port, file and media access policies supported by the product.

b) Reporting of security events and its current status to the Reflex Disknet Pro server.

(64) The Reflex Disknet Pro client is started during boot as a service on its workstation host. In practice, user interaction with the client is dictated by the policy it enforces and there is little in the way of a user interface with the client apart from warning messages, some of which are configurable at the server, when a policy enforcement event occurs.

(65) An 'icon' is displayed within the system tray that indicates installation and start up of the client. By clicking on this icon a number of short menus associated with policy enforcement and various status and help information in respect to the client may be accessed.

[F5.1] When a user logs on, the client downloads the profile assigned to a user. The profile downloaded takes the form of a XML file, this will be protected from interference by the user by the Windows operating system file access controls. When a user for whom no profile has been assigned logs on, the client will enforce a default profile, downloaded at service startup or installation. The default profile can be customised by the Administrator, the default profile that is supplied within the standard installation of the product defines a prohibitive policy for protection, i.e. essentially no access.

[F5.2] The clients will generate audit records as required by the profile it enforces, the majority of the events recorded relate to the policy being enforced and are described in relation to these. However, a number of events relate to the operation of the client service, namely:

a) Service Start-up \ Shutdown

b) Starting Profile Download

c) Profile Download Fail

d) User has enabled \ disabled a system component

[F5.3] The client enforces the security policies (Port Guard, Program Security Guard, RMM) as described in the following paragraphs. Normally these policies are as mandated by the profile and cannot be overridden. However, it is possible to provide, as an option in the profile, the capability for a user to disable some of the policies. This privilege obviously must not be generally granted but can be of value to Administrators who need to modify the configuration of a client workstation.

(66) The policy options are accessed via menus available from the system tray icon, these will normally be inactive for most profiles but for additional protection the profile can be configured to prevent the display of these options.

6.1.3.1 Port Guard (port access security policy)

[F6.1] This component controls access to various peripherals \ ports selectively allowed to users (per profile) the forms of access being None, Read Only or Full (Read \ Write). In general the Port Guard policy is implemented within the User Mode (as opposed to Kernel Mode) of the OS and is independent of the physical transfer protocol such as USB or Firewire used to access the peripheral. The ports & peripherals identified are:

- The floppy drive
- Removable hard drives
- Removable storage such as USB memory sticks and ZIP drives
- Optical devices (CDs, DVDs)
- Printer Ports (LPT). (Traditionally, this would just be the parallel port, but in practice any device drivers that implement a local print service can be blocked even though access is provided by an alternative physical route e.g. USB)
- Serial Ports (COM). (Traditionally, the serial port was used to access a modem, but again any device driver that provides a communication-type port will be blocked.)
- Infrared ports (IRDA)
- Other devices, namely CE devices.

[F6.2] RDP can generate audit reports in respect to:

a) Hard disk configuration changed

b) Port guard events (i.e. port access blocking)

c) Removable hard drive file creation and modification (in RMM Audit Log)

6.1.3.2 Program Security Guard (file introduction security policy)

[F7.1] This component provides authorised Administrators with a fully scalable method for preventing the introduction of new, and the modification of existing defined file types within file systems accessible to the user. A forbidden file type will be recognised by the type extension in its filename.

[F7.2] If required, additional file types, i.e. as recognised by an extension, can be defined within a profile. Only three character file extensions are currently supported as other types typically form part of an install package that PSG would prevent from being renamed to executable types anyway, therefore preventing these types from executing. The standard installation of

RDP includes a list of the most common file types and a default profile that blocks the introduction of executable files.

[F7.3] Additionally, the PSG unauthorised execution attempt feature will prevent renamed executable files from executing unless they are running as a system account. This functionality may be suppressed by checking the 'Disable executable process check' option in the PSG tab of a profile.

[F7.4] Since certain programs such as virus checkers and installers will need to create files to perform their functions, the profile allows these to be explicitly exempted from the policy. RDP includes a predefined list of potential exemptions and Administrators can identify further programs.

[F7.5] PSG's settings for unsafe file types and exempted products are stored in a database file that can be stored for backup purposes or for import into another RDP Server.

[F7.6] RDP can generate audit reports in respect to:

a) Unauthorised (PSG) File Operations, i.e. attempts to create by copying or renaming files of forbidden type. Also, the deletion of such file types.

b) Unauthorised program execution

c) Unauthorised execution attempt

6.1.3.3 Removable Media Manager (authorised media security policy)

[F8.1] Removable media (i.e. media without an associated MBR flag) will be authenticated for use within the RDP domain. The use of this MBR flag is determined deep in the ATA specification if a device tells Windows it is fixed (like a HDD) it gets a MBR when formatted.

[F8.2] However, media classed as removable gets no MBR. So, for example, removable hard drives (with MBR) are handled by Port Guard policy and not RMM's.

[F8.3] During authentication a digital cryptographic checksum will be assigned to the media. The checksum will be constructed using a media identification key, which is specific to a system generated during system installation, and data that presents a digest of the particular media files. As long as the media are used within the domain the Reflex Disknet Pro clients will maintain the checksum to be consistent with the media's content. However, if media are modified outside of the domain, i.e. on a machine without a Reflex Disknet Pro client or a client with a different Media ID, then an inconsistent checksum will be generated.

[F8.4] RMM operates in two modes, dependant on RDP's Enhanced Mode status. If Enhanced Mode is operational, it provides read \ write access to files in the first seven-folder levels of a file system, starting from and including the file system root. RMM can read the directory structure beyond these seven levels but will allow no file access. The Enhanced Mode checksum will indicate any changes to the media within this seven-folder level, aside from file renames. When Enhanced Mode is not in operation, RMM will provide access to all of the levels in a file system but the checksum will only indicate significant changes to the media.

[F8.5] The media authentication process, that assigns the digital checksum, will also normally include a scan prior to authentication. The client detects if known anti-virus products are available on the workstation and if so will add the virus scanner(s) into the scanning sequence. Further, RDP incorporates a data scanner that will detect forbidden file types, in particular executables, (see 'Reflex DataScan' later in this section). Successful media scans will be a prerequisite to media authentication.

[F8.6] The RMM policy will block attempts to introduce unauthenticated media or media that fail the authentication check.

[F8.7] Media may be authorised or reauthorised for use within a domain by users, whose profile grant this privilege. Authorisation will be prompted by a simple interface that pops up when unauthorised media are introduced at a workstation. The interface provides a short sequence of screens that guide the user through the process, this allows the user to:

[F8.8] a) Cancel authorisation, the media will remain unauthorised and not be able to be used within the domain.

[F8.9] b) Inspecting the content of media prior to its authentication. As an option in their profiles certain users may be given the capability to delete files from the media at this stage.

[F8.10] c) Inspecting the scans that will be applied as part of authentication. As an option in their profiles certain users may be given the capability to skip the scan from the authentication process at this stage.

[F8.11] As a profile option it is possible to grant users automatic media authentication, which will force a RDP client to attempt authentication of media when these are introduced into the system but give the user no options to control the authentication process. This is useful where it is desirable to provide users with access to removable media but also necessary to ensure that policies for media usage and virus scanning are followed.

[F8.12] Authentication of media audit events that can be configured for the RMM policy are:

a) Unauthorised removable media found

b) Successful media authentication

c) Unsuccessful media authentication

d) Scanner Event

e) Reflex DataScan Event

f) RMM scan skipped

[F8.13] Third party scanners currently supported by RMM for media scanning are to be found in this knowledge base article on Reflex Magnetics' website:
http://www.reflex-magnetics.co.uk/knowledgebase/KBID6039

[F8.14] 'Reflex DataScan' is incorporated into the RMM component, DataScan being a data-only scanner in that it detects, reports & fails all executable code as opposed to just viral code as an anti-virus scanner does. DataScan is optionally used as part of the RMM scanning process when authorising media to be authenticated and signatured for use in the TOE environment.

(67) DataScan has its own profile contained in an XML file, which lists the allowed and disallowed file types as established by the authorised Administrator. Although in reality the default settings are preserved as executable code is – generally speaking - a static entity. This profile is protected by MS Windows XP security by setting the permissions on the user profile(s) on the machine executing the TOE to only allow authorised Administrators write access to the profile file(s).

[F8.15] Whilst authenticated media are tied to the domain hosting the Reflex Disknet Pro server it is possible for an Administrator to export the Media ID string for backup and for reuse within other domains hosting the Reflex Disknet Pro product to allow them to share media.

[F8.16] It is also possible for an Administrator to revoke all previously authorised media, if security has been compromised, thus enforcing re-authorisation of media. This is achieved by changing the Media ID on all machines within the protected environment via the Disknet Pro console. This process may be reversed by re-importing the original Media ID providing a backup was taken during installation.

6.1.3.4 Interaction between components

(68) It should be noted that although to a large degree the various policies described above can be considered and configured as being independent there is interaction between them most notably:

a) The PSG policy will as normally configured prevent the installation of executable file types, this will interfere with the installation of device drivers even with "Plug and Play" if they were not introduced prior to the installation of the Reflex Disknet Pro client. Without the installation of relevant device drivers Port Guard will be unable to provide selective access to peripherals.

b) The RMM policy obviously requires access to the peripherals hosting the removable media, thus where this policy is configured the profile should also allow at least read access to the peripheral type.

c) The PG policy requires PSG to be active to govern the read-only devices as dictated by the profile. Should PSG be disabled in such a profile, any PG read-only devices in that same profile will automatically become full access. The Disknet Pro console will warn the Administrator in such an event.

d) The RMM policy does not authorise removable hard drives but the RMM Audit Log will record any data transfer to\from it. This information is recorded regardless if RMM policy is in force or not, only RMM Audit needs to be active.

6.2 Required Mechanisms

(69) The RMM functionality employs a SHA1 cryptographic hash algorithm as per the TOE Security Function labeled '[F8.3]', (FDP_ACF.1.1). Used as part of the media authentication process and the key associated with this, the Media Identification Key, it is protected by the host OS file system DAC and by procedure.

6.3 Assurance Measures

(70) Deliverables will be produced to comply with the Common Criteria Security Assurance Requirements for EAL2.

7.0 PROTECTION PROFILE (PP) CLAIMS

(71) There are no specific PP claims.

8.0 RATIONALE

8.1 Introduction

(72) This section provides the rationale for the selection, creation, and use of the security policies, objectives and components. Section 8.2 provides the rationale for the existence of the security objectives based upon the stated security policies while Section 8.3 provides the lower-level rationale for the existence of functional and assurance components based upon the stated security objectives. Section 8.4 provides a table to demonstrate that all dependencies between security functional components have been met.

(73) In addition to providing a complete rationale, Section 8 also provides the necessary application notes needed to understand how a TOE must meet the stated security objectives. These application notes provide additional information about a particular family\component\element that a developer or evaluator may need in order to fully understand how the component is to be applied.

8.2 Security Objectives Rationale

(74) The following two tables demonstrate how the objectives of the TOE and the TOE environment counter the threats identified environment counter the threats identified in Section 3.2.

(75) The third, Table 8-3, demonstrates the direct correlation between the (Environmental) Assumptions and the Environmental Objectives that fulfill them by means of the one-to-one mapping shown.

8.2.1 Meeting the threats with the TOE Objectives

TOE Objectives / Threats	O-Policy-controlled-Media-Access	O-Policy-controlled-File-Types	O-Policy-controlled-Port-Access	O-Monitoring-of-Policy-Enforcement
T-UnAuthorised-Media	**X**		**O**	**O**
T-UnAuthorised-FileTypes		**X**		**O**
T-UnAuthorised-Peripherals			**X**	**O**

Table 8-1

Key
X – Direct contribution to meeting a threat
O – Indirect contribution to meeting a threat

The **T-UnAuthorised-Media** threat is met directly by the **O-Policy-controlled-Media-Access** objective, the **O-Monitoring-of-Policy-Enforcement** objective reinforces this by drawing attention

to attempts to bypass policy. The indirect relationship with **O-Policy-controlled-Port-Access** is established as port access is required for a port through which media was expected to be accessed.

T-UnAuthorised-FileTypes has a direct correlation to the **O-Policy-controlled-File-Types** objective, the **O-Monitoring-of-Policy-Enforcement** objective reinforces this by drawing attention to attempts to bypass policy.

The **T-UnAuthorised-Peripherals** threat is directly addressed by the **O-Policy-controlled-Port-Access** objective, the **O-Monitoring-of-Policy-Enforcement** objective reinforces this by drawing attention to attempts to bypass policy.

8.2.2 Meeting the threats with the Environmental Objectives

Environmental Objectives / Threats	OE-Network	OE-OSInstall	OE-UserAccounts	OE-Boot	OE-Install	OE-Admin	OE-Users	OE-EnhancedMode
T-UnAuthorised-Media	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**X**
T-UnAuthorised-FileTypes	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**X**
T-UnAuthorised-Peripherals	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**O**

Table 8-2

Key
O – Indirect contribution to meeting a threat

X – Indirect contribution to meeting a threat

(76) All of the environmental objectives contribute towards countering the threats since if they are not achieved policies could be corrupted or bypassed.

(77) **OE-Network** ensures that an attacker cannot bypass physical access to a server or gain indirect network access so as to try and compromise the security of the TOE.

(78) **OE-OSInstall** is essential for the correct operation of the TOE.

(79) **OE-UserAccounts** ensures that users can be effectively assigned to policies such that their access will not allow them to tamper with the TOE.

(80) **OE-Boot** protects the startup and configuration of the TOE operation upon the hardware on which it is installed.

(81) **OE-Install** confirms that the TOE will operate as expected and both **OE-Admin** and **OE-Users** make sure that the TOE is operated as expected by authorised and competent users.

(82) **OE-EnhancedMode** ensures all removable media changes are detected and those outside its cordon are inaccessible.

8.2.3. Assumptions for the Environment Rationale

Environmental Objectives / Assumptions	OE-Users	OE-Admin	OE-Install	OE-Boot	OE-UserAccounts	OE-OSInstall	OE-Network	OE-EnhancedMode
E-Users	X							
E-Admin		X						
E-Install			X					
E-Boot				X				
E-UserAccounts					X			
E-OSInstall						X		
E-Network							X	
E-EnhancedMode								X

Table 8-3

Key
X – Direct assumption fulfilment by an objective

(83) Security Objectives for the Environment are taken directly from the Assumptions for the Environment since the assumptions identify the environmental constraints that must be achieved to ensure the security of the TOE.

8.3 Security Requirements Rationale

(84) This section provides evidence that demonstrates that the security objectives for the TOE are satisfied by the security requirements.

(85) These mappings demonstrate that all TOE security requirements can be traced back to one or more TOE security objective(s), and, conversely, all TOE security objectives are supported by at least one security requirement.

8.3.1 TOE security functional requirements are appropriate

(86) This section demonstrates that the functional components selected for the TOE provide complete coverage of the defined security objectives. The mapping of components to security objectives is depicted in the following table.

Security Functional Requirements / TOE Objectives	FDP_ACC.1	FDP_ACF.1	FMT_MSA.1	FMT_MSA.3	FAU_GEN.1	FAU_ARP.1	FAU_SAA.1	FAU_SAR.1	FAU_SAR.3	FAU_SEL.1	FMT_MTD.1	FMT_SMF.1
O-Policy-controlled-Port-Access	X	X	X	X								
O-Policy-controlled-File-Types	X	X	X	X								
O-Policy-controlled-Media-Access	X	X	X	X								
O-Monitoring-of-Policy-Enforcement					X	X	X	X	X	X	X	X

Table 8-4: Mapping of TOE Objectives to TOE SFRs

Key
X – Direct contribution to meeting a TOE Objective

(87) **O-Policy-controlled-Port-Access** is fulfilled in part by SFRs FDP_ACC.1 and FDP_ACF.1 since they enforce the Port Guard policy on the users of the TOE and FMT_MSA.1 enables an authorised Administrator to configure this policy. Whilst FMT_MSA.3 insures against network communication issues and the like when enforcing policy by providing default rulings in such circumstances.

(88) **O-Policy-controlled-File-Types** requires SFRs FDP_ACC.1 and FDP_ACF.1 as they enforce the Program Security Guard policy on the users of the TOE and FMT_MSA.1 enables an authorised Administrator to configure this policy. Whilst FMT_MSA.3 insures against network communication issues and the like when enforcing policy by providing default rulings in such circumstances.

(89) **O-Policy-controlled-Media-Access** is catered for by SFRs FDP_ACC.1 and FDP_ACF.1 as they enforce the Removable Media Manager policy on the users of the TOE and FMT_MSA.1 enables an authorised Administrator to configure this policy. Whilst FMT_MSA.3 insures

against network communication issues and the like when enforcing policy by providing default rulings in such circumstances.

(90) **O-Monitoring-of-Policy-Enforcement** is addressed by FAU_GEN.1 and FAU_ARP.1 since these ensure that the TOE will record audit information and raise alerts for selected events. FAU_SAA.1 covers the potential for policy violation. Whereas FAU_SAR.1, FAU_SAR.3 and FAU_SEL.1 fulfill the providing and management of requirements for the policy. FMT_MTD.1 and FMT_SMF.1 provide the ability for an Administrator to define and access the audit information recorded.

8.3.2 IT environment functional requirements are appropriate

Security Functional Requirements / Environmental Objectives	FPT_STM.1	FPT_SEP.1	FMT_SMR.1	FIA_UID.1	FPT_ITT.1
OE-Network		**X**	**X**		
OE-OSInstall	**X**	**X**		**X**	**X**
OE-UserAccounts		**X**	**X**	**X**	
OE-Boot		**O**			
OE-Install		**X**	**X**	**X**	**X**
OE-Admin	**O**		**X**	**X**	
OE-Users					
OE-EnhancedMode	**O**	**X**			**O**

Table 8-5: Mapping of Environmental Objectives to TOE SFRs

Key
X – Direct contribution to meeting an Environmental Objective
O – Indirect contribution to meeting an Environmental Objective

(91) The security requirements for the IT environment will be achieved if the environmental objectives are met.

(92) **FPT_STM.1** will be achieved by the correct installation of hardware and its operating system since it gets its times from the underlying OS and is consistent. OE-OSInstall note: it is assumed that the installation will also involve the correct setting of the time.

(93) **FPT_SEP.1** will be achieved by the correct installation of the TOE and its host OS platform by authorised Administrators, for, once installed, the TOE provides a secure domain within the existing domain infrastructure.

(94) **FMT_SMR.1** will be achieved by the provision of user group accounts from the existing domain in which the TOE operates. The TOE utilises these accounts and their respective privileges to emulate their use within the TOE arena. Authorised Administrators of the TOE will be system users who can logon to the machine where the Reflex Disknet Pro Administration Console is installed and whose permissions allow them access to the MMC for Disknet.
OE-UserAccounts note: TOE user group accounts may optionally be synchronised with the groups within an NT domain, (from which they originally derived).

(95) **FIA_UID.1** will be satisfied by the existing MS Windows security that determines a user's identity, by means of supplying a correct domain username and password, before access to that machine within the TOE domain can be granted.

(96) **FPT_ITT.1** will be achieved by the correct installation of both the Windows XP OS and the TOE. The SSPI functionality provided by Windows will therefore protect the TOE network connections.

8.3.3 Security Requirement dependencies are satisfied

SFR	Dependencies Addressed by TOE	Dependencies by TOE IT environment
TOE SFRs		
FDP_ACC.1	FDP_ACF.1	
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	
FMT_MSA.1	FDP_ACC.1, FMT_SMF.1	FMT_SMR.1
FMT_MSA.3	FMT_MSA.1	FMT_SMR.1
FAU_GEN.1		FPT_STM.1
FAU_ARP.1	FAU_SAA.1	
FAU_SAA.1	FAU_GEN.1	
FAU_SAR.1	FAU_GEN.1	
FAU_SAR.3	FAU_SAR.1	
FAU_SEL.1	FAU_GEN.1, FAU_MTD.1	
FMT_MTD.1	FMT_SMF.1	FMT_SMR.1
FMT_SMF.1	CC identifies no dependencies	
IT Environment SFRs		
FPT_STM.1	CC identifies no dependencies	
FPT_SEP.1	CC identifies no dependencies	
FMT_SMR.1		FIA_UID.1
FIA_UID.1	CC identifies no dependencies	
FPT_ITT.1	CC identifies no dependencies	

Table 8-6: Mapping of SFR Dependencies for the TOE and the IT Environment

(97) All dependencies shown in the above table are those specified by CC Part 2. In the previous section some of the requirements, especially SFRs, have been assigned to the IT Environment because they are essentially addressed by the operating system. The discussion in the previous section provides further details.

8.3.4 Security Requirements are mutually supportive

(98) The only interactions between the security requirements specified for the TOE are those that are identified in the CC Part 2 as dependencies between the SFRs. These dependencies are documented and demonstrated to be satisfied in Section 8.3.2. These interactions are specified in the CC Part 2, and are therefore mutually supportive.

8.3.5 Security assurance requirements rationale

(99) The assurance level EAL2 was selected as providing a moderate level of independently assured security, including confidence that the TOE will not be tampered with during delivery. This level of assurance should be sufficient to allow the TOE to be used to protect unclassified but sensitive information such as that found in government organisations. Such applications require evidence of third party functional and known vulnerability testing, good quality guidance documentation and a well specified external interface.

8.3.6 ST complies with the referenced PPs

(100) This Security Target does not claim compliance with a Protection Profile.

8.4 IT Security Functions Rationale

8.4.1 IT security functions are appropriate

(101) The table below shows the mapping of the TOE Security Functions to the SFRs.

Security Functional Requirement	Security Function
FDP_ACC.1.1	[F6.1] (PG), [F7.1] (PSG), [F8.1] (RMM)
FDP_ACF.1.1 a)	[F2.2], [F2.3], [F2.4]
FDP_ACF.1.1 b)	[F8.3]
FDP_ACF.1.2	[F6.1] (PG), [F7.4] (PSG), [F8.3] -> [F8.10], inclusive, [F8.13], [F8.14] (RMM)
FDP_ACF.1.3	[F5.1], [F5.3]
FDP_ACF.1.4	[F7.1], [F7.2] (PSG)
FMT_MSA.1.1	[F1.1], [F2.1] -> [F2.4], inclusive, [F4.2]
FMT_MSA.3.1	[F2.1]
FMT_MSA.3.2	[F2.2], [F2.3], [F2.4], [F5.2], [F7.1] -> [F7.4], inclusive [F8.6] -> [F8.11], inclusive
FAU_GEN.1.1 a)	[F5.2]

FAU_GEN.1.1 b)	[F5.2], [F3.1] -> [F3.9], inclusive
FAU_GEN.1.1 c)	[F6.2] (PG), [F7.5] (PSG), [F8.12] (RMM)
FAU_GEN.1.2	[F3.2], [F3.10]
FAU_ARP.1.1	[F3.8]
FAU_SAA.1.1	[F3.3]
FAU_SAA.1.2 a)	[F3.1], [F3.2]
FAU_SAA.1.2 b)	[F3.8]
FAU_SAR.1.1	[F1.1]
FAU_SAR.1.2	[F1.1], [F3.1], [F3.2]
FAU_SAR.3.1	[F3.3], [F3.4]
FAU_SEL.1.1	[F3.3] -> [F3.7], inclusive
FMT_MTD.1.1	[F1.1] (since only authorised Administrators have server access) [F7.5], [F8.15], [F8.16]
FMT_SMF.1.1 a)	[F1.1] [F2.1] -> [F2.4] , inclusive, [F4.2]
FMT_SMF.1.1 b)	[F3.1], [F3.2], [F4.1]
FMT_SMF.1.1 c)	[F1.1], [F3.1] -> [F3.10], inclusive
FMT_SMF.1.1 d)	[F3.8]

Table 8-7: Mapping TOE Security Functions to the SFRs

(102) As can be seen by the table above all Security Functional Requirements of the TOE are fully provided by the IT security functions specified in the TOE Summary Specification.

(103) Also demonstrated in Table 8-7, all IT Security Functions identified for the TOE in the TOE Summary Specification are required to meet the TOE Security Functional Requirements.

8.4.2 IT security functions are mutually supportive

(104) The mutually supportive nature of the IT security functions can be derived from the mutual support of the SFRs (as described in Section 8.3.4), as each of the IT functions can be mapped to one or more SFRs, as demonstrated in Table 8-7.

8.4.3 Strength of Function claims are appropriate

(105) A strength of function claim of BASIC is deemed appropriate as Disknet Pro will prevent the anticipated threats from everyday users as detailed in section 3.2.2 of this ST.

9.0 NOTES ON DEVIATIONS FROM CC

(106) This ST has no deviations from version 2.2 of the Common Criteria.