UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P215

REFLEX DISKNET PRO

Version 4.50.1

Issue 1.0

April 2005

UK IT Security Evaluation and Certification Scheme, Certification Body,
CESG, Hubble Road, Cheltenham, GL51 0EX
United Kingdom

ARRANGEMENT ON THE
RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

CERTIFICATION STATEMENT

Reflex Disknet Pro provides a policy driven mechanism for securing an organisation's information and for ensuring data integrity.

Reflex Disknet Pro Version 4.50.1 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL2 for the specified Common Criteria Part 2 conformant functionality in the specified environment, when running on the platforms specified in Annex A.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body UK IT Security Evaluation and Certification Scheme
Date authorised	26 April 2005

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

This list does not include well known IT terms such as LAN, GUI, PC, HTML, ... or standard Common Criteria abbreviations such as TOE, TSF, ... (See Common Criteria Part 1[b], Section 2.3)

ETR	Evaluation Technical Report
MySQL	My Structured Query Language
PG	Port Guard
PSG	Program Security Guard
RMM	Removable Media Manager
SHA	Secure Hashing Algorithm
SSPI	Security Support Provider Interface

(This page is intentionally left blank)

REFERENCES

a. Security Target for Reflex Magnetics Disknet Pro Version 4.50.1,
Reflex Magnetics Limited,
REFLEX.DN.PRO, Issue 2.6, 25 April 2005.

b. Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-001, Version 2.2, January 2004.

c. Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-002, Version 2.2, January 2004.

d. Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-003, Version 2.2, January 2004.

e. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 5.0, July 2002.

f. CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

g. CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 1.0, October 2003.

h. Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-004, Version 2.2, January 2004.

i. LFD/T324 Evaluation Technical Report: Reflex Magnetics Disknet Pro 4.50.1,
EDS Information Assurance,
P23596/T324/R-01/01, Issue 1.0, April 2005.

j. Reflex Disknet Pro 4 Installation Guide,
Reflex Magnetics Limited,
Version 1.4, March 2004.

k. Using Reflex Disknet Pro 4.x with Microsoft Windows XP Professional Service Pack 2,
Reflex Magnetics Limited,
March 2005.

l. Relex Disknet Pro Administrator Guide,
Reflex Magnetics Limited,
Online Help, Version 1.9, March 2005.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Reflex Disknet Pro Version 4.50.1 to the Sponsor, Reflex Magnetics Limited, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [Reference a] which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The version of the product evaluated was:

Reflex Disknet Pro Version 4.50.1.

This product is also described in this report as the Target of Evaluation (TOE). The Developer was Reflex Magnetics Limited.

4. Reflex Disknet Pro provides a policy driven mechanism for securing an organisation's information and ensuring data integrity. The Disknet Pro policy is implemented via a Security Profile associated with each user.

5. Each client machine within the Reflex Disknet Pro domain houses software components that handle specific areas of system security. These components can be controlled remotely by Authorised Administrators using a Disknet Pro Administration Console associated with a Disknet Pro Server, upon which all client activity is selectively recorded for auditing.

6. Specifically, the Reflex Disknet Pro product is intended to perform the following functions:

a. To ensure that the appropriate Security Profile is applied to a user at logon.

b. To control access to I/O Ports by providing no access, read-only access and full-access options.

c. To ensure that only authorised removable media devices can be accessed by authorised users. Every item of removable media in the Reflex Disknet Pro protected environment has to be scanned and given a signature before a user can access it. When authorised removable media have had files modified or written to them outside of the Reflex Disknet Pro protected environment, the device signature will be invalidated and will need to be re-authorised before access is permitted again.

d. To ensure that any user cannot modify or delete resident programs on the machine executing the TOE.

e. 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.

7. Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

8. An overview of the TOE's security architecture can be found in Annex B.

TOE Scope

9. The TOE consists of the Disknet Pro Server Version 4.50 and Disknet Pro Client Version 4.50.1 software. It excludes the MySQL software, underlying Operating Systems and hardware platforms and the SSPI communications between Server and Clients.

10. The features of the TOE which have been evaluated include the following.

a. Removable Media Manager (RMM).

b. Program Security Guard (PSG).

c. Port Guard (PG).

d. Data Authorization Module (Reflex DataScan).

e. Auditing and Monitoring (via the Disknet Pro Server software).

11. The following product features are excluded from the TOE.

a. Encryption Policy Manager, which optionally supports the encryption of removable media.

b. Reflex ScreenMail, which provides antivirus and active code protection for inbound and outbound emails, using Microsoft Outlook or Outlook Express.

12. Where Reflex Disknet Pro invokes proprietary virus scanners the operation of these virus scanners is outside the scope of the TOE.

13. The TOE is assumed to be in an environment with both physical and procedural security measures, with more rigorous requirements being applied to server platforms. It also makes functional assumptions about security features of the Operating System, for example timestamps and domain separation.

Protection Profile Conformance

14. The Security Target [a] did not claim conformance to any protection profile.

Assurance

15. The Security Target [a] specified the assurance requirements for the evaluation. Predefined Evaluation Assurance Level EAL2 was used. Common Criteria Part 3 [d] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [b].

Strength of Function Claims

16. The minimum Strength of Function (SoF) was SoF-Basic. This was claimed for the digital cryptographic checksum used by the RMM component when authenticating media.

17. This mechanism uses an SHA-1 hashing algorithm. This uses information derived from the installation, media and media contents.

Security Policy

18. There are no Organizational Security Policies or rules with which the TOE must comply.

Security Claims

19. The Security Target [a] fully specifies the TOE's security objectives, the threats which these objectives counter and Security Functional Requirements (SFRs) and security functions to elaborate the objectives. All of the SFRs are taken from CC Part 2 [c]; use of this standard facilitates comparison with other evaluated products.

Evaluation Conduct

20. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 [e- g]. The Scheme has established a Certification Body which is managed by CESG on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the Common Criteria Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

21. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [a], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [d] and the Common Evaluation Methodology (CEM) [h].

22. The Certification Body monitored the evaluation which was carried out by the EDS Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the Evaluation Technical Report (ETR) [i] to the Certification Body in April 2005. The Certification Body then produced this Certification Report.

General Points

23. The evaluation addressed the security functionality claimed in the Security Target [a] with reference to the assumed operating environment specified by the Security Target. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

24. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the products and whether such patches have been evaluated and certified.

25. The issue of a Certification Report is not an endorsement of a product.

II. EVALUATION FINDINGS

Introduction

26. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [i] under the CC Part 3 [d] headings. The following sections note considerations that are of particular relevance to consumers.

Delivery

27. There is a single route for delivery, with the product being supplied directly from the Developer to the customer. The product is supplied on a single, shrink-wrapped, sealed CD and is delivered by registered post, courier, or as requested by the client.

28. On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

Installation and Guidance Documentation

29. Installation instructions are provided in the Installation Guide [j]. Additional guidance [k] is provided for installation on Windows XP Pro, with Service Pack 2.

30. Guidance documentation is provided by the online help available with the product [l].

Strength of Function

31. The SoF claim for the TOE was as given above under “Strength of Function Claims”. Based on their examination of all the evaluation deliverables, the Evaluators confirmed that the SoF claim of SoF-Basic was upheld for the digital cryptographic checksum mechanism.

Vulnerability Analysis

32. The Evaluators’ vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

33. Initial evaluation and testing was carried out using Reflex Disknet Pro Version 4.50. Evaluator tests revealed an exploitable vulnerability in this version. Subsequently the Developers produced an updated product, Version 4.50.1, which removed this vulnerability. The Evaluators repeated all necessary work to ensure that previous results of the evaluation were still valid. The Developers repeated all tests on the new version and the Evaluators also repeated their testing.

(This page is intentionally left blank)

III. EVALUATION OUTCOME

Certification Result

34. After due consideration of the ETR [i], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Reflex Disknet Pro Version 4.50.1 in the specified environment meets the Common Criteria Part 3 conformant requirements of EAL2 for the specified Common Criteria Part 2 conformant functionality, when running on the platforms specified in Annex A.

35. The minimum Strength of Function claimed for the digital cryptographic checksum mechanism was SoF-basic. The Certification Body determined that the TOE meets this minimum SoF claim.

Recommendations

36. Prospective consumers of Reflex Disknet Pro Version 4.50.1 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

37. Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under ‘TOE Scope’ and ‘Evaluation Findings’.

38. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

39. The above ‘Evaluation Findings’ include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE consists of the Disknet Pro Server Version 4.50 and Disknet Pro Client Version 4.50.1 software. The Disknet Pro Administration Console is part of the Disknet Pro Server software. Details of the Delivery process are given in Section II under 'Delivery.'

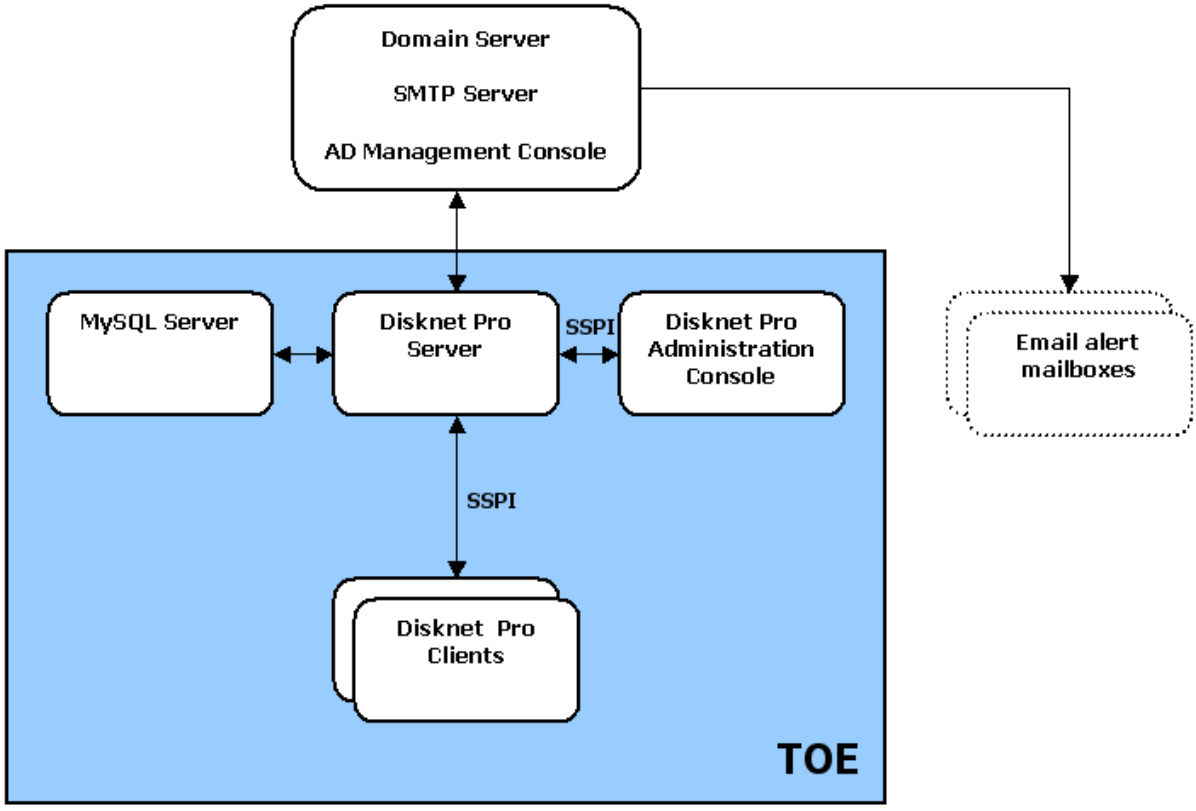
TOE Documentation

2. The main supporting guidance document evaluated was the online guidance provided with the product [l].

3. Further discussion of the supporting guidance material is given in Section II under the heading 'Installation and Guidance Documentation'.

TOE Configuration

4. The evaluated configuration is illustrated in the following diagram:



5. The Disknet Pro Server, Disknet Pro Administration Console and MySQL Server can be on separate platforms or can be combined in a single platform.

6. The Domain Server, SMTP Server and Active Directory Management Console are outside the scope of the TOE. They can be on the same server, as illustrated, or on separate platforms.

Test Configuration

7. The configuration used for all testing consisted of a number of standard PC platforms linked by an Ethernet hub.

8. For initial Developer testing and Evaluator testing on 3 March 2005 and 9 March 2005, the installed version of software was Reflex Disknet Pro Version 4.50.

9. The platforms used were as follows:

a. SRVR-TEST-2K, a Pentium 4, 1.7GHz PC with 512 MB RAM, running Microsoft Windows 2000 Server, acting as **Primary Domain Controller, SMTP Server and Active Directory Management Console**.

b. TEST-PC22-XP, a Pentium 4, 1.5 GHz PC with 256 MB RAM, running Microsoft Windows XP Pro, Service Pack 1, with the **Reflex Disknet Pro Server** software.

c. TEST-PC33-XP, a Pentium 4, 1.7 GHz PC with 256 MB RAM, running Microsoft Windows XP Pro, Service Pack 1, with **the Disknet Pro Administration Console** software.

d. TEST-PC5-2K, a Pentium 2, 400 MHz PC with 163 MB RAM, running Microsoft Windows 2000, Service Pack 4, with the **MySQL Server** software, Version 4.0.20.

e. TEST-PC55-XP, a Pentium 4, 1.5 GHz PC with 256 MB RAM, used for some tests, running Microsoft Windows XP Pro, Service Pack 1, hosting **Disknet Pro Server, Disknet Pro Administration Console and MySQL Server** (Version 4.0.20) software on the same platform.

f. TEST-PC2-2K, a Pentium 4, 1.7 GHz PC with 256 MB RAM, running Microsoft **Windows 2000**, Service Pack 4, acting as a **Reflex Disknet Pro Client**.

g. TEST-PC44-2K, a Pentium 4, 1.5 GHz PC with 256 MB RAM, running Microsoft **Windows 2000**, Service Pack 4, acting as a **Reflex Disknet Pro Client**.

h. TEST-PC3-XP, a Pentium 4, 1.7 GHz PC with 256 MB RAM, running Microsoft **Windows XP Pro**, Service Pack 1, acting as a **Reflex Disknet Pro Client**.

i. TEST-PC4SP2-XP, a Pentium 4, 1.7 GHz PC with 256 MB RAM, running Microsoft **Windows XP Pro**, Service Pack 2, acting as a **Reflex Disknet Pro Client**.

j. SALES-DEM-XP, a Celeron, 1.2 GHz laptop with 256 MB RAM, running Microsoft **Windows XP Pro**, Service Pack 1, acting as a **Reflex Disknet Pro Client**.

10. The only impact of differences with Service Pack 1 and Service Pack 2 is that differences in default firewall settings make the installation process slightly different, as described above

under 'Installation and Guidance Documentation'. As an added check, some further testing was carried out on 18 March, still using Reflex Disknet Pro Version 4.50, with all Windows XP Pro platforms upgraded to Service Pack 2.

11. For repeat Developer and Evaluator Testing from 30 March to 1 April 2005, Version 4.50.1 was installed on all Reflex Disknet Pro Client platforms.

12. The test configuration used is the Developer's test configuration which is also used for testing Windows 2000 clients. For this evaluation, all Reflex Disknet Pro Client tests used Windows XP Pro.

Environmental Configuration

13. This evaluation covered only environmental configurations in which server and client platforms ran under Windows XP Pro, with either Service Pack 1 or Service Pack 2. The product can also be used with Windows 2000, which was not included in this evaluation.

14. Details of the environmental configuration used for testing is included in the section 'Test Configuration' above.

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the main product architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of the report and in Annex A.

Architectural Features

2. The main components, as illustrated in the diagram in Annex A are as follows.

a. The Disknet Pro Server, under the direction of an authorized administrator, requests domain users and groups from the Domain Server to furnish its user base. This request is synchronized at regular intervals to keep the Disknet Pro Server in line with the Domain Server.

b. The Disknet Pro Administration Console carries requests via the secure SSPI connection to the Disknet Pro Server and sets up Security Profiles for the Disknet Pro clients machines and users.

c. Disknet Pro Client machines enforce the Disknet Pro policy as governed by their Security Profiles and communicate details of user activity to the Disknet Pro Server. Policy specific events are audited and monitored by the Disknet Pro Server.

d. The MySQL Server holds the MySQL database that stores user, group profile and auditing data as fed and updated by the Disknet Pro Server. (Note that optical media audit data is held directly on the Disknet Pro Server.)

Design Subsystems

3. The Reflex Disknet Pro Administration Console provides a user interface to the policy database. It can be used for viewing and filtering event logs, configuring server access permissions and other administration tasks.

4. Reflex Disknet Pro Server has the following components:

a. The Disknet Pro Administration Console, as described above.

b. The Disknet Server Service, which performs database management tasks and ensures the integrity of policy information. Operations are only allowed on the policy database if a connected Administration Console has successfully authenticated to the service and holds the necessary privileges.

c. Domain Synchronisation, started at configurable intervals to synchronise Windows group membership with Disknet groups. This uses the MySQL database directly.

d. An Email Alert Trigger component, which communicates between the Disknet Pro Server and the SMTP Server.

5. The main subsystems of Reflex Disknet Pro Client are as follows.

a. Port Guard (PG) is a Microsoft Windows service, which constitutes the port access facility of Reflex Disknet Pro, controlling access to individual ports on the client machines.

b. Program Security Guard (PSG) consists of a kernel mode driver and a notification module. These prevent the creation, modification or deletion of Disknet Pro protected file types, usually executable code.

c. The Removable Media Manager (RMM) consists of a kernel driver, a Microsoft Windows service, a user interface and a user messaging component. When new removable media are introduced into the system, RMM checks and verifies the Disknet Pro signature on the device. The signature is valid if no new files have been added or existing files modified since the last access. If there is no valid signature the authorization process will be started and a new signature will be created.

d. The Data Authorisation Module, Reflex DataScan, a scanner for executable code and other file types.

Hardware and Firmware Dependencies

6. The TOE includes no hardware or firmware components. Reflex Disknet Pro makes use of the Microsoft Windows Operating System which forms part of its environment, as described elsewhere in this Report, and in turn this Operating System relies on its underlying hardware platforms. All communication between the TOE and the hardware is via the Operating System.

TSF Interfaces

7. The main outlet for Administrator use is the Administration Console, which forms part of the Reflex Disknet Pro Server.

8. Communication between the Disknet Server Service, Disknet Pro Administration Console and Disknet Pro Clients uses TCP/IP protocols, encrypted and authenticated by Microsoft SSPI.

9. The Disknet Pro Server also has interfaces with the following.

- The Domain Server.
- The SMTP Server.
- The MySQL Server.
- Additional Administration Consoles.
- Disknet Pro Client machines.

10. Disknet Pro Client has an interface with users, via a menu system with user messages.

11. Disknet Pro Client also has interface as follows.

- With kernel mode operation.
- With device drivers via Port Guard.
- With the system tray, via the Disknet Client service.
- With the user via PSG and RMM.

- With the Data Authorisation Module, Reflex DataScan and other scanners.

12. User interfaces are as follows.

- The Reflex Disknet Pro system tray menu.
- RMM import wizard.
- The Data Authorisation Module, Reflex DataScan.
- Disknet custom messages.
- Third party antivirus software.
- Microsoft Windows messages.

(This page is intentionally left blank)

ANNEX C: PRODUCT TESTING

IT Product Testing

1. Developer tests and Evaluators' repeat tests both tested all major subsystems of Reflex Disknet Pro. Similarly the Evaluators' functional tests and penetration tests covered all major subsystems. Both Developer and Evaluator tests covered all SFRs and all external interfaces.

2. Evaluators used a number of different media types for their tests. The Evaluators also repeated the installation and configuration processes.

3. The Evaluators used the same test configuration as the Developers. Details are given in Annex A under 'Test Configuration.'

4. This configuration enabled the Evaluators to test two configurations - with the MySQL Server and Administration Console on the same server as the Disknet Pro Server, and with three separate servers.

Platform Issues

5. Platforms used for Reflex Disknet Pro Server and Client software, Administration Console software and MySQL Server software can be any PC platforms running Microsoft Windows 2000 or Windows XP Pro Operating Systems.

6. The Evaluators carried out tests with a number of platform configurations and confirmed that results were valid for configurations using Windows XP Pro with Service Packs 1 and 2. All interaction between the software and the hardware is via the Operating Systems and, after evaluating the evidence and the test results, the Evaluators concluded that results are valid for any valid Windows XP Pro platforms using Service Pack 1 or 2.

7. Because of changes to the firewall settings under Windows XP Pro between Service Pack 1 and Service Pack 2, different installation guidance is given for the two Service Packs.

(This page is intentionally left blank)