UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P200

Red Hat Enterprise Linux

Version 3 with security update RHSA-2003:416
running on specified Dell and Hewlett-Packard platforms

Issue 1.0

February 2004

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.

Trademarks:

The following trademarks are acknowledged:

Red Hat is a trademark of Red Hat Incorporated; Oracle is a trademark of the Oracle Corporation, Hewlett-Packard is a trademark of the Hewlett-Packard Company; Dell is a trademark of Dell Incorporated; and Intel is a trademark of the Intel Corporation. All other product or company names are used for identification purposes only and may be trademarks of their respective owners.

CERTIFICATION STATEMENT

Red Hat Enterprise Linux is a commercially available distribution of the Linux operating system.

Red Hat Enterprise Linux Version 3with security update RHSA-2003:416, in its AS, ES and WS variants, has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL2 for the specified Common Criteria Part 2 extended 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	6 February 2004

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

API	Application Programmer Interface
AS	Version of Red Hat Enterprise Linux for large scale deployment
CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
ECG	Evaluated Configuration Guide
ES	Version of Red Hat Enterprise Linux for medium scale deployment
ETR	Evaluation Technical Report
OR	Observation Report
OSP	Organizational Security Policy
SCSI	Small Computer System Interface
SFR	Security Functional Requirement
SoF	Strength of Functions
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UKSP	United Kingdom Scheme Publication
WS	Version of Red Hat Enterprise Linux for workstation use

(This page is intentionally left blank)

REFERENCES

a. Red Hat Enterprise Linux 3: Security Target,
Oracle Corporation,
Version 1.7, January 2004.

b. Common Criteria Part 1,
Common Criteria Interpretations Management Board,
CCIMB-99-031, Version 2.1, August 1999.

c. Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-99-032, Version 2.1, August 1999.

d. Common Criteria Part 3,
Common Criteria Interpretations Management Board,
CCIMB-99-033, Version 2.1, August 1999.

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

f. CLEF Requirements - Startup and Operation,
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,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
Version 1.0, CEM-099/045, August 1999.

i. Evaluation Technical Report: Red Hat Enterprise Linux 3,
Syntegra CLEF,
LFS/T445/ETR, Issue 1.0, 19 December 2003.

j. Addendum to Evaluation Technical Report: Red Hat Enterprise Linux 3,
Syntegra CLEF,
LFS/T445/ETR_A, Issue 1.0, 3 February 2004.

k. User/ Administration Guidance for the Evaluated Configuration of Red Hat Enterprise Linux 3,
Red Hat Incorporated,
Issue 1.5, December 2003.

l. Evaluated Configuration Guide for Red Hat Enterprise Linux 3,
Syntegra,
ECG, Version 1.6, 2 February 2004.

(This page is intentionally left blank)

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Red Hat Enterprise Linux Version 3 to the Sponsor, Oracle Corporation, 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 versions of the product evaluated were:

Red Hat Enterprise Linux AS (Version 3) with security update RHSA-2003:416,
Red Hat Enterprise Linux ES (Version 3) with security update RHSA-2003:416, and
Red Hat Enterprise Linux WS (Version 3) with security update RHSA-2003:416.

These products are also described in this report as the Target of Evaluation (TOE), and they are referred to generically as Red Hat Enterprise Linux Version 3.

4. Linux is a freely available operating system, which has grown through contributions from many international software developers. Red Hat Enterprise Linux is a commercially supported distribution of the operating system, provided by Red Hat Incorporated.

5. The Linux operating system operates a multi-user multi-tasking environment and provides services at several layers. At the lowest level, the Linux kernel interacts with the hardware platform and provides common services to application programs. Linux also provides other basic services including file systems, device drivers, system utilities and user interfaces. (The graphical interfaces provided by Linux are outside the scope of the TOE.)

6. The Linux kernel operates in the processor's privileged mode with full access to all resources of the computer. Other parts of the operating system support code, which do not need to run in privileged mode, are contained in the system libraries. This includes a large number of system utilities and user utilities.

7. Red Hat Enterprise Linux consists of three separate products, built around a common core. These products are;

a. Red Hat Enterprise Linux AS - supporting servers for large departmental and data-centre deployments;

b. Red Hat Enterprise Linux ES - supporting medium scale departmental deployments; and

c. Red Hat Enterprise Linux WS - supporting workstations, suitable for software development[1] or client applications.

8. This evaluation covered the AS, ES and WS variants of Red Hat Enterprise Linux, and included testing on two platforms for each variant - one Dell and one Hewlett-Packard.

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

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

TOE Scope

11. The TOE provides for a level of protection appropriate for an assumed non-hostile and well managed user community. It provides protection against threats of inadvertent or casual attempts to break system security.

12. It is not intended to be applicable to circumstances in which protection is required against determined attempts by well funded hostile attackers to breach security, and it does not fully address the threats posed by malicious system development or administrative personnel.

13. The TOE was evaluated in standalone mode. Most of its network facilities (e.g. DNS, NFS, NIS and Xwindows) were excluded from the evaluated configuration, but the Security Target did include Security Functions (IA.9, IA.10 and IA.11) relating to remote login.

14. The TOE, with support from its IT environment, provides security features in the following areas:

- Identification and Authentication,
- Discretionary Access Control,
- Object Reuse,
- Process Separation, and
- Self-Testing.

15. The following features of Red Hat Enterprise Linux were specifically excluded from the evaluation:

- Apache Web Server;
- Kerberos;
- Crypto IP Encapsulation;
- Nmap;
- LILO;
- Network File System (NFS);
- Domain Name Service (DNS);
- Dynamic Host Configuration Protocol (DHCP);

[1] Note that not all of the functions for software development are permitted in the evaluated configuration of the TOE.

- Network Information System (NIS);
- Automatic updating using Red Hat Up2Date;
- X-Windows graphical interface;
- Support for AppleTalk;
- Support for IPX;
- Red Hat Cluster Manager.

16. Users of Red Hat Enterprise Linux Version 3 should also note that it has not been possible to provide assurance for the Security Function [IA.15] in the Security Target [a]. This function, which states that passwords will be encrypted using the MD5 message-digest algorithm, should be considered as out of the scope of the evaluation. The evaluators could identify that some encryption took place but were not able to test for the use of the MD5 algorithm.

17. For details of the specific platforms evaluated, see Annex C under 'Platform Issues'.

Protection Profile Conformance

18. The Security Target [a] did not claim conformance to any protection profile. (It was based on the Controlled Access Protection Profile, but did not include its full security functional requirements or its full assurance requirements.)

Assurance

19. 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

20. The minimum Strength of Function (SoF) was SoF-Medium. This was claimed for the authentication mechanism, and the following SoF claims were also made.

a. For each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than 1 in 1 000 000.

b. For multiple attempts to use the authentication mechanism during a one minute period, the probability that a random attempt in that minute will succeed is less than 1 in 100 000.

c. Any feedback given during an attempt to use the authentication mechanism will not reduce the probability below the above metrics.

Security Policy

21. The TOE Organizational Security Policies (OSPs) that characterize the TOE Security Policy are detailed in the Security Target [a]. These policies state the following.

a. Only those users who have been authorised to access the information within the system may access the system.

b. The system must limit the access to, modification of, and destruction of the information in protected resources to those authorised users which have a "need to know" for that information.

c. The users of the system shall be held accountable for their actions within the system.

Security Claims

22. The Security Target [a] fully specifies the TOE's security objectives, the OSPs which these objectives meet and security functional requirements and security functions to elaborate the objectives. Most of the SFRs are taken from CC Part 2 [c]; use of this standard facilitates comparison with other evaluated products.

23. Deviations from the wording of CC Part 2 [c], which are fully described in the Security Target [a], are listed below.

a. The SFR FDP_RIP.3 has been added. This is identical to FDP_RIP.2, except that 'objects' has been replaced by 'subjects'.

b. For FIA_USB.1 the expression 'appropriate security attributes' has been replaced with a more explicit list of attributes.

c. For FAU_GEN.1 the auditable events have been presented in a table rather than as a list in order to clarify the information.

Evaluation Conduct

24. 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.

25. 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].

26. The Certification Body monitored the evaluation, which was carried out by the Syntegra Commercial Evaluation Facility (CLEF). The CLEF submitted the Evaluation Technical Report (ETR) [i] to the Certification Body in December 2003.

27. Following the discovery and publication of a kernel memory map vulnerability[2], the Developers issued a security update and the Evaluators reassessed the assurance provided by the updated version of the TOE. (This included further Evaluator testing of the product in its updated form.) They issued an addendum to the ETR [j] which completed the evaluation and the Certification Body then produced this Certification Report.

General Points

28. 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.

29. 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.

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

[2] This vulnerability is identified as CAN-2003-0985 in the Common Vulnerabilities and Exposures database at http://www.cve.mitre.org; and as BugTraq 9356 at http://www.securutyfocus.com. The Red Hat Security identification is RHSA 2003:416.

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

31. 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

32. The Evaluators examined the methods of secure delivery, described below, and checked each delivery process.

a. Physical Delivery.
Three separate product boxes (sealed and shrink wrapped) are supplied for the versions AS, ES and WS of the TOE. Each product box contains the TOE with documentation and instructions, and includes public key information for verifying the TOE. All items are labelled with a unique part number.

b. Electronic Delivery.
Following purchase via the Red Hat web site, an email is sent from Red Hat giving instructions on how to download the product. This process, which can only be completed by registering at the web site with a username and password, also includes the use of public key information for verifying the TOE.

33. The public key information supplied consists of a digital signature, which can be checked at the Red Hat web site http://www.redhat.com/solutions/security/news/publickey.html. The ECG [l] includes instructions for the validation of the software using the digital signature and Gnu Privacy Guard software. (Gnu Privacy Guard software is included with the delivered Red Hat Enterprise Linux software. For greater security, this software can be downloaded independently via the Gnu web site http://www.gnupg.org)

34. Delivery of the security update, RHSA-2003:416, which is described in the ECG [l], also includes the ability to check validity via digital signature using Gnu Privacy Guard.

35. On receipt of the TOE, the user 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

36. The main guidance for users and administrators is provided in 'User/ Administrator Guidance for the Evaluated Configuration for Red Hat Enterprise Linux 3' [k], cross-referenced where relevant to documentation available on-line (through the ***man*** command).

37. Additional information on the secure installation of the evaluated configuration is provided in 'Evaluated Configuration Guide for Red Hat Enterprise Linux 3' (ECG) [l].

38. The evaluated configuration includes a security update as described above under 'Evaluation Conduct'. Instructions on the installation of this update are included in the ECG [l].

Strength of Function

39. The SoF claims for the TOE were as given above under "Strength of Function Claims".

40. Based on their examination of all the evaluation deliverables, the Evaluators confirmed that the authentication mechanism met the strength claim of SoF-medium and the other SoF metrics specified.

Vulnerability Analysis

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

42. The Evaluators carried out penetration testing as part of their vulnerability analysis. They did not identify any exploitable vulnerabilities.

III. EVALUATION OUTCOME

Certification Result

43. 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 Red Hat Enterprise Linux Version 3 with security update RHSA-2003:416, running on specified Dell and Hewlett-Packard platforms meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL2 for the specified Common Criteria Part 2 extended functionality, in the specified environment, when running on the platforms specified in Annex A.

44. The minimum Strength of Function for the authentication mechanism was SoF-medium. The Certification Body has determined that the TOE meets this SoF claim and the claimed SoF metrics.

Recommendations

45. Prospective consumers of Red Hat Enterprise Linux Version 3 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.

46. Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under 'TOE Scope'.

47. Physical access to the configured TOE should be controlled and the TOE hardware and software should be protected from unauthorized modification.

48. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration [k, l].

49. The above 'Evaluation Findings' include 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 Red Hat Enterprise Linux (AS, ES or WS) version 3 For full details of the evaluated configuration, see the ECG [l].

2. The CDROM Part Numbers for Physical Delivery are as follows:

- Red Hat Enterrpise Linux AS for the x86 architecture version 3- Installation CD 1 of 4 - CDR0126US
- Red Hat Enterrpise Linux ES for the x86 architecture version 3- Installation CD 1 of 4 - CDR0131US
- Red Hat Enterrpise Linux WS for the x86 architecture version 3- Installation CD 1 of 4 - CDR0134US-R1
- Red Hat Enterrpise Linux for the x86 architecture version 3- Installation CD 2 of 4 CDR0137US-R2
- Red Hat Enterrpise Linux for the x86 architecture version 3- Installation CD 3 of 4 CDR0142US-R1
- Red Hat Enterrpise Linux for the x86 architecture version 3- Installation CD 4 of 4 CDR0147US-R1

3. Note that the ECG [l] includes instructions for the installation of the security update, RHSA-2003:416.

TOE Documentation

4. Discussion of the supporting guidance material is given in Section II under the heading 'Installation and Guidance Documentation'. (See [k, l].)

TOE Configuration

5. The configuration used for testing was as specified in the ECG [l].

Environmental Configuration

6. For details of the environmental configuration, see the ECG [l].

7. Details of the hardware platforms tested are given in the table below.

TOE Type	Platform	CPU	RAM	Hard Disk	Network Interface(s)
AS	Dell PowerEdge 6650	4 Intel Xeon (2.4 GHz)	4 GBytes	2 at 36 GBytes	2 embedded GB
AS	HP Proliant ML570	2 Intel Xeon (2.5 GHz)	1 GBytes	2 at 72.8 GBytes	HP NC3163 embedded
ES	Dell PowerEdge 2650	2 Intel Xeon (2.4 GHz)	2 GBytes	2 at 33.9 GBytes	2 embedded GB
ES	HP Proliant ML570	2 Intel Xeon (2.5 GHz)	1 GBytes	2 at 72.8 GBytes	HP NC3163 embedded
WS	Dell Precision 650	2 Intel Xeon (2.4 GHz)	2 GBytes	2 at 33.9 GBytes	1 embedded
WS	HP d350	1 Intel Pentium 4 (2.66 GHz)	512 MBytes	1 at 40 GBytes	Integrated Broadcom Ethernet

8. Section 2.3 of the ECG lists all the included software packages with their version numbers. In addition, Section 2.5 of the ECG lists some additional packages which are considered optional to the evaluated configuration. For the Evaluators' testing, all the optional packages were included in the TOE environment. (Note that for WS variants, these additional packages are not permitted and were not loaded for testing.)

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 Linux operating system operates a multi-user multi-tasking environment and provides services at several layers. At the lowest level, the Linux kernel interacts with the hardware platform and provides common services to application programs. Linux also provides other basic services including file systems, device drivers, system utilities and user interfaces. (The graphical interfaces provided by Linux are outside the scope of the TOE.)

3. The Linux kernel operates in the processor's privileged mode with full access to all resources of the computer. Other parts of the operating system support code, which do not need to run in privileged mode, are contained in the system libraries. This includes a large number of system utilities and user utilities.

Design Subsystems

4. The kernel subsystems of Linux are as follows.

   a. The File Input/Output subsystem organises information in block storage devices in directories and files.

   b. The Inter Process Communication subsystem allows processes to communicate with each other.

   c. The Process Control subsystem creates and destroys processes and controls their connections to external systems.

   d. The Memory Management subsystem allocates and frees physical memory and handles virtual memory mapped to the address spaces of running processes.

   e. The Device Drivers subsystem provides interfaces between the kernel and hardware devices.

   f. The Networking subsystem controls the delivery of packets of information across program and network interfaces.

5. Non-kernel subsystems of Linux are as follows.

   a. The System Initialization subsystem - controlling the startup of the operating system.

   b. The Identification and Authentication subsystem - establishing the identity of users and verifying user credentials.

c. The System Administration subsystem- consisting of several programs grouped into subgroups for User Administration, Group Administration, Authentication Administration, Access Control Administration, System Test Utilities, Security and Miscellaneous.

d. The Audit subsystem - containing two separate logging daemons for programming applications and for the kernel.

e. The Schedule subsystem - allowing the administrator to schedule processes to run unattended (consisting of the commands `at`, `cron` and `logrotate`).

Hardware and Firmware Dependencies

6. The evaluation only applies to the platforms identified in Annex C under 'Platform Issues' and excludes the underlying hardware.

7. The Device Drivers subsystem of the Linux kernel includes a number of different drivers for different peripheral hardware types.

8. Assumed hardware dependencies are:

a. The CPU supports two-state processing, allowing the kernel to operate in privileged mode;

b. The CPU and/or motherboard provides a Memory Management Unit to support separate memory spaces for each process;

c. The motherboard includes a battery backup for the clock to maintain time information when the system is shut down;

d. The CPU or other hardware provides a periodic cycle time to support internal time management in the kernel; and

e. network interface cards (if present) are not configured to support special external command features.

TSF Interfaces

9. The external interfaces of the TOE are categorized as:

a. kernel-hardware interfaces; and

b. Application Programmer Interface (API) and shell interfaces.

10. The kernel-hardware interfaces include interfaces to the following hardware:

- keyboard,
- monitor,
- video card,
- network cards,

- processor,
- bus,
- memory,
- hard drive,
- SCSI controller, and
- real-time clock.

11. All communication with users and administrators is via API or shell interfaces.

(This page is intentionally left blank)

ANNEX C: PRODUCT TESTING

IT Product Testing

1. Testing covered only the command line interface of Red Hat Enterprise Linux. Graphical interfaces were out of scope of the evaluation.

2. Each platform under test was connected via a hub to a platform running Red Hat Linux 9 to enable testing the ability to connect to the TOE from a remote source.

3. The Evaluators' testing included repeated Developer testing; Evaluators' independent testing and penetration testing.

4. All initial Developer and Evaluator testing was carried out on Red Hat Enterprise Linux Version 3 without the security update. Following the discovery and publication of a kernel memory map vulnerability, the Developers issued a security update. As part of the Evaluators' reassessment of the assurance provided by the version of the TOE with the security update they carried out further Evaluator testing of the updated product.

Platform Issues

5. Red Hat Enterprise Linux Version 3 is designed to run on a wide range of Intel x86-compatible platforms. (The "Red Hat Ready" program can be used to confirm suitability.) Red Hat Enterprise Linux Version 3 has three variant products to support platforms of different scale.

6. The evaluation included tests on the following hardware platforms. For each variant, testing was carried out on a Dell platform and a Hewlett-Packard platform.

- (AS) Dell PowerEdge 6650 (4 processors)
- (AS) Hewlett-Packard Proliant ML570
- (ES) Dell PowerEdge 2650
- (ES) Hewlett-Packard Proliant ML570
- (WS) Dell Precision 650
- (WS) Hewlett-Packard d530

7. For fuller details of the hardware test platforms, see Annex A.

8. Developer functional testing was carried out only on a Dell Precision 650 running Red Hat Enterprise Linux Version WS 3. The Evaluators repeated these tests on the other platforms listed and performed further independent and penetration tests on each of the platforms listed above.

9. The results of this Evaluation are not claimed to apply to platforms (and associated TOE types) other than those listed in Annex A.

(This page is intentionally left blank)