UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P207

Marconi Selenia Communications MPS

Multi-Protocol Switch: Models 115 & 145 (Software version 1.4 pack 2)

Issue 1.0

July 2004

UK IT Security Evaluation and Certification Scheme Certification Body,
CESG, Hubble Road, Cheltenham, Glos 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. *

* Whilst the Arrangement has not yet been extended to address ALC_FLR.1, a working agreement exists amongst Parties to the Arrangement to recognise the Common Evaluation Methodology ALC_FLR supplement (reference [h] in this report) and the resultant inclusion of ALC_FLR.1 elements in certificates issued by a Qualified Certification Body.

CERTIFICATION STATEMENT

Marconi Selenia Communications MPS (Multi-Protocol Switch) can work as an ATM switch and/or ATM cross-connect. It provides a set of ATM and inter-working interfaces to provide integration of user and network services when connected to existing circuit-oriented military and civil communication networks. See Security Target [reference a] for more details.

The evaluated versions are models 115 and 145 (with software version 1.4 pack 2), which include the same types of hardware but differ in size (14 and 6 slots) respectively. These variants are collectively referred to as MPS throughout this report and are described in detail in Annex A.

MPS Version 1.4 pack 2 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL4 with ALC_FLR.1, for the specified Common Criteria Part 2 extended functionality when running on the specified platforms.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Head of the Certification Body, UK IT Security Evaluation and Certification Scheme
Date authorised	July 2004

(This page is intentionally blank)

TABLE OF CONTENTS

CERTIFICATION STATEMENT ..... **iii**

TABLE OF CONTENTS ..... **v**

ABBREVIATIONS ..... **vii**

REFERENCES ..... **ix**

I. EXECUTIVE SUMMARY ..... **x**

Introduction 1
Evaluated Product 1
TOE Scope 2
Protection Profile Conformance 2
Assurance 2
Strength of Function Claims 2
Security Policy 2
Security Claims 3
Evaluation Conduct 3
General Points 4

II. EVALUATION FINDINGS **5**

Introduction 5
Delivery 5
Installation and Guidance Documentation 5
Strength of Function 5
Vulnerability Analysis 5
Platform Issues 5
Flaw Remediation 6

III. EVALUATION OUTCOME **7**

Certification Result 7
Recommendations 7

ANNEX A: EVALUATED CONFIGURATION **1**

ANNEX B: PRODUCT SECURITY ARCHITECTURE **1**

ANNEX C: PRODUCT TESTING **1**

(This page is intentionally blank)

ABBREVIATIONS

ATM	Asynchronous Transfer Mode
CC	Common Criteria
CCIMB	Common Criteria Interpretation Management Board
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IP	Internet Protocol
ISDN	Integrated Services Digital Network
MLS	Multi-Level Security
MPS	Multi-Protocol Switch
MSM	Management & Switching Module
PIN	Personal Identification Number
RAM	Random Access Memory
SFR	Security Functional Requirement
SoF	Strength of Function
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UDP	User Datagram Protocol
UKSP	United Kingdom Scheme Publication

(This page is intentionally blank)

REFERENCES

a. MPS Security Target,
Marconi Selenia Communications,
6ti-sd000001-e, Issue 07, 26 July 2004.

b. Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model,
Common Criteria Interpretation Management Board,
CCIMB-99-031, Version 2.1, August 1999.

c. Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Requirements,
Common Criteria Interpretation Management Board,
CCIMB-99-032, Version 2.1, August 1999.

d. Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Requirements,
Common Criteria Interpretation 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. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.

g. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Evaluation Methodology Editorial Board,
CEM-99/045, Version 1.0, August 1999.

h. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation,
Common Criteria Interpretation Management Board,
CEM-2001/0015R, Version 1.1, February 2002.

i. Evaluation Technical Report for LFL/T161,
LogicaCMG CLEF,
LFL/T161/ETR, Issue 1.0, 10 June 2004.

j. Procedures for Installation, Generation and Start-up,
Marconi Selenia Communications, 6tr-sd000146-b, Issue 1, 21 November, 2003.

k. Delivery Procedure,
Marconi Selenia Communications, 6tr-sd000145-b, Issue 2, 9 April 2004.

l. Administrator Guidance,
Marconi Selenia Communications, str-sd000147b, Issue 3, 25 May 2004

m User Guidance,
Marconi Selenia Communications, 6tr-sd000148-b, Issue 1, 16 January 2004

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of MPS 115 & 145 Version 1.4 pack 2 to the Sponsor, Marconi Selenia Communications, 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 [a], which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The TOE was developed by Marconi Selenia Communications and is an ATM switch and/or ATM cross-connect. It provides a set of ATM and inter-working interfaces to provide integration of user and network services when connected to existing circuit-oriented military and civil communication networks. See reference [a] for more details.

4. The versions evaluated were MPS 115 & 145, software version 1.4 pack 2. The product is also described in this report as the Target of Evaluation (TOE) and as MPS.

5. The evaluated product consists of a chassis and plug-in cards comprising a Management and Switching Module (MSM), Power Supply and various interface modules. The interface modules can handle ATM, ISDN, IP, Eurocom and Stanag. Management users communicate with the TOE (i.e. the MSM) via a dedicated serial and ethernet port. The MSM controls the other cards using a separate internal ethernet bus.

6. Multiple TOEs can be connected together using an ATM trunk interface. Where the TOE connects to another type of switch outside the security boundary, this is defined as a gateway interface.

7. A key feature of the TOE is the ability to be able to take account of the security level of subscribers and of routes. Subscribers can either be permanently associated with a particular interface or can be allowed to use self-affiliation to be temporarily associated with different interfaces. A 6 digit PIN protects against unauthorised use of this featue. See the Security Target [a] for more details.

8. Multi-Level Security (MLS) is implemented so that callers are alerted by an audible warning tone when the call is downgraded with respect to the claimed security level. Alternatively, subscribers can be made non-downgradeable so that calls cannot be set-up unless the claimed security level of the call is obtained. MLS can also be dynamic during conference calls; changing as various subscribers join or leave the conference. However, note that gateway networks must always be configured to be non-downgradeable in this case.

9. Annex A provides details of the evaluated configuration of the TOE.

10. Annex B provides an overview of the TOE's security architecture.

11. Annex C describes the testing of the TOE.

TOE Scope

12. The scope covers the MPS hardware and the software running on the various cards. However, the management network terminal and/or network are out of scope and must be protected separately. Password protection of the management interface was included in the evaluation but it is assumed that the clear text passwords cannot be intercepted and that the UDP & TCP/IP protocols available on the management network (such as TFTP and telnet) will not be misused or attacked. Therefore physical access to these connections must be restricted to authorised management users.

13. It is assumed that the TOE will be kept physically secure and so, although it is claimed that passwords are encrypted when stored, the algorithm used and its implementation was not evaluated. Also the high strength of function assumes that an appropriate policy on management passwords is set by the relevant authority and adhered to.

Protection Profile Conformance

14. No conformance to a Protection Profile is claimed.

Assurance

15. The Security Target [a] specified the assurance requirements for the evaluation. The predefined Evaluation Assurance Level EAL4 was used, augmented by ALC_FLR.1 "Basic Flaw Remediation."

16. CC Part 3 [d] describes an increasing scale of assurance given by predefined assurance levels EAL1 to EAL7.

17. An overview of CC is given in CC Part 1 [b].

Strength of Function Claims

18. The Security Target claims high Strength of Function (SoF) for the subscriber affiliation and management user passwords. This claim was verified as they use a 6 digit PIN and an 8 character alphanumeric string respectively. However the password SoF relies on the implementation of an effective policy. As stated above, encryption of stored passwords was not evaluated.

Security Policy

19. The Security Target [a] states that the TOE must comply with a number of Organisational Security Policies and it is very important that these are implemented in order to ensure secure operation of the TOE. The policies relate to the following:

- Audit review
- Default configuration

- Flow of information
- Need-to-know
- Notification of failure

20. There are a number of assumptions in the Security Target, which users should read and be aware of. For example, a network management policy must be implemented to prevent multiple affiliations by a subscriber and gateway interfaces must only be connected to non-hostile and trusted 'IT entities'.

Security Claims

21. The Security Target [a] fully specifies the TOE's security objectives, the threats that the objectives counter, and the Security Function Requirements (SFRs) and TOE Security Functions (TSF) to elaborate the objectives.

22. All of the SFRs are taken from CC Part 2 [c]; use of this standard facilitates comparison with other evaluated products. Security functionality claims are made for IT security functions grouped under the following categories:

- Access Control
- Information Flow Control
- Failure Management
- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functions
- Resource Utilization
- Trusted Path and Channels

Evaluation Conduct

23. The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication (UKSP) 01 [e] and UKSP 02 [f]. 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 Mutual

Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

24. 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.

25. To ensure that the Security Target [a] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against that baseline.

26. The evaluation was performed in accordance with CC Part 3 [d], the Common Evaluation Methodology (CEM) [g], the CEM supplement on Flaw Remediation [h] and the appropriate interpretations.

27. The Certification Body monitored the evaluation, which was performed by the LogicaCMG Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the Evaluation Technical Report (ETR) [i] to the Certification Body in July 2004. The Certification Body then produced this 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.

29. The evaluated configuration is specified in Annex A. Prospective consumers are advised to check that it matches their identified requirements, and to give due consideration to the recommendations and caveats of this Certification Report.

30. 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.

31. 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 product and whether such patches have been evaluated and certified. However see the discussion below under the heading 'Flaw Remediation' regarding the application of patches generated as a result of the Developer's flaw remediation procedure.

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

II. EVALUATION FINDINGS

Introduction

33. 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.

34. The following sections note considerations of particular relevance to consumers.

Delivery

35. On receiving the TOE, the consumer is recommended to check that it is the evaluated version and to check that the security of the TOE has not been compromised during delivery.

36. Delivery guidance [k] should be read and a secure shipping method should be agreed with the supplier when ordering the TOE. The normal procedure is for software to be pre-installed on the TOE and protected with a 'strong' password.

Installation and Guidance Documentation

37. Secure installation, generation and startup of the TOE are described in the Installation and Startup guidance [j]. The Administrator Guidance [l] should also be read.

Strength of Function

38. The SoF claim for the TOE is identified above under the heading 'Strength of Function Claims'.

Vulnerability Analysis

39. The Developer's vulnerability analysis describes the disposition of all known vulnerabilities relating to the TOE identified by design analysis and an extensive search of public domain sources of vulnerability.

40. The Evaluators' vulnerability analysis considered public domain sources on a wide range of different recognised websites, but found no vulnerabilities beyond those considered in the developer's analysis. The Evaluators' analysis also considered the evaluation deliverables for potential vulnerabilities. The Evaluators confirmed that the Developer's vulnerability analysis was consistent with the Security Target and with the countermeasures detailed in the Installation and Startup guidance [j] and the Administration Guide [l]. This analysis resulted in the identification of penetration tests, which were then executed by the evaluators. No exploitable vulnerabilities were identified.

Platform Issues

41. The hardware tested is described in Annex A. Customers should be aware that if functional parts of the hardware are changed, the product will no longer be in its evaluated configuration.

Flaw Remediation

42. When problems are identified in the TOE, new versions of software will be developed and distributed to clients. Customers should agree the method of notification and supply of the updated software with the supplier. The updated software will not be the certified product but making use of such updates is recommended if they correct an exploitable vulnerability.

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 MPS 115 & 145 Version 1.4 pack 2 meets the Common Criteria Part 3 [d] augmented requirements of Evaluation Assurance Level EAL4 with ALC_FLR.1, for the specified Common Criteria Part 2 [c] functionality.

44. The TOE meets the minimum SoF claim of SoF-high and the metric given above under the heading 'Strength of Function Claims'.

Recommendations

45. Prospective consumers of the TOE should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a].

46. The TOE should be used in accordance with a number of environmental considerations, as specified in the Security Target [a].

47. The TOE should be delivered, installed, configured and used in accordance with the supporting guidance documentation [j- l] included in the evaluated configuration.

48. As stated in the security target, when a gateway is connected to a Secure Capable Entity and Conference Facility is required, the "Gateway Capability of being downgraded" should not be set.

49. Only the evaluated TOE configuration should be installed. That for which EAL4 assurance has been demonstrated is specified in Annex A, with further relevant information given above under the headings 'TOE Scope' and 'Evaluation Findings'.

50. Strictly, whilst ALC_FLR.1 gives confidence in the Developer's flaw remediation procedure, this will not maintain the full EAL4 assurance if the TOE configuration is changed by the application of patches. Nevertheless the application of patches generated under this procedure is recommended, if and where the patches fix exploitable vulnerabilities discovered since this report was issued.

51. It is therefore recommended that consumers contact the developer to receive information and updates related to TOE security flaws and that consumers report any suspected security flaws.

52. Further recommendations are provided above under the heading 'Evaluation Findings'.

(This page is intentionally blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The evaluated TOE software is uniquely identified as:

- MPS Software Version 1.4 pack 2

2. The following MPS115 hardware parts (and associated part-number) are included in the evaluated configuration:

- Wired Cover Assembly (144-4118/01.01)
- Blank Panel Netmod (341-4706/01.01)
- Blank Panel MSM (341-4707/01.01)
- 24/28V Power Supply Unit (141-6083/01.01)
- 110/220V Power Supply Unit (141-6082/01.01)
- MSM Unit (141-6081/11.01)
- 4 x 155 Mbps ATM Optical Unit (141-6084/01.01)
- 3 x N Mbps ATM FEC Unit (141-6175/01.01)
- 4 x 2 Mbps ISDN E1T1 Unit (141-6222/01.01)
- 4 x 2 Mbps EUROCOM Unit (141-6223/01.01)
- 16 x S0 ISDN Unit (141-6272/01.01)
- 8 x (10/100 Mbps) IP Unit (141-6087/01.01)

3. The following MPS145 hardware parts (and associated part-number) are included in the evaluated configuration:

- Wired Cover Assembly (143-4154/03.01)
- Blank Panel (341-4769/01.01)
- AC/DC Power Supply Unit (141-6191/01.01)
- MSM Unit (141-6187/11.01)
- 4 x 155 Mbps ATM Optical Unit (141-6186/01.01)
- 3 x N Mbps ATM FEC Unit (141-6209/01.01)
- 4 x 2 Mbps PRI ISDN Unit (141-6249/01.01)
- 4 x 2 Mbps EUROCOM Unit (141-6250/01.01)
- 16 x S0 ISDN Unit (141-6273/01.01)
- 8 x (10/100 Mbps) IP Unit (141-6188/01.01)

TOE Documentation

4. The guidance documents evaluated were:

- Installation Guidance and Startup Guide [j]
- Delivery Procedures [k]
- Administrator Guidance [l]
- User Guidance [m]

TOE Configuration

5. The TOE should be configured in accordance with the guidance documents identified above.

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the product's main 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 this report and in Annex A.

Architectural Features

2. The hardware consists of a number of plug-in modules, which include the power supply, Management and Switching Module (MSM), ATM interfaces and non-ATM interfaces (called Inter-Working Elements). All of the interface cards (including the Inter-Working Elements) have an ATM link to the MSM, which performs the switching. There is also an internal ethernet bus link to the MSM for control purposes. In addition, the MSM has external serial and ethernet ports for management users.

3. All of the modules contain an MPC860 processor, which is the platform for the control software, an ATM chipset, RAM and external interfaces etc.

4. The embedded software is based on a modular design and distributed across the various boards. The main control functions and the interface with the management user are located on the MSM board. The software architecture is designed to provide abstraction of lower level functions e.g. communication between modules and handling of interrupts.

Design Subsystems

5. Hardware subsystems are the individual boards as described above. Within the interface boards, the design is split into ATM base modules and Interface modules.

6. The software design documents describe how modules are provided to cover a number of functional areas:

- Identification & Authentication
- User Data Protection
- Auditing
- Intrusion Detection
- Protection & Recovery

7. The software modules themselves are distributed in families, which can be distributed, hierarchical or strictly hierarchical. They are further classified as system, base or application modules.

TSF Interface

8. The external interfaces of the TOE can be defined in terms of their physical specification (there are a total of 21 – see Security Target for more details):

- 7 x ATM
- 12 x Inter-Working Element (various protocols)
- 2 x Management (ethernet & serial)

9. Only authorised administrators should have physical access to the management ports, which are used to configure the TOE (e.g. using a telnet log-in).

10. The other interfaces are defined by the various protocols concerned. In addition (if permitted), ISDN subscribers can make use of the self-affiliation facility.

ANNEX C: PRODUCT TESTING

IT Product Testing

1. The Evaluators performed independent functional testing on the TOE to confirm that it operates as specified. They also repeated a sample of the Developer's tests to confirm the adequacy of the Developer's testing of all of all subsystems, TSFs and TSF interfaces.

2. The Evaluators then performed penetration testing which confirmed the SoF claimed in the Security Target [a] for the password authentication mechanism. The penetration testing also confirmed that all identified potential vulnerabilities in the TOE have been addressed, ie that the TOE in its intended environment has no exploitable vulnerabilities. All testing was performed using a testing facility at the developer's site.

3. During their testing, the Evaluators highlighted the fact that gateway networks should always be assigned as 'non-downgradeable' (as described in the Security Target) by demonstrating that dynamic Multi-Level Security in a conference call is not handled correctly across a gateway.

(This page is intentionally blank)