UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

CERTIFICATION REPORT No. P143

DFTS SWITCH

Nortel Passport Switch 6480 running software Version 5.0.16

Issue 1.0

April 2000

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 152
Cheltenham, Glos GL52 5UF
United Kingdom

RECOGNITION AGREEMENT OF
INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Agreement Group and as such:

- indicates that it is the issuer's claim that this certificate is a conformant certificate as defined in this Agreement; and

- therefore gives grounds for confidence, though it cannot in itself guarantee, that the certificate is a conformant certificate and that it will in practice be recognised by the other Members of the Agreement Group.

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:

CERTIFICATION STATEMENT

The DFTS Switch, which consists of Nortel Passport Switch 6480, is a telecommunications switch for use in a packet switching network.

The DFTS Switch, which consists of Nortel Passport Switch 6480 running software Version 5.0.16, has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the requirements of ITSEC Assurance Level E1.

Originator	**CESG** Certifier
Approval	**CESG** Technical Manager of the Certification Body
Authorisation	**CESG** Senior Executive UK IT Security Evaluation and Certification Scheme
Date authorised	7 April 2000

(This page is intentionally left blank)

TABLE OF CONTENTS

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

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

ABBREVIATIONS ..... **vii**

REFERENCES ..... **ix**

I. INTRODUCTION **1**

Intended Audience 1
Identification of Target of Evaluation 1
Evaluation 1
General Points 2

II. EVALUATION FINDINGS **3**

Introduction 3
Correctness - Construction 3
Correctness - Operation 3
Effectiveness - Construction 4
Effectiveness - Operation 5
Specific Functionality 5
Unresolved Issues 5

III. CONCLUSIONS **7**

Certification Result 7
Recommendations 7

ANNEX A: SUMMARY OF THE SECURITY TARGET **9**

ANNEX B: EVALUATED CONFIGURATION **11**

(This page is intentionally left blank)

ABBREVIATIONS

CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
CUG	Closed User Group
DFTS	Defence Fixed Telecommunications System
ETR	Evaluation Technical Report
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
NCC	Network Control Centre
NCS	Network Control System
NMS	Network Management System
NUA	Network User Address
PSS	Packet Switched Service
PVC	Permanent Virtual Circuit
SEF	Security Enforcing Function
SoM	Strength of Mechanisms
TOE	Target of Evaluation
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

a. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 3.0, 2 December 1996.

b. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.

c. Security Target for the Nortel Passport and DPN-100 Switches,
INCA,
DCN 1998101403, Issue 3.0, 28 January 2000.

d. Harmonised Information Technology Security Evaluation Criteria,
Commission of the European Communities,
CD-71-91-502-EN-C, Version 1.2, June 1991.

e. Information Technology Security Evaluation Manual,
Commission of the European Communities,
Version 1.0, 10 September 1993.

f. Manual of Computer Security Evaluation, Part I, Evaluation Procedures,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 3.0, October 1994.

g. Manual of Computer Security Evaluation, Part III, Evaluation Techniques and Tools,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 2.0, 30 July 1997.

h. ITSEC Joint Interpretation Library (ITSEC JIL),
Joint Interpretation Working Group,
Version 1.0, July 1996.

i. Task LFL/T107 Evaluation Technical Report 1,
Logica CLEF,
CLEF.24188.30.5.1, Issue 1, 23 April 1999.

j. Task LFL/T107 Evaluation Technical Report 2,
Logica CLEF,
CLEF.24188.30.T107.2, Issue 1, 14 January 2000,
as amended by AL 1, 21 January 2000,
as amended by AL 2, 6 April 2000.

k. Passport Hardware Installation Guide,
Publication 241-7001-125,
Version 5.0S1, November 1998.

l. Passport NMS Connectivity User Guide,
Publication 241-7001-135,
Version 5.0S1, November 1998.

m. Passport Operations and Maintenance Description,
Publication 241-7001-151,
Version 5.0S1, November 1998.

n. Passport Operations and Maintenance Guide,
Publication 241-7001-150,
Version 5.0S1, November 1998.

o. Passport StartUp Guide,
Publication 241-7001-130,
Version 5.0S1, November 1998.

p. System Security Policy for DFTS,
DFTS,
DCN 1999081403, Issue 3.0, 7 September 1999.

q. Certification Report No. S102, DFTS Packet Switched Service,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, April 2000.

I. INTRODUCTION

Intended Audience

1. This Certification Report states the outcome of the IT security evaluation of DFTS Switch, consisting of Nortel Passport Switch 6480 running software Version 5.0.16, to the Sponsor, DFTS, and is intended to assist potential users when judging the suitability of the product for their particular requirements.

Identification of Target of Evaluation

2. The version of the product evaluated was:

Nortel Passport Switch 6480 running software Version 5.0.16

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

3. The TOE is a switch, designed to form part of a packet switched data communications service. Its purpose is to support high capacity services on the network. It provides access protocol support for Frame Relay, Asynchronous Transfer Mode and LAN interconnect.

4. The TOE forms a component of the DFTS Packet Switched Service (PSS), which has been certified to ITSEC Assurance Level E1 [q].

Evaluation

5. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UKSP 01 and UKSP 02 [References a, b]. The Scheme has established a Certification Body which is jointly managed by the Communications-Electronics Security Group (CESG) and the Department of Trade and Industry on behalf of Her Majesty's Government.

6. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [c], which users are advised to read. (A copy of the Security Target may be obtained from the Sponsor.) The criteria against which the TOE was judged are described in the IT Security Evaluation Criteria (ITSEC) [d]. This describes how the degree of assurance is expressed in terms of the levels E0 to E6 where E0 represents no assurance. The methodology used is described in the IT Security Evaluation Manual (ITSEM) [e], UKSP 05 [f, g] and the ITSEC Joint Interpretation Library [h].

7. The Certification Body monitored the evaluation, which was carried out by the Logica Commercial Evaluation Facility (CLEF). The evaluation was completed in January 2000 when the CLEF submitted the second of 2 Evaluation Technical Reports (ETRs) [i, j] to the Certification Body which, in turn, produced this Certification Report.

8. The Target Assurance Level for the product, as required by the Security Target [c], was E1. The Strength of Mechanisms (SoM) claim was Basic in respect of the user-chosen password mechanism.

9. The minimum SoM for the search for vulnerabilities conducted by the Evaluators was strength Basic.

General Points

10. Prospective users of the TOE are reminded that the security functionality evaluated is that claimed in the Security Target [c]. This functionality may not necessarily meet all the threats that a user has identified in a particular operating environment. The assumed threats, intended method of use and environment are as stated in the Security Target. The TOE should only be used in its evaluated configuration (as indicated in Annex B) and in accordance with the recommendations and caveats contained in this report. It is the responsibility of purchasers to ensure that DFTS Switch meets their requirements.

11. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher assurance levels) 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. Users (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. Users are reminded of the security dangers inherent in downloading 'hot-fixes' where these are available, and that the UK Certification Body provides no assurance whatsoever for patches obtained in this manner. More up to date information on known security vulnerabilities within individual certified products and systems can be found on the IT Security Evaluation and Certification Scheme web site www.itsec.gov.uk.

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

II. EVALUATION FINDINGS

Introduction

13. The evaluation of Nortel Passport Switch 6480 followed the generic Evaluation Work Programme described in the ITSEM [e] with work packages structured around the evaluator actions described in the ITSEC [d]. The results of this work were reported in the ETRs [i, j] and under the ITSEC headings. This Certification Report summarises the assurance results in relation to the security functionality claimed in the Security Target [c].

Correctness - Construction

14. This aspect of the evaluation examined both the development process (ie the Security Target, the Architectural Design, the Implementation) and the environment in which it took place. The results were as follows:

a. The final version of the Security Target [c] stated the Security Enforcing Functions (SEFs) provided by the TOE, and contained a product rationale identifying its method of use and intended environment; it also stated how the product's functionality was appropriate for that method of use and was adequate to counter the assumed threats.

b. The Architectural Design properly stated the general structure of the TOE, together with any external interfaces and supporting hardware or firmware; it also clearly detailed how the SEFs of the TOE are provided.

c. The correctness of the implementation was satisfactory, ie all security enforcing functions offered in the Security Target were identifiable in the test documentation and the associated tests were repeatable.

d. Witnessing a repeat of all the Developer’s functional tests produced no differences in the test results.

e. The configuration control list stated how the TOE is uniquely identified.

15. The Evaluators concluded that the TOE met the requirements for ITSEC E1 in respect of its Security Target, Architectural Design, Implementation and Development Environment.

Correctness - Operation

16. The Evaluators checked and confirmed that:

a. the operational documentation [k-o] adequately stated the SEFs relevant to system managers (there are no users in the conventional sense) and how to operate the TOE in a secure manner;

b. the delivery and configuration documentation stated the delivery arrangements from the development environment to the customer and the required system generation aspects;

c. the startup and operation documentation adequately stated the procedures for secure startup and operation and, where relevant, for the deactivation or modification of SEFs; and

d. the information supplied stated how these procedures maintain the security of the TOE.

17. The Evaluators concluded that the Operational Documentation and the Operational Environment satisfied the requirements for ITSEC E1.

Effectiveness - Construction

18. This aspect of the evaluation dealt with:

a. the suitability of the TOE's SEFs to counter the threats identified in the Security Target [c];

b. the ability of the SEFs and mechanisms to bind together in a way that is mutually supportive and provides an integrated and effective whole;

c. the ability of the TOE's security mechanisms to withstand direct attack; and

d. the question of whether known security vulnerabilities in the construction of the TOE could, in practice, compromise its security.

19. The Evaluators were satisfied that:

a. the Suitability Analysis confirmed that all the threats listed in the Security Target [c] were adequately countered by one or more of the stated SEFs and mechanisms;

b. the Binding Analysis demonstrated that it was not possible for any SEF or mechanism to conflict with or contradict the intent of any other SEF or mechanism;

c. there were no known exploitable construction vulnerabilities;

d. the independent vulnerability analysis and penetration testing did not reveal any exploitable vulnerabilities in the TOE that were not satisfactorily corrected or neutralised;

e. the SoM Analysis listed all the security enforcing mechanisms identified as critical within the TOE, and the strength rating of the user chosen password mechanism was Basic as claimed.

20. The Evaluators concluded that the TOE is adjudged to have met the requirements for ITSEC E1 in respect of Suitability, Binding, SoM and Construction Vulnerability.

Effectiveness - Operation

21. This work involved:

    a. checking that the TOE can be used in a secure manner and assessing whether known vulnerabilities in its operation could, in practice, compromise its security; and

    b. checking the List of Known Vulnerabilities in the operation of the TOE, as supplied by the Sponsor, and assessing the impact of these vulnerabilities and the measures proposed to counter their effects.

22. The evaluation confirmed that:

    a. the TOE could not be configured or used in a manner which was insecure but which a manager would reasonably believe to be secure;

    b. the countermeasures proposed by the Sponsor in the List of Known Vulnerabilities in Operational Use were entirely satisfactory; and

    c. the independent vulnerability analysis and penetration testing did not reveal any exploitable vulnerabilities in the operation of the TOE.

23. The Evaluators concluded that the TOE meets the requirements for ITSEC E1 in respect of Ease of Use and Operational Vulnerability.

Specific Functionality

24. The Evaluators concluded that all the functionality claimed in the Security Target [c] had been met.

Unresolved Issues

25. During penetration testing with the PSS, the Evaluators observed that when logging on as a 'System' User with an incorrect password, using the Nortel Network Management Workstation (NMS) Version 10.9, the NMS interface gave the impression that access to the switch had been granted. However, the Evaluators satisfied themselves that commands to the Passport Switch were rejected and that data could neither be viewed nor amended. The Evaluators concluded, therefore, that security functionality within the PSS (and therefore within the switch) is not affected and no SEFs in either the Switch or the PSS are undermined and that the assurance of the TOE is not affected. The Evaluators recommend that the NMS interface should be updated to report when a System User's password is incorrect.

(This page is intentionally left blank)

III. CONCLUSIONS

Certification Result

26. After due consideration of the ETRs [i, j] produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that DFTS Switch, consisting of Nortel Passport Switch 6480 running software Version 5.0.16, meets the requirements of ITSEC Assurance Level E1.

Recommendations

27. The product should only be used in accordance with the intended environment and method of use stated in the Security Target [c]. Particular care should be taken that the product is configured and used in accordance with the operational documentation [k-o].

28. Potential users of the product should understand the specific scope of the certification by reading this report in conjunction with the Security Target [c]. Only the relevant evaluated product configuration as defined in Annex B should be installed. In particular, potential users of the product should note that the product has only been tested within the environment of the DFTS Packet Switched Service and using configurations which are relevant to that application.

29. Potential users of the product are recommended to maintain an up to date record of the manufacturer's default password. The manufacturer's default password should, however, only be used during initial installation and for recovery from complete reset of the product when, for instance, configuration data has been lost.

(This page is intentionally left blank)

ANNEX A: SUMMARY OF THE SECURITY TARGET

Introduction

1. The Security Target is given in [c]. The Product Rationale is summarised below.

Product Rationale

Intended Method of Use

2. The Nortel Passport Switch 6480 has been selected by INCA as one of several switches to be used in the DFTS PSS and is utilised to provide an interface between user access lines and the PSS network, in particular to provide high capacity services.

Assumed Threats

3. The threats to DFTS are listed in the overall System Security Policy [p].

Summary of Security Features

4. The PSS Switches are required to provide SEFs as follows:

Access Control

- PS-AC1: The switch shall verify that the NUA of an incoming packet belongs to the CUG of the subscriber before passing the data to the subscriber.
- PS-AC2: The switch shall keep data in one CUG separate from data in all the other CUGs.
- PS-AC3: The switch shall verify that the protocol of the incoming packet is the same as the protocol of the Subscriber port before passing the data to the subscriber.
- PS-AC4: The switch shall keep data in one PVC separate from all other data.
- PS-AC5: The switches shall keep data in one direct connection separate from all other data.
- PS-AC6: The switches shall limit a User's access to that functionality required for their role.

Authentication

- PS-AUTH1: The switch shall require users to be identified and authenticated.

Security Accounting

- PS-ACC1: It shall be possible to record all configuration changes to a switch.
- PS-ACC2: It shall be possible to record all connections to PSS Switches together with details of all calls established. This information shall be sent automatically to the NMS.
- PS-ACC3: It shall be possible to record the exercise of any function by the NCC Manager/Local Site Security Officer to selectively prevent (turn-off) the system accounting or alarm for any given event, except the event which produces an accounting record of changes in the Accounting and Audit functions.
- PS-ACC4: It shall be possible to record switch log-on and log-off
- PS-ACC5: It shall be possible to record switch administration activities including changes to User account profiles

Audit, Object Re-use, Accuracy of Data, Data Exchange

- No SEFs are required for the PSS Switches.

Reliability of service

- PS-RS1: The switch shall only allow access to configuration information (including any NCS) from the management CUG.
- PS-RS2: The switch shall restrict access to call-record information to authorised users within the management CUG.

Target Assurance Level

5. The Target Assurance Level for the product, as defined in the Security Target [c], was E1 as defined in ITSEC [d].

ANNEX B: EVALUATED CONFIGURATION

Hardware

1. The Passport 6480 is built from 3 Assembly units:

- Cable Management assembly
- Cooling Unit
- Shelf Assembly - houses up to 16 processor cards (Control Processors (CP) and Function Processors (FP)) and the power converters, providing distribution of secondary power and communications between FPs through the backplane.

2. The TOE can support one or two CPs. When a second CP is fitted, it operates in a passive stand-by mode, providing redundancy. The CP consists of a processor module, an interface module and a SCSI disk drive. The processor module connects the CP to the switch backplane, providing an interface with the bus. The interface module supports CP shelf management functions. The SCSI disk drive stores the Passport software, access control and authentication data, configuration data and audit and call-accounting data pending its upload to the NMS.

3. Up to 15 FPs can be fitted (14 with a second CP), each FP provides either trunk or local access interface ports. The FPs switch data from external sources (either trunk connections or local access lines) through the bus and out of the switch through other FPs. All variants of FP run the same switch software. The FPs may be mixed to meet the specific trunk and local access connectivity required.

4. All Passport 6480 switches on the DFTS PSS run the same version of software (see paragraph 6 below), and all have the same physical configuration, except for the mix of FPs.

Firmware

5. There is no firmware relevant to security in the TOE.

Software

6. The software component of the TOE is Nortel Passport Switch 6480 running software Version 5.0.16.

Tested Configuration

7. The Evaluators conducted their penetration testing on the Operational DFTS PSS at the DFTS Network Control Centre and using configurations which are relevant to that application.

(This page is intentionally left blank)