UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P191

NOKIA IPSO 3.5 and 3.5.1

Versions IPSO-3.5-FCS14-01.11.2003-012500-1041
and IPSO-3.5.1-FCS4-01.27.2003-222758-963

running on specified platforms

Issue 1.0

July 2003

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

All product or company names are used for identification purposes only and may be trademarks of their respective owners.

CERTIFICATION STATEMENT

Nokia IPSO 3.5 Version IPSO-3.5-FCS14-01.11.2003-012500-1041 and Nokia IPSO 3.5.1 Version IPSO-3.5.1-FCS4-01.27.2003-222758-963 are versions of a configurable UNIX-based operating system that are embedded in Nokia's IP Network Application Platform 'appliances'. Nokia IPSO Versions 3.5 and 3.5.1 are stripped of various services that are not required for the operation of those appliances, hence are not intended as a general-purpose operating systems and are not marketed independently of their use in those appliances.

Nokia IPSO 3.5 Version IPSO-3.5-FCS14-01.11.2003-012500-1041 and Nokia IPSO 3.5.1 Version IPSO-3.5.1-FCS4-01.27.2003-222758-963 have been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and have met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 conformant functionality when running on the platforms specified in Annex A.

The MD5 hash codes for software downloaded from the Developer's website are:

`e15bb4f2d3735002e41f9a95032f93be` for IPSO-3.5-FCS14-01.11.2003-012500-1041, and
`8295dcb2270ef5cf0f710db433ce1776` for IPSO-3.5.1-FCS4-01.27.2003-222758-963.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Head of the Certification Body UK IT Security Evaluation and Certification Scheme
Date authorised	7 July 2003

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

BIOS	Basic Input/Output System
CC	Common Criteria
CEM	Common Evaluation Methodology
CLEF	Commercial Evaluation Facility
DES	Data Encryption Standard
DNS	Domain Name Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ITSEC	Information Technology Security Evaluation Criteria
LAN	Local Area Network
MD5	Message Digest algorithm number 5
NFS	Network File System
RAM	Random Access Memory
RC4	A publicly available cypher system
RSA	Rivest, Shamir and Adleman
SEF	Security Enforcing Function
SFR	Security Functional Requirement
SoF	Strength of Functions
SSL	Secure Sockets Layer
TOE	Target of Evaluation
TSF	TOE Security Functions
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

a. Nokia IPSO 3.5 and 3.5.1 CC EAL4 Evaluation, CC Security Target,
LogicaCMG,
116788/C2/5, Issue 2.0, 13 March 2003.

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

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

d. Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-99-032, 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 Criteria Evaluation Methodology Editorial Board,
Version 1.0, CEM-099/045, August 1999.

h. Certification Report Number for Nokia IPSO 3.5 and 3.5.1,
UK Security Evaluation and Certification Schemes Certification Body,
P187, Issue 1.0, 16 June 2003.

i. EAL4 Delta Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 14 Addendum, Issue 2c, 21 March 2000.

j. LFA/T176 Nokia IPSO 3.5 and 3.5.1 Evaluation: Evaluation Technical Report,
LogicaCMG,
116788/T53/1, Issue 1.0, April 2003.

k. Nokia Voyager Reference 3.5,
Nokia Internet Communications,
N450583001.

l. Getting Started Guide and Release Notes, Nokia IPSO 3.5 FCS 14,
Nokia Internet Communications,
N450906001, Revision A, January 2003.

m. Getting Started Guide and Release Notes, Nokia IPSO 3.5.1 FCS 4,
Nokia Internet Communications,
N450934001, Revision A, February 2003.

n. Installation, Nokia IP100 series,
Nokia Internet Communications,
N450445001, Revision A, October 2000.

o. Installation, Nokia IP300 series,
Nokia Internet Communications,
N450312003a, March 2001.

p. Installation, Nokia IP400 series,
Nokia Internet Communications,
45-0220-003b, January 2000.

q. Installation, Nokia IP500 series,
Nokia Internet Communications,
N450452002a, June 2001.

r. Installation, Nokia IP600 series,
Nokia Internet Communications,
N450346003a, March 2001.

s. Installation, Nokia IP700 series,
Nokia Internet Communications,
N450436002a, July 2001.

t. Operation Instructions for Common Criteria EAL4 and ITSEC E3 Compliance, Nokia IPSO 3.5,
Nokia Internet Communications,
N450703002, Revision A, March 2003.

u. Multi-Platform Rationale, Nokia IPSO 3.5 and 3.5.1,
Nokia Internet Communications,
N450951001 Revision D, February 2003.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Nokia IPSO 3.5 Version IPSO-3.5-FCS14-01.11.2003-012500-1041 and Nokia IPSO 3.5.1 Version IPSO-3.5.1-FCS4-01.27.2003-222758-963 to the Sponsor, Nokia Internet 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 [Reference a] which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The versions of the product evaluated were:

Nokia IPSO 3.5 Version IPSO-3.5-FCS14-01.11.2003-012500-1041 and

Nokia IPSO 3.5.1 Version IPSO-3.5.1-FCS4-01.27.2003-222758-963

These products are also described in this report as the Target of Evaluation (TOE), and referred to as 'IPSO Versions 3.5 and 3.5.1'. The Developer was Nokia Internet Communications.

4. The only difference between the two versions is that IPSO Version 3.5.1 has additional drivers to support the hardware models on which it runs. Nokia IP350 and Nokia IP380 run only under Version 3.5.1; other evaluated platforms run only under IPSO Version 3.5.

5. The TOE is a configurable UNIX-based operating system, stripped of unneeded services, security hardened, and embedded in Nokia's IP Network Application Platform appliances. An appliance is delivered to a customer (typically a network administrator) with Nokia IPSO 3.5 or IPSO 3.5.1 and one or more security applications, pre-installed by Nokia on the appliance hard drive.

6. Services not present in the TOE that are commonly found in general purpose UNIX implementations include: sendmail; Berkeley "r" commands (e.g. 'rsh', 'rlogin', 'rexec'); exportable file systems (e.g. NFS); remote user information daemons (e.g. 'finger', 'who', 'talk'); DNS server (e.g. BIND); news server; printing server; X Window System; compilers or development environments on the system. Those services are not required for the operation of the appliance and they have, historically, represented potential security risks.

7. The features of the TOE are intended to provide a secure platform on which to run one or more security software applications (e.g. a firewall), that are selected and pre-installed by Nokia. No other applications can be loaded onto, or run on, the appliance. The appliance is typically put into continuous service running the application; the application is pre-configured to start automatically and would be stopped manually by the administrator only to perform maintenance.

8. The Security Enforcing Functions (SEFs) of the TOE provide secure administrative management of the appliance. Only administrators can access the appliance management system. There are no users of the appliance that are not administrators. Administrators are divided into 2 roles: *admin* (with view and modify privileges) and *monitor* (with view privilege only). The role-based access control system prevents administrators from accessing resources except those they are required to manage. Administrators are accountable for their actions through identification and authentication procedures (i.e. user name and password). The TOE also provides resource isolation and auditing of security-relevant events.

9. Although the TOE is derived from UNIX, the administrators access resources through the appliance's Voyager web server. During normal operation, the administrators are not provided with the normal UNIX command line, user accounts, user groups and access to the file system. Only the *admin* administrators are permitted to modify security-related objects and they are held accountable for all actions that modify such objects. Modify operations are logged as accounting data and the TOE provides the administrators with the means of auditing such data. The *monitor* administrators are limited to viewing objects, including security-related objects.

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

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

TOE Scope

12. See Annex A for details of the evaluated configuration, Annex B for the Product Security Architecture and Annex C for platform issues relating to product testing.

13. Access to the TOE is assumed to be via the Voyager web browser. Use of the command-line interface from the console serial port is not covered by the evaluation. It is assumed that the TOE is configured so that the command line interface is disabled from all interfaces and the console serial port is disabled.

14. The assumed threats (described in the Security Target [a]) are as follows:

- **T1** An attacker (possibly, but not necessarily, an authorised user of the TOE) may impersonate an authorised user of the TOE.
- **T2** An authorised administrator of the TOE may gain unauthorised access to information or resources.
- **T3** An undetected violation of the security policy may be caused as a result of an attacker (possibly, but not necessarily, an authorised user of the TOE) attempting to perform actions that the individual is not authorised to do.
- **T4** An undetected violation of the security policy may be caused as a result of an authorised user of the TOE, intentionally or otherwise (e.g. by Trojan Horse attack), performing actions that the user is authorised to do.
- **T5** An attacker may compromise the confidentiality of passwords and management data, leading to unauthorised disclosure or modification.

15. For details of the environmental assumptions (classed as user-related, media-related, network-related and audit-related) which form the context of how these threats are met, see the Security Target [a].

Protection Profile Conformance

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

Assurance

17. The Security Target [a] specified the assurance requirements for the evaluation. Predefined evaluation assurance level EAL4 was used. Common Criteria (CC) Part 3 [b] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [c].

Strength of Function Claims

18. The minimum Strength of Function (SoF) was SoF-Medium. This was claimed for the password-checking algorithm.

19. The cryptographic mechanisms for the TOE (i.e. DES, Triple DES and RC4 encryption algorithms, Diffie-Hellman and RSA public key exchange, and the MD5 hash algorithm) are publicly known and, as such, it is the policy of the national authority for cryptographic mechanisms, CESG, not to comment on their appropriateness or strength.

Security Policy

20. The TOE security policy is an Informal Security Policy Model concerned with Discretionary Access Control and is detailed in the Security Target [a].

Security Claims

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

22. Functionality claimed in the Security Target [a] included claims for:

- identification and authentication,
- role-based access control,
- accountability,
- audit, and
- data exchange.

Evaluation Conduct

23. 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, 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. 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 [b] and the Common Evaluation Methodology (CEM) [g].

25. The TOE Security Functions (TSF) and security environment, together with much of the supporting evaluation deliverables, remained unchanged from those of IPSO Versions 3.5 and 3.5.1, which had previously been certified by the IT Security Evaluation and Certification Scheme to the ITSEC E3 assurance level [h]. For the evaluation of IPSO Versions 3.5 and 3.5.1 to EAL4, the Evaluators used the guidance in EAL4 Delta Evaluation [i]. They addressed every CEM [g] EAL4 work unit but made some use of the previous evaluation results where these were valid for both the previous ITSEC E3 evaluation and the CEM requirements.

26. The Certification Body monitored the evaluation which was carried out by the CMG Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the Evaluation Technical Report (ETR) [j] to the Certification Body in April 2003. The Certification Body then produced this Certification Report.

General Points

27. 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.

28. 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.

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

II. EVALUATION FINDINGS

Introduction

30. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [j] under the CC Part 3 [b] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with the subsequent assurance maintenance and re-evaluation of the TOE.

Delivery

31. Software is pre-installed on appliances by Nokia at the factory. As customers purchase Nokia appliances via several routes (e.g. direct, via distribution, via Value Added Resellers), there is a time lag between installation of the software and delivery of the appliance to the customer. A customer is sent a user name and password. These are used to access Nokia's support website, via a Secure Sockets Layer (SSL) session. This enables the customer to download the evaluated version of the TOE and install its image on the purchased appliance via Voyager. The customer can verify the authenticity of that image, by calculating its MD5 hash on the appliance and then comparing the result with the MD5 hash identified in this report.

32. MD5 has codes for the evaluated products are:

`e15bb4f2d3735002e41f9a95032f93be` for IPSO-3.5-FCS14-01.11.2003-012500-1041, and
`8295dcb2270ef5cf0f710db433ce1776` for IPSO-3.5.1-FCS4-01.27.2003-222758-963.

33. 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

34. General guidance on installation can be found in the Nokia Voyager Reference, the IPSO Getting Started and Release Notes and the Installation Notes for the Nokia IP Hardware series [k-s].

35. In addition, for configuration of the TOE in a secure state, users should see 'Operation Instructions for ITSEC E3 Compliance [t].

Strength of Function

36. 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 password mechanism was the only probabilistic or permutational mechanism in the TOE, and that its algorithm met the minimum strength claim. The SoF claim of SoF-Medium was therefore upheld.

Vulnerability Analysis

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

38. The Evaluators identified the following operational vulnerabilities:

- passwords not managed properly;
- person given the wrong privileges;
- accidental deletion of *admin* users;
- accounting log overflows;
- unauthorised software changes;
- attempted security breaches not noted or acted upon; and
- SSL not configured correctly.

39. Adequate countermeasures were provided for each of these vulnerabilities.

40. The Evaluators devised and conducted penetration tests, based on the earlier ITSEC E3 evaluation of IPSO Versions 3.5 and 3.5.1 but updated and augmented, between 14 March and 24 March 2003. They found no exploitable vulnerabilities.

41. The use of automated test tools did reveal the following vulnerabilities, which were not considered to be exploitable.

a. The version of *mod_ssl* was vulnerable to buffer overflow, potentially allowing an attacker to open a shell on the host machine. The Evaluators considered that exploitation of this vulnerability would require greater resources than the claimed SoF-Medium.

b. The TOE responded to netmask requests, which could provide information about the network subnet structure.

c. The TOE responded to ICMP timestamp requests, which might enable attacks on time-based pseudo-random number generators.

d. The version of the web-server running could be determined.

III. EVALUATION OUTCOME

Certification Result

42. After due consideration of the ETR [j], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Nokia IPSO 3.5 Version IPSO-3.5-FCS14-01.11.2003-012500-1041 and Nokia IPSO 3.5.1 Version IPSO-3.5.1-FCS4-01.27.2003-222758-963 running on the specified platforms meet the Common Criteria Part 3 conformant requirements of EAL4 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on the platforms specified in Annex A.

43. The MD5 hash codes for software downloaded from the Developer's website are:

`e15bb4f2d3735002e41f9a95032f93be` for IPSO-3.5-FCS14-01.11.2003-012500-1041, and
`8295dcb2270ef5cf0f710db433ce1776` for IPSO-3.5.1-FCS4-01.27.2003-222758-963.

44. The minimum Strength of Function claimed for the password-checking algorithm was SoF-medium.

45. The Certification Body has also determined that the TOE meets the minimum SoF claim of SoF-Medium given above under "Strength of Function Claims".

Recommendations

46. Prospective consumers of IPSO Versions 3.5 and 3.5.1 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.

47. 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'.

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

49. 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 Nokia IPSO configurable UNIX-based operating system, embedded in Nokia IP Network Application Platform appliances as listed in Annex C under 'Platform Issues'.

2. The TOE is not intended as a general-purpose operating system and it is not marketed independently of its use within Nokia's appliances. Its purpose is to provide a secure platform on which to run security software applications (e.g. a firewall), that Nokia has pre-installed on the appliance; no other applications can be installed or run on the appliance.

3. The appliance is delivered to the customer (typically a network administrator) with the TOE and the security applications pre-loaded on the appliance hard drive.

4. The installation procedure involves connecting a terminal or terminal emulator to the 'console' serial port, to set an Ethernet port IP address and a password. Then the terminal can be disconnected, the appliance can be connected to an Ethernet LAN, and a web browser (such as Netscape Navigator or Microsoft Internet Explorer) running on a PC on the network can be used to complete the configuration through the appliance's Voyager web server.

5. Following the initial entry of IP address and password parameters through the console port, the console port may be disabled so that no further access is permitted from that port.

TOE Documentation

6. The supporting guidance documents evaluated were [k-s]. In addition, for details of the evaluated configuration see Operation Instructions for ITSEC E3 Compliance, Nokia IPSO 3.5 [t].

TOE Configuration

7. The TOE maintains two roles for its administrative users - *admin* (able to create, modify and delete data) and *monitor* (with read-only access).

8. The platforms under test were networked together for the purposes of testing and the IP330 and IP380 were configured as a Monitored Circuit pair.

Environmental Configuration

9. The Security Target [a] identified and explained security environmental assumptions which were categorized as user-related, media-related, network-related and audit-related.

(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. Nokia IPSO is not a general-purpose operating system and is used only on Nokia IP Network Application Platforms. A single binary constructed from the IPSO source files runs on all hardware platforms. These platforms are pre-configured with one or more security applications selected by Nokia for integration into the appliance.

Hardware and Firmware Dependencies

3. Some code relating to the CPU chip set interface, instrumentation, and features such as hot swap, executes conditionally depending on the specific platform. Otherwise IPSO functionality is identical for all platforms.

4. The firmware of the computer platform was Award BIOS 4.51PG Plug and Play extension (Version 1.0A). There were no firmware dependencies affecting the evaluation.

TSF Interfaces

5. Access to the TOE is assumed to via the Voyager web browser. Use of the command-line interface from the console serial port is not covered by the evaluation. It is assumed that the TOE is configured so that the command line interface is disabled from all interfaces and the console serial port is disabled.

(This page is intentionally left blank)

ANNEX C: PRODUCT TESTING

IT Product Testing

1. For details of the configuration tested see Annexes A and B.

2. Also, see Annex B under 'TSF Interfaces' for the TSF interfaces tested.

Platform Issues

3. The only differences between IPSO Version 3.5 and IPSO Version 3.5.1 are in the low-level hardware-specific drivers. Drivers specific to the IP350 and IP380 platforms have been added to Version 3.5.1. Nokia IP350 and Nokia IP380 run only under IPSO Version 3.5.1; other evaluated platforms run only under IPSO Version 3.5.

4. The evaluation and penetration testing of the TOE was conducted on the Nokia IP120, IP330 and IP440 hardware platforms for IPSO 3.5 and IP380 for IPSO 3.5.1. Hence the evaluation results apply to the TOE running on those platforms.

5. All tests were carried out on the IP330 platform (for IPSO 3.5) and the IP380 (for IPSO 3.5.1). A selection of the tests were repeated on the IP120 and IP440 platforms.

6. Additionally, the Sponsor provided a rationale [u] and test evidence, to the satisfaction of the evaluators, which justified extending the evaluation results to additional hardware platforms. The results of the evaluation therefore hold for the following platforms:

- Nokia IP110 (Version 3.5)
- Nokia IP120 (Version 3.5)
- Nokia IP330 (Version 3.5)
- Nokia IP440 (Version 3.5)
- Nokia IP530 (Version 3.5)
- Nokia IP650 (Version 3.5)
- Nokia IP710 (Version 3.5)
- Nokia IP740 (Version 3.5)
- Nokia IP350 (Version 3.5.1)
- Nokia IP380 (Version 3.5.1)

7. The hardware platforms differ in respect of their processor type (National GX1, AMD K6-2 or Intel Pentium III), processor speed (from 300 MHz to 1 GHz); RAM size (64 MB to 1 GB); hard disk size (from 5 to 20 Gigabytes); number of Ethernet ports (from 3 to 20), and types of Ethernet ports available.

(This page is intentionally left blank)