Copy No.

Doc Ref	**116788/C2/5**
Client	**Nokia**
Project	**IPSO 3.5 and 3.5.1 CC EAL4 Evaluation**
Title	**CC Security Target**
Date	**10 March 2003**

Review & Approval

Issue:	2.0	**LogicaCMG**
R&A Number:	116788/C1/11	**LFA CLEF**
Originator:		Kings Court
J I Goodson		91-93 High Street
		Camberley
Approval (PM):		Surrey GU15 3RN
R Worswick		Tel: (01276) 686678
		Fax: (01276) 685205
Approval (QAR):		
M J Orchard		

Distribution List

Copy No	Recipient
1	Nokia
2	LFA CLEF Evaluators
3	File

Contents

1 Introduction

1.1 ST Identification

1.1.1 Title: Security Target for Nokia IPSO 3.5 and IPSO 3.5.1.

1.1.2 Assurance Level: EAL4

1.1.3 This document is the Common Criteria [CC] compliant Security Target for Nokia's IPSO 3.5 and IPSO 3.5.1.

1.2 ST Overview

1.2.1 This Security Target specifies the security environment, objectives and features of Nokia's IPSO operating system versions 3.5 and 3.5.1 (referred to as the product) as submitted for evaluation to the [CC] evaluation assurance level EAL4.

1.2.2 IPSO is a configurable UNIX-based operating system stripped of unnecessary services and security hardened. It is intended to provide a secure platform to run one or more software applications selected by Nokia.

1.3 CC Conformance

1.3.1 The product is [CC] Part 2 and Part 3 conformant with a claimed assurance level of EAL4.

1.3.2 No conformance with a Protection Profile is claimed.

1.4 Document Structure

1.4.1 Section 2 provides the description of the TOE.

1.4.2 Section 3 provides the statement of the TOE security environment.

1.4.3 Section 4 provides the statement of the security objectives.

1.4.4 Section 5 provides the statement of the IT security requirements.

1.4.5 Section 6 provides the TOE summary specification

1.4.6 Section 7 provides the rationale

1.5 Conventions

In the SFRs in Chapter 5, the results of the assignment, selection and refinement operations have been retained in brackets – […].

1.6 Terminology

Single gender words such as 'he' or 'she' have been used for convenience and are intended to imply either gender.

1.7 Abbreviations

HMG	Her Majesty's Government
IP	Internet Protocol
ITSEC	IT Security Evaluation Criteria
RBAC	Role-based Access Control

SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
SSL	Secure Sockets Layer
TOE	Target of Evaluation
TSF	TOE Security Functions
UK	United Kingdom

1.8 References

[CC] Common Criteria for Information Technology Security Evaluation, CCIMB-99-031 to 3, Version 2.1, August 1999

[VREF] Voyager Reference Guide , Nokia, N450392005a

[E3_GUIDE] Operation Instructions for ITSEC E3 Compliance, Nokia, N450703001

[MD5] The MD5 Message-Digest Algorithm, R Rivest, RFC 1321, April 1992

[SSL] The SSL Protocol Version 3.0, Alan O Freier, Philip Karlton and Paul C Kocher, 18 November 1996

2 TOE Description

2.1 Summary of TOE

2.1.1 Nokia IPSO is a configurable UNIX-based operating system, stripped of unnecessary services, security hardened, and embedded in Nokia's IP Network Application Platform "appliances." Services not present in Nokia's implementation of UNIX that are commonly found in general purpose UNIX implementations include sendmail; Berkeley "r" commands, such as 'rsh', 'rlogin', 'rexec', etc.; exportable file systems, such as NFS; remote user information daemons such as 'finger', 'who', and 'talk'; DNS server such as BIND; news server; printing server; X Window System; compiler or development environment on the system. None of these services is required for operation of the security appliance; each service historically has represented potential security risks. Therefore they are not present in IPSO, Nokia's implementation of UNIX.

2.1.2 Nokia IPSO is not a general-purpose operating system, and is not marketed independently of its use within Nokia's appliances. It implements role-based access control (as required to distinguish between *admin* and *monitor* roles) for access to the appliance management system.

2.1.3 The features of Nokia IPSO are intended to provide secure platforms to run one or more security software applications selected by Nokia, on which a significant amount of trust can be placed. No other applications can be loaded onto or run on the appliance. The security functionality provides secure administrative management of the appliance.

2.1.4 A Nokia IP Network Applications Platform system (appliance) consists of a hardware platform running IPSO and one or more security applications selected by Nokia for integration into the network application appliance.

2.1.5 The Nokia appliance is delivered to the customer (typically a network administrator) with the IPSO operating system and one or more security applications pre-loaded on the appliance hard drive. 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. The terminal can then be disconnected, the appliance 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 then be used to complete the configuration through the appliance's Voyager web server. Note that 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.

2.1.6 There are no users of the appliance that are not administrators. Administrators are the only individuals capable of accessing the appliance management system. Administrators of the appliance are divided into two roles – *admin* with view/modify privileges, and *monitor* with view-only privileges. Objects that may be viewed or modified are specifically predetermined within IPSO. Administrators do not have access to the appliance file system or other objects not predetermined by IPSO. The role-based access control system prevents administrators from accessing resources other than those they are required to manage. Although IPSO is derived from UNIX, administrators access resources through the appliance's Voyager web server, and during normal operation are not provided with the normal UNIX command line, user accounts and user groups, or access to the file system (see ENV.U.8 in Chapter 3).

2.1.7 The appliance is typically placed into continuous service running a security application, such as a firewall software application. The application is pre-configured to start up automatically, and would be stopped manually by the administrator only to perform maintenance activities.

2.2 Hardware Platform

2.2.1 IPSO runs on a number of PC compatible hardware platforms. IPSO 3.5 executes on the Nokia IP Security Platforms, Models IP110/120, IP330, IP440, IP530, IP650 and IP740. IPSO 3.5.1 executes on the Nokia IP Security Platforms, Models IP350 and IP380.

2.2.2 The principle differences in the hardware are the different processors (Pentium or compatible) and the different network interfaces that are available.

2.2.3 A single binary constructed from IPSO's source files runs on all the hardware platforms. Certain code relating to the CPU chip set interface, instrumentation, and features such as hot swap, executes conditionally depending on the specific platform. Otherwise, all IPSO functionality is identical – the single binary runs on each platform, implementing IPSO's functionality using the same executable files.

2.3 Summary of Security Features

2.3.1 **Identification and Authentication** – Users must be identified and authenticated before they can have any other access to the TOE. Only *admin* users can modify passwords while no user can read passwords.

2.3.2 **Role-based Access Control –** *Admin* users can read and modify data while *monitor* users can only read data. There are no differences in the data that users can read.

2.3.3 **Accountability –** The following events are audited:

a) user identification and authentication

b) modify/delete/create access to data controlled by the Role-based Access Control (including user accounts)

c) events affecting auditing

d) start-up and shutdown of the TOE.

2.3.4 **Audit –** There are facilities to manage audit logs and to read them.

2.3.5 **Data Exchange –** There are facilities to protect data passed between a user's web browser and IPSO.

3 TOE Security Environment

3.1 Assumptions

3.1.1 Introduction

This section indicates the minimum physical and procedural measures required to maintain security of the IPSO operating system versions 3.5 and 3.5.1. It is not a complete list, as specific measures may be required for different configurations and sites.

3.1.2 User-related

3.1.2.1 **ENV.U.1** The product must not be configured in a way that none of the *admin* administrators can access IPSO.

3.1.2.2 **ENV.U.2** In order for the product to be able to enforce individual accountability, each individual user must have a unique user name.

3.1.2.3 **ENV.U.3** Users must not disclose their passwords to other individuals.

3.1.2.4 **ENV.U.4** Procedures shall be established to ensure that user passwords generated by an administrator during user account creation or modification are distributed in a secure manner, as appropriate for the clearance of the system.

3.1.2.5 **ENV.U.5** Procedures shall be established to ensure that an *admin* administrator changes passwords regularly.

3.1.2.6 **ENV.U.6** The product must be configured such that passwords have a minimum length of 8 characters and are not easy to guess.

3.1.2.7 **ENV.U.7** Only an *admin* administrator shall be allowed to introduce new software onto the system.

3.1.2.8 **ENV.U.8** During normal operation, access must be via the Voyager web browser interface of the TOE. Use of the command-line interface from the console serial port is for initial installation only, and its use beyond initial installation is not covered by this evaluation. The product must be configured such that the command line interface is disabled from all interfaces, and such that the console serial port is disabled.

3.1.2.9 **ENV.U.9** Configuration enabling command line access as a “maintenance mode” may be performed only after physically disconnecting user/subscriber networks.

3.1.2.10 **ENV.U.10** Users must include one administrator with view/modify authorization – *admin,* with user name “admin”. Additional *admin* administrators may be added, each with a unique user name up to 8 characters. In addition, one *monitor* administrator with view-only authorization must be included, with user name “monitor”. Additional *monitor* administrators may be added, each with a unique user name up to 8 characters, with UID not assigned to zero. The product is supplied to customers initially configured with only one *admin* administrator with the user name “admin” and one *monitor* administrator with the user name “monitor”.

3.1.3 Media-related

3.1.3.1 **ENV.M.1** The media on which authentication data is stored (internal hard disk drive of the TOE Platform) must not be physically removable by unauthorized users. Removable media must not be configured on the platform.

3.1.3.2 **ENV.M.2** The media on which audit data is stored (internal hard disk drive of the TOE Platform, or storage media on a remote computer) must not be physically removable by unauthorized users.

3.1.4 Network-related

3.1.4.1 **ENV.N.1** All bridges and routers will correctly pass data without modification, to assist in ensuring network availability.

3.1.4.2 **ENV.N.2** All network and peripheral cabling shall be approved for the transmittal of the most sensitive data held by the system. Such physical links must be adequately protected against threats to the confidentiality and integrity of the data transmitted.

3.1.4.3 **ENV.N.3** Procedures shall exist to ensure that the hardware, software, and firmware components that comprise the networked product are distributed, installed and configured in a secure manner.

3.1.4.4 **ENV.N.4** SNMP (Simple Network Management Protocol), Telnet, FTP, tftp, and SSH shall be disabled on the TOE during normal operation.

3.1.4.5 **ENV.N.5** Facilities and/or procedures shall exist where necessary for the secure handling (including generation and destruction) of SSL keys.

3.1.4.6 The following assumptions (**ENV.N.6** to **ENV.N.9** inclusive) apply in environments where specific threats to distributed systems need to be countered. Typically such threats are countered by cryptographic protection of network connections. In the TOE, these threats are countered through the use of a secured connection from the administrator to the TOE, implemented using the TOE's SSL functionality. This evaluation assumes the TOE is configured to require SSL to contribute to the required protection.

3.1.4.7 **ENV.N.6** Procedures and/or mechanisms shall exist to ensure that data transferred between the TOE platform and administrators is not made available or disclosed to unauthorized users or processes, where this is considered a threat.

3.1.4.8 **ENV.N.7** Procedures and/or mechanisms shall exist to ensure that the unauthorized modification, replay or destruction of data being transferred between the TOE platform and administrators is prevented and/or detected, where this is considered a threat.

3.1.4.9 **ENV.N.8** Procedures and/or mechanisms shall exist to ensure that the unauthorized modification or spoofing of the identity of the source TOE platform of data received, is prevented and/or detected, where this is considered a threat.

3.1.4.10 **ENV.N.9** Procedures and/or mechanisms shall exist to ensure that web browsers used by administrators are in accordance with the security policy including appropriate configuration of the workstation, and unauthorized users cannot gain access to cached credentials such as SSL keys.

3.1.5 Audit-related

3.1.5.1 **ENV.A.1** Procedures shall exist to ensure that the audit trail for the product is regularly analyzed and archived, to allow retrospective inspection. In particular, authentication failures shall be audited and regularly inspected to detect occurrences of possible automated attacks.

3.1.5.2 **ENV.A.2** The auditing system shall be configured such that the loss of audit data is minimized upon:

a) planned or unplanned shutdown; or

b) lack of available audit storage.

3.2 Threats

3.2.1 This section identifies the threats to the TOE.

3.2.2 **T1** An attacker (possibly, but not necessarily, an authorized user of the TOE) may impersonate an authorized user of the TOE.

3.2.3 **T2** An authorized administrator of the TOE may gain unauthorized access to information or resources.

3.2.4 **T3** An undetected violation of the security policy may be caused as a result of an attacker (possibly, but not necessarily, an authorized user of the TOE) attempting to perform actions that the individual is not authorized to do.

3.2.5 **T4** An undetected violation of the security policy may be caused as a result of an authorized user of the TOE, intentionally or otherwise (e.g. by Trojan Horse attack), performing actions that the user is authorized to do.

3.2.6 **T5** An attacker may compromise the confidentiality of passwords and management data, leading to unauthorized disclosure or modification.

3.3 Organisational Security Policies

There are no organisational security policies.

4 Security Objectives

4.1 Security Objectives for the TOE

4.1.1 **SO.1** Providing administrators of the TOE with the means of carrying out a restricted set of operations on objects – *admin* administrators view/modify operations, and *monitor* administrators view-only operations.

4.1.2 **SO.2** Providing administrators of the TOE with the means of holding individual users accountable for any actions they perform that are relevant to security.

4.1.3 *Note:* In the TOE, only *admin* administrators are permitted to modify security-related objects, and the *admin* administrators are held accountable for all actions that modify security-related objects. *Monitor* administrators are limited to viewing objects including security-related objects. Modify operations are logged as accounting data and the TOE provides administrators with the means of auditing that accounting data.

4.1.4 *Note:* The TOE is intended for use in a network environment that requires discretionary protection of information and/or resources, individual accountability through logon procedures, and resource isolation. These requirements are met by the TOE using the logon procedure and role-based access control for discretionary protection of information and resources and contribute to individual accountability along with accounting and audit provisions. The operating system kernel mechanism provides for resource isolation.

4.2 Security Objectives for the Environment

4.2.1 User-related

4.2.1.1 **EO.U.1** The product must not be configured in a way that none of the *admin* administrators can access IPSO.

4.2.1.2 **EO.U.2** In order for the product to be able to enforce individual accountability, each individual user must have a unique user name ID.

4.2.1.3 **EO.U.3** Users must not disclose their passwords to other individuals.

4.2.1.4 **EO.U.4** Procedures shall be established to ensure that user passwords generated by an administrator during user account creation or modification are distributed in a secure manner, as appropriate for the clearance of the system.

4.2.1.5 **EO.U.5** Procedures shall be established to ensure that an *admin* administrator changes passwords regularly.

4.2.1.6 **EO.U.6** The product must be configured such that passwords have a minimum length of 8 characters and are not easy to guess.

4.2.1.7 **EO.U.7** Only an *admin* administrator shall be allowed to introduce new software onto the system.

4.2.1.8 **EO.U.8** During normal operation, access must be via the Voyager web browser interface of the TOE. Use of the command-line interface from the console serial port is for initial installation only, and its use beyond initial installation is not covered by this evaluation. The product must be configured such that the command line interface is disabled from all interfaces, and such that the console serial port is disabled.

4.2.1.9 **EO.U.9** Configuration enabling command line access as a "maintenance mode" may be performed only after physically disconnecting user/subscriber networks.

4.2.1.10 **EO.U.10** Users must include one administrator with view/modify authorization – *admin*, with user name “admin”. Additional *admin* administrators may be added, each with unique user name up to 8 characters. In addition, one *monitor* administrator with view-only authorization must be included, with user name “monitor”. Additional *monitor* administrators may be added, each with unique user name up to 8 characters, with UID not assigned to zero. The product is supplied to customers initially configured with only one *admin* administrator with the user name “admin” and one *monitor* administrator with the user name “monitor”.

4.2.2 Media-related

4.2.2.1 **EO.M.1** The media on which authentication data is stored (internal hard disk drive of the TOE Platform) must not be physically removable by unauthorized users. Removable media must not be configured on the platform.

4.2.2.2 **EO.M.2** The media on which audit data is stored (internal hard disk drive of the TOE Platform, or storage media on a remote computer) must not be physically removable by unauthorized users.

4.2.3 Network-related

4.2.3.1 **EO.N.1** All bridges and routers will correctly pass data without modification, to assist in ensuring network availability.

4.2.3.2 **EO.N.2** All network and peripheral cabling shall be approved for the transmittal of the most sensitive data held by the system. Such physical links must be adequately protected against threats to the confidentiality and integrity of the data transmitted.

4.2.3.3 **EO.N.3** Procedures shall exist to ensure that the hardware, software, and firmware components that comprise the networked product are distributed, installed and configured in a secure manner.

4.2.3.4 **EO.N.4** SNMP (Simple Network Management Protocol), Telnet, FTP, tftp, and SSH shall be disabled on the TOE during normal operation.

4.2.3.5 **EO.N.5** Facilities and/or procedures shall exist where necessary for the secure handling (including generation and destruction) of SSL keys.

4.2.3.6 The following objectives (**EO.N.6** to **EO.N.9** inclusive) apply in environments where specific threats to distributed systems need to be countered. Typically such threats are countered by cryptographic protection of network connections. In the TOE, these threats are countered through the use of a secured connection from the administrator to the TOE, implemented using the TOE’s SSL functionality. This evaluation assumes the TOE is configured to require SSL to contribute to the required protection.

4.2.3.7 **EO.N.6** Procedures and/or mechanisms shall exist to ensure that data transferred between the TOE platform and administrators is not made available or disclosed to unauthorized users or processes, where this is considered a threat.

4.2.3.8 **EO.N.7** Procedures and/or mechanisms shall exist to ensure that the unauthorized modification, replay or destruction of data being transferred between the TOE platform and administrators is prevented and/or detected, where this is considered a threat.

4.2.3.9 **EO.N.8** Procedures and/or mechanisms shall exist to ensure that the unauthorized modification or spoofing of the identity of the source TOE platform of data received, is prevented and/or detected, where this is considered a threat.

4.2.3.10 **EO.N.9** Procedures and/or mechanisms shall exist to ensure that web browsers used by administrators are in accordance with the security policy including appropriate configuration of the workstation, and unauthorized users cannot gain access to cached credentials such as SSL keys.

4.2.4 Audit-related

4.2.4.1 **EO.A.1** Procedures shall exist to ensure that the audit trail for the product is regularly analyzed and archived, to allow retrospective inspection. In particular, authentication failures shall be audited and regularly inspected to detect occurrences of possible automated attacks.

4.2.4.2 **EO.A.2** The auditing system shall be configured such that the loss of audit data is minimized upon:

a) planned or unplanned shutdown; or

b) lack of available audit storage.

5 Security Requirements

5.1 TOE Security Functional Requirements

5.1.1 FAU_GEN.1 Audit data generation

5.1.1.1 **FAU_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:

a) start-up and shutdown of the audit functions;

b) [the events identified in Table 1].

5.1.1.2 **FAU_GEN.1.2** The TSF shall record within each audit record at least the following information:

a) date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) for each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [the information identified in the details column of Table 1].

Table 1 – Auditable Events

Event	**Details**
a) use of the Identification and Authentication mechanism	IP address of the network node from which the login attempt emanated
b) actions that attempt to exercise rights to modify, delete or add an object (or combination of objects) which is subject to role based access control	
c) creation or deletion of monitor accounts	name of user account
d) audit trail saturation[1]	notification issued to the administrator
e) start-up[2] and shutdown of the TOE	

5.1.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.3 FAU_SAR.1 Audit review

5.1.3.1 **FAU_SAR.1.1** The TSF shall provide [all authenticated users] with the capability to read [all audit information] from the audit records.

5.1.3.2 **FAU_SAR.1.2** The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

[1] No subject identity recorded because no user caused the event.

[2] No subject identity recorded because no user identity is available – the TOE is started up merely by switching it on.

5.1.4 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [the list of cryptographic operations specified in [Table 2] in accordance with a specified cryptographic algorithm [as specified in Table 2] and cryptographic key sizes [as specified in Table 2] that meet the following:[standards as specified in Table 2][3].

Table 2 – Cryptographic Operations

Cryptographic Operation	Cryptographic Algorithm	Key Size	Standard
a) Password hashing	MD5	n/a	[MD5]
b) Encryption of data between administrator browser and IPSO, and server authentication	SSL	128bit	[SSL] using OpenSSL available through www.openssl.org

5.1.5 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [Role Based Access Control (RBAC) SFP] on

a) [all users

b) objects as defined in [VREF]

c) operations as defined in [VREF] (view or modify/create/delete)].

5.1.6 FDP_ACF.1 Security attribute based access control

5.1.6.1 **FDP_ACF.1.1** The TSF shall enforce the [RBAC SFP] to objects based on [the role of the authenticated user (*admin* or *monitor*)].

5.1.6.2 **FDP_ACF.1.2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) [if the user is an *admin* user then view and create/modify/delete access is allowed

b) if the user is a *monitor* user then only view access is allowed].

5.1.6.3 **FDP_ACF.1.3** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

5.1.6.4 **FDP_ACF.1.4** The TSF shall explicitly deny access of subjects to objects based on the [none].

5.1.7 FIA_UAU.2 User authentication before any action

FIA_UID.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.8 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

[3] The required information has been provided in tabular form in the interests of clarity.

5.1.9 FMT_MSA.1 Management of security attributes

5.1.9.1 **FMT_MSA.1.1** The TSF shall enforce the [RBAC SFP] to restrict the ability to [perform the operations defined in Table 3 on] the security attributes [defined in Table 3] to [the roles defined in Table 3].

5.1.9.2 Application Note: The only security attribute that can be specified is the user role and that is specified indirectly by the *admin* user by specifying the uid. If the uid = 0 then the user role is *admin*. If the uid ≠ 0 then the user role is *monitor*.

Table 3 – Allowed Operations on Security Attributes

Operation	**Data**	**User Role**
a) create/modify/delete as defined in [VREF]	user account data including user role but excluding user password	*admin*
b) read	user account data including user role but excluding user password	*admin, monitor*

5.1.10 FMT_MTD.1 Management of TSF data

5.1.10.1 **FMT_MTD.1.1** The TSF shall restrict the ability to [perform the operations defined in Table 4 on] the [data listed in Table 4] to [users as defined in Table 4].

5.1.10.2 Application Note: All access to all TOE data is controlled by the RBAC SFP.

Table 4 – Allowed Operations on TSF Data

Operation	**Data**	**User Role**
a) create/modify/delete as defined in [VREF]	audit logs time/date backups	*admin*
b) read	audit logs time/date backups	*admin, monitor*
c) modify	user passwords	*admin*
d) read	user passwords	none

5.1.11 FMT_SMR.1 Security roles

5.1.11.1 **FMT_SMR.1.1** The TSF shall maintain the roles [*admin* and *monitor*].

5.1.11.2 **FMT_SMR.1.2** The TSF shall be able to associate users with roles.

5.1.12 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.2 Strength of Functions

The claimed minimum strength of function is SOF-Medium.

5.3 TOE Security Assurance Requirements

The TOE security assurance requirements are those of evaluation assurance level EAL4 with no augmentation or extension.

5.4 Security Requirements for the IT Environment

There are no security requirements for the IT environment.

6 TOE Summary Specification

6.1 Introduction

The majority of the TOE security functions are identical to the Security Enforcing Functions from the ITSEC E3 evaluation of the TOE.

6.2 TOE Security Functions

6.2.1 Identification and Authentication

6.2.1.1 **SEF.IA.1** The TOE shall require users to uniquely identify and authenticate themselves to it prior to all other interactions between the TOE and the user.

6.2.1.2 **SEF.IA.2** The TOE shall authenticate the claimed identity of the user before allowing any interaction between the TOE and the user other than identification and authentication.

6.2.1.3 **SEF.IA.3** The TOE shall control access to authentication data (passwords) as follows:

a) The TOE shall provide functions to allow *admin* administrators to modify authentication data

b) The TOE shall prevent *admin* administrators from observing authentication data, i.e. passwords

c) The TOE shall prevent *monitor* administrators from observing, modifying or deleting authentication data.

6.2.2 Role-Based Access Control

6.2.2.1 **SEF.RBAC.1** Only an *admin* administrator shall be able to create new *monitor* or *admin* accounts or delete existing *monitor* or *admin* accounts.

6.2.2.2 **SEF.RBAC.2** The TOE shall ensure that only *admin* administrators can create subjects to act on their behalf. The number of such subjects is finite.

6.2.2.3 **SEF.RBAC.3** The TOE shall constrain administrators to a limited set of operations.

6.2.2.4 **SEF.RBAC.4** The TOE shall implement a RBAC mechanism that allows *admin* administrators to view and modify a predetermined set of objects, and *monitor* administrators to only view the predetermined set of objects.

6.2.3 Accountability

6.2.3.1 **SEF.ACT.1** The TOE shall be able to log use of the identification and authentication mechanism together with the following data: Date; time; user identity; IP address of the network node from which the request emanated; success or failure of the attempt.

6.2.3.2 **SEF.ACT.2** The TOE shall be able to log actions that attempt to exercise access rights to modify, delete, or add an object (or a combination of objects) which is subject to role-based access control (including attempts to delete an object) together with the following data: Date; time; user identity; name of the object; type of access attempt; success or failure of the attempt.

6.2.3.3 **SEF.ACT.3** The TOE shall be able to log the creation, or deletion, of *monitor* administrator accounts together with the following data: Date; time; identity of the user implementing the change; name of the user account involved; type of action (i.e. creation, deletion).

6.2.3.4 **SEF.ACT.4** The TOE shall be able to log security relevant events affecting the operation of the auditing functions (shutdown of the auditing functions, audit trail saturation), together with the following data: Date; time; type of event; and in the case of audit trail saturation, notification issued to the administrator.

6.2.3.5 **SEF.ACT.5** The TOE shall be able to log the startup and shutdown of the TOE together with the following data: Date; time; user identity (shut down only); type of action.

6.2.3.6 **SEF.ACT.6** The TOE shall provide a reliable source of date and time information for (amongst other things) the time stamping of audit records.

6.2.4 Audit

6.2.4.1 **SEF.AUD.1** The TOE shall provide functions that support the creation and maintenance of the accountability files.

6.2.4.2 **SEF.AUD.2** The TOE shall include facilities to review the accountability files.

6.2.5 Data Exchange

SEF.DE.1 The TOE shall provide functions that support security of data during transmission over communications channels between the TOE and administrators (communications security). Security protections provided by the TOE include TOE authentication, confidentiality of authentication (password) and configuration information, and data integrity.

6.3 Required Security Mechanisms

The following mechanisms are required:

a) **M1** The TOE shall apply the MD5 public encryption function, a one-way function, to authentication data (passwords) before storing them in the TOE. The application of this one-way function makes it impractical for an attacker to learn passwords by locating authentication data stored in the TOE. No SOF claim is required because this is an encryption algorithm.

b) **M2** The TOE shall employ the SSL (Secure Sockets Layer) protocol using DES, 3DES, and RC4 public encryption algorithms, and Diffie-Hellman and RSA public key exchange. Encryption ensures privacy of authentication data and TOE configuration data. Key exchange ensures the authenticity of the TOE to the administrator. No SOF claim is required because this is an encryption algorithm.

6.4 Assurance Measures

Table 5 summarises the way in which each of the EAL4 assurance requirements as defined in Part 3 of [CC] is satisfied by assurance measures. The identified ITSEC documentation may need some small modifications to meet the [CC] requirements.

Table 5 – Satisfaction of EAL4 Assurance Requirements by Assurance Measures

EAL4 Assurance Components	Assurance Measures
ACM_AUT.1 Partial CM automation	IPSO ITSEC CM documentation
ACM_CAP.4 Generation support and acceptance procedures	IPSO ITSEC CM documentation
ACM_SCP.2 Problem tracking CM coverage	IPSO ITSEC CM documentation

Table 5 – Satisfaction of EAL4 Assurance Requirements by Assurance Measures

EAL4 Assurance Components	Assurance Measures
ADO_DEL.2 Detection of modification	IPSO ITSEC Delivery documentation
ADO_IGS.1 Installation, generation, and start-up procedures	IPSO Installation Guide
ADV_FSP.2 Fully defined external interfaces	IPSO Functional Specification
ADV_HLD.2 Security enforcing high-level design	IPSO Architectural Design
ADV_IMP.1 Subset of the implementation of the TSF	IPSO source code
ADV_LLD.1 Descriptive low-level design	IPSO Detailed Design
ADV_RCR.1 Informal correspondence demonstration	embedded in the different levels of TOE specification
ADV_SPM.1 Informal TOE security policy model	IPSO CC Security Target (this document)
AGD_ADM.1 Administrator guidance	Voyager User Guide IPSO ITSEC E3 Guidance
AGD_USR.1 User guidance	n/a – all users are administrators
ALC_DVS.1 Identification of security measures	IPSO ITSEC development environment documentation
ALC_LCD.1 Developer defined life-cycle model	IPSO ITSEC development environment documentation
ALC_TAT.1 Well-defined development tools	IPSO ITSEC development environment documentation
ATE_COV.2 Analysis of coverage	ITSEC Test Documentation
ATE_DPT.1 Testing: high-level design	ITSEC Test Documentation
ATE_FUN.1 Functional testing	ITSEC Test Documentation
ATE_IND.2 Independent testing – sample	Evaluator testing
AVA_MSU.2 Validation of analysis	IPSO Misuse Analysis (based on IPSO ITSEC Ease of Use analysis
AVA_SOF.1 Strength of TOE security function evaluation	IPSO SOF Analysis (based on IPSO ITSEC Strength of Mechanisms analysis
AVA_VLA.2 Independent vulnerability analysis	IPSO Vulnerability Analysis (based on IPSO ITSEC Vulnerability Analyses

7 Rationale

7.1 Introduction

This section demonstrates that the TOE provides an effective set of IT security countermeasures within the security environment and that the TOE Summary Specification addresses the requirements.

7.2 Security Objectives Rationale

7.2.1 Table 6 shows the mapping of threats to security objectives. It can be seen that each threat is addressed by at least one security objective and each security objective is used to address at least one threat.

Table 6 – Mapping of Threats to Security Objectives

Threat	SO.1	SO.2	Environmental Assumptions
T1	✓	✓	ENV.U.2 to 6
T2	✓		
T3		✓	ENVA.1/2
T4		✓	ENVA.1/2, ENV.U.7
T5	✓	✓	ENVA.1/2, ENV.U.2 to 6

7.2.2 Each of the Environmental Objectives EO.X.n is identical to the corresponding Environmental Assumption ENV.X.n. Hence there is complete coverage of the assumptions by the objectives and vice versa.

7.2.3 The following paragraphs address each of the threats. All the arguments assume ENV.U.8, i.e. that the Voyager web browser interface is used since the use of the console serial port is not covered by the evaluation.

7.2.4 **T1** The TOE limits the facilities available to a user according to her role determined according to the user's providing a valid user name and password at logon. Only *admin* users can change user account data and all such operations are audited and the audit records can be read by all authenticated users. The environmental assumptions ensure that each user is given a unique user name and that passwords are managed in a secure manner.

7.2.5 **T2** The TOE limits access to a restricted set of data via the browser interface. This cannot be varied. *Admin* users have read and modify access to the data while *monitor* users have only read access. Again, the operations cannot be varied.

7.2.6 **T3** No access to the TOE is allowed until the user has been authenticated and then the TOE audits all actions that are security relevant. This auditing cannot be varied. ENV.A.1/2 ensure that audit is not lost and that the audit logs are regularly inspected.

7.2.7 **T4** The TOE audits all actions that are security relevant. This auditing cannot be varied. ENV.U.7 ensures that only an *admin* user can change the TOE software.

7.2.8 **T5** Only authenticated users can access management data and no user can read passwords. *Admin* users can set passwords for other users but ENV.U.2 to 6 ensure that passwords are managed in a secure manner. All security related actions are audited and ENV.A.1/2 ensure that audit data is not lost and that the audit records are inspected regularly so that attempted attacks will be noticed.

7.3 Security Requirements Rationale

7.3.1 Security Functional Requirements Cover Objectives

7.3.1.1 Table 7 shows the coverage of the security objectives by the SFRs.

Table 7 – Mapping of Security Objectives to SFRs

Security Objective	Security Functional Requirements										
	FAU_GEN.1/2	**FAU_SAR.1**	**FCS_COP.1**	**FDP_ACC.1**	**FDP_ACF.1**	**FIA_UAU.2**	**FIA_UID.2**	**FMT_MSA.1**	**FMT_MTD.1**	**FMT_SMR.1**	**FMT_STM.1**
SO.1			✓	✓	✓	✓	✓	✓	✓	✓	
SO.2	✓	✓				✓	✓				✓

7.3.1.2 SO.1 is addressed by the following SFRs:

a) FMT_SMR.1 ensures there are only two roles, viz. *admin* and *monitor*

b) FIA_UAU.2 and FIA_UID.2 ensure that users are identified and authenticated before they can perform any other action with the TOE

c) FCS_COP.1 ensures that passwords are protected when stored in IPSO or in transit between the user's web browser and IPSO.

d) FDP_ACC.1, FDP_ACF.1, FMT_MSA.1 and FMT_MTD.1 ensure that the available actions are controlled according to the user's role.

7.3.1.3 SO.2 is addressed by the following SFRs:

a) FIA_UAU.2 and FIA_UID.2 ensure that users are identified and authenticated before they can perform any other action with the TOE

b) FAU_GEN1/2 and FAU_SAR.1 ensure that relevant events are audited and there are facilities to examine the audit records

c) FMT_STM.1 ensures that the audit record timestamp is reliable so that it can be related to real time.

7.3.2 Satisfaction of Dependencies

7.3.2.1 Table 8 shows the dependencies on each of the SFRs. All the dependencies are present with the following exceptions:

7.3.2.2 FIA_UID.1 – FIA_UID.2 is hierarchical to FIA_UID.1 and is therefore a suitable substitute.

7.3.2.3 FCS_CKM.1 and FCS_CKM.4 – These components are not required for the password hashing algorithm MD5 since it does not have keys. For SSL, these components have been replaced by the environment assumption ENV.N.5 since SSL operates over the network connection between the user’s web browser and the TOE.

7.3.2.4 FMT_MSA.2 and FMT_MSA.3 – These components are not required because, as stated under FMT_MSA.1 above, the (*admin*) user cannot specify any security attributes directly. She must specify the user’s uid which then determines the user’s role. The uid must be entered explicitly as a positive integer so that there is no default security attribute.

Table 8 – SFR Dependencies

Security Functional Requirements		Dependencies	
Element	**Component Name**	**Component**	**Present ?**
FAU_GEN.1	Audit data generation	FPT_STM.1	3
FAU_GEN.2	User identity association	FAU_GEN.1 FIA_UID.1	3 7
FAU_SAR.1	Audit review	FAU_GEN.1	3
FCS_COP.1	Cryptographic operation	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	7 7 7
FDP_ACC.1	Subset access control	FDP_ACF.1	3
FDP_ACF.1	Security attribute based access control	FDP_ACC.1 FMT_MSA.3	3 7
FIA_UAU.2	User authentication before any action	FIA_UID.2	3
FIA_UID.2	User identification before any action	–	–
FMT_MSA.1	Management of security attributes	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1	3 3
FMT_MTD.1	Management of TSF data	FMT_SMR.1	3
FMT_SMR.1	Security roles	FIA_UID.1	7
FPT_STM.1	Reliable time stamps	–	–

7.3.3 Internal Consistency of SFRs

7.3.3.1 The SFRs were selected from the pre-defined functional components in Part 2 of [CC]. Assignment, selection and refinement operations were performed using consistent computer security and TOE-specific terminology.

7.3.3.2 Multiple instantiation of identical components has been used using a tabular format for clarity.

7.3.3.3 The interactions are those identified as dependencies in Part 2 of [CC]. As shown in Section 7.3.2 above, all the dependencies are present or their absence is justified. Hence the SFR are mutually supportive.

7.3.4 Compliance with PPs

No compliance with any PP is claimed.

7.3.5 Justification of Assurance Level

The TOE is intended for use in a wide range of environments including UK HMG systems. ITSEC E3 or [CC] EAL4 are common assurance levels requirements for the UK HMG systems and so EAL4 is an appropriate assurance level for IPSO.

7.3.6 Justification for Strength of Function Claim

The SOF claim for the TOE is SOF-medium. This has been chosen as being commensurate with the EAL4 assurance level and the SOF claims for mechanisms in this Security Target.

7.4 TOE Summary Specification Rationale

7.4.1 Table 9 shows how the SFRs are satisfied by the TOE Security Functions. This section shows that all the SFRs are met and that each SF is required.

7.4.2 The SFs are mutually supportive in the same way that the SFRs they map to are mutually supportive.

Table 9 – SFR to Security Function Mapping

Security Functional Requirements		
Element	**Component Name**	**Security Functions (SEF.AAA.n)**
FAU_GEN.1	Audit data generation	ACT.1, ACT.2, ACT.3, ACT.4, ACT.5
FAU_GEN.2	User identity association	• ACT.1, ACT.2, ACT.3, ACT.4, ACT.5
FAU_SAR.1	Audit review	AUD.2, RBAC.4
FCS_COP.1	Cryptographic operation	IA.3, DE.1 and mechanisms M1 and M2
FDP_ACC.1	Subset access control	RBAC.1, RBAC.2, RBAC.3, RBAC.4
FDP_ACF.1	Security attribute based access control	RBAC.1, RBAC.2, RBAC.3, RBAC.4
FIA_UAU.2	User authentication before any action	IA.1, IA.2
FIA_UID.2	User identification before any action	IA.1
FMT_MSA.1	Management of security attributes	RBAC.1
FMT_MTD.1	Management of TSF data	IA.3, RBAC.2, RBAC.3, RBAC.4

Table 9 – SFR to Security Function Mapping

Security Functional Requirements		
Element	**Component Name**	**Security Functions (SEF.AAA.n)**
FMT_SMR.1	Security roles	RBAC.1
FPT_STM.1	Reliable time stamps	ACT.6

7.4.3 FAU_GEN.1 is addressed by the following SFs:

a) SEF.ACT.1, SEF.ACT.2, SEF.ACT.3, SEF.ACT.4 and SEF.ACT.5 ensure that the TOE is able to generate the audit records for the events required by FAU_GEN.1.1 containing the information required by FAU_GEN.1.2 and Table 1.

7.4.4 FAU_GEN.2 is addressed by the following SFs:

a) SEF.ACT.1, SEF.ACT.2, SEF.ACT.3, SEF.ACT.4 and SEF.ACT.5 ensure that the TOE records in the audit record the identity of the user causing an event, except for:

i) audit trail saturation because it is not attributable to any one user

ii) TOE start-up because there is no user identity available – the TOE is just switched on.

7.4.5 FAU_SAR.1 is addressed by the following SFs:

a) SEF.AUD.2 provides facilities to read and interpret audit records

b) SEF.RBAC.4 ensures that only authenticated users can read the audit records.

7.4.6 FCS_COP.1 is addressed by the following SFs:

a) SEF.IA.3 requires that passwords cannot be read

b) SEF.DE.1 requires functions to protect the security of data in transit between the TOE and administrators

c) Mechanisms M1 and M2 provide the required cryptographic operations.

7.4.7 FDP_ACC.1 is addressed by the following SFs:

a) SEF.RBAC.1, SEF.RBAC.2, SEF.RBAC.3 and SEF.RBAC.4 provide the required RBAC SFP.

7.4.8 FDP_ACF.1 is addressed by the following SFs:

a) SEF.RBAC.1, SEF.RBAC.2, SEF.RBAC.3 and SEF.RBAC.4 restrict the operations allowed and the type of access permitted by subjects (user roles) to objects in accordance with the requirements

7.4.9 FIA_UAU.2 is addressed by the following SFs:

a) SEF.IA.1 and SEF.IA.2 require authentication of a user prior to any other interaction with the TOE.

7.4.10 FIA_UID.2 is addressed by the following SFs:

a) SEF.IA.1 requires identification of a user prior to any other interaction with the TOE.

7.4.11 FMT_MSA.1 is addressed by the following SFs:

a) SEF.RBAC.1 restricts the type of access permitted by user roles to user account data in accordance with the requirements.

7.4.12 FMT_MTD.1 is addressed by the following SFs:

a) SEF.IA.3 restricts the type of access permitted by user roles to passwords in accordance with the requirements

b) SEF.RBAC.2, SEF.RBAC.3 and SEF.RBAC.4 restrict the type of access permitted by user roles to other TSF data in accordance with the requirements.

7.4.13 FMT_SMR.1 is addressed by the following SFs:

a) SEF.RBAC.1 maintains user roles (Note that user roles are explicitly associated with users – see 5.1.9.2)

7.4.14 FPT_STM.1 is addressed by the following SFs:

a) SEF.ACT.6 provides for reliable time stamps on audit records.

7.4.15 The compliance of assurance measures with assurance requirements is demonstrated in Section 6.4.