# THALES COMMUNICATIONS S. A.

# SECURITY TARGET

# EXTERNAL COMMUNICATIONS MANAGEMENT SYSTEM

Prepared by:

IBM Global Services CLEF
IBM UK Ltd
Meudon House
Meudon Avenue
Farnborough
Hampshire GU14 7NB

Date: 15 January 2004
Issue: 1.2
Reference: Thales/ECMS/ST/1.2

## REVISION HISTORY

| Issue | Description | Date |
|---|---|---|
| 0.A | First Draft | 25 March 2003 |
| 0.B | Second Draft following further discussions with Thales | 16 April 2003 |
| 0.C | Third Draft incorporating changes proposed by DOMUS. | 17 July 2003 |
| 0.D | Forth Draft. Minor modification to Table 7-8 and insertion of TOE version number. Introduction of two IT environment security objectives to address the CB concerns regarding a reference monitor. | 28 July 2003 |
| 0.E | Fifth Draft. Insertion of the SFR for the IT environment session, providing relevant rationales, plus editorial changes to address the CB concerns regarding a reference monitor. | 06 August 2003 |
| 1.0 | First Release | 05 January 2004 |
| 1.1 | Update to first release following discussion with DOMUS | 12 January 2004 |
| 1.2 | Inclusion of password assumption | 15 January 2004 |

## TABLE OF CONTENTS

**Page**

## ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| API | Application Programme Interface |
| CC | Common Criteria |
| CCC | Communications Control Centre |
| CCCS | Canadian Common Criteria Scheme |
| CCMS | Communications Control and Monitoring System |
| CEM | Common Methodology for Information Technology Security |
| CIC | Combat Information Centre |
| COTS | Commercial-Off-The-Shelf |
| EAL | Evaluation Assurance Level |
| ECMS | External Communications Management System |
| ICMS | Internal Communications Management System |
| LAN | Local Area Network |
| NATO | North Atlantic Treaty Organisation |
| PC | Personal Computer |
| PP | Protection Profile |
| SARs | Security Assurance Requirements |
| SFP | Security Functional Policy |
| SFRs | Security Functional Requirements |
| ST | Security Target |
| TBD | To Be Determined |
| TCP/IP | Transfer Control Protocol/Internet Protocol |
| Thales | Thales Communications S. A. |
| TOE | Target of Evaluation |
| TSC | TSF Scope of Control |
| TSF | TOE Security Function |
| TSP | TOE Security Policy |

# 1 INTRODUCTION

## 1.1 Identification

| | |
|---|---|
| Title: | Security Target<br>External Communications Management System<br>Version 4.1 |
| Release Date: | 12 January 2004 |
| Level of Assurance: | EAL3 |
| Keywords: | Communications Management System |

## 1.2 Conformance Claim

The Thales External Communications Management System Version 4.1 is the Target of Evaluation (TOE) for this Common Criteria (CC) Version 2.1 Part 2 and CC Version 2.1 Part 3 conformant evaluation.

The TOE conforms to the requirements of the Common Criteria for Information Technology Security Evaluation, August 1999, Version 2.1, CCIMB-99-032 ([CC]), for an Evaluation Assurance Level (EAL) 3 evaluation.

## 1.3 Strength of Functions

The claimed strength of function is medium.

## 1.4 Structure

The structure of this document follows that defined in [CC] Part 1, Annex C:

- Section 2 is the TOE description;
- Section 3 provides a statement of the TOE security environment;
- Section 4 provides the statement of IT security objectives;
- Section 5 provides a statement of IT security requirements;
- Section 6 provides the TOE summary specification, which includes the detailed specification of the IT functions; and

- Section 7 provides the rationale for the security objectives, security requirements and TOE summary specification.

# 2 TOE DESCRIPTION

## 2.1 Introduction

The External Communications Management System (ECMS) Version 4.1, together with the ICMS (Internal Communications Management System), form the CCMS (Communications Control and Monitoring System) which manages all internal and external communications equipment on the Belgian Navy’s WIELINGEN frigate.

The ECMS is a software application that runs on CCMS workstations. It manages the following aspects of the communications system:

- Radio equipment such as HF transmitters, HF receivers, V/UHF transceivers and modems

- Radio services supported by this equipment offering voice and data communication services.

The TOE for this evaluation is the ECMS Host application.

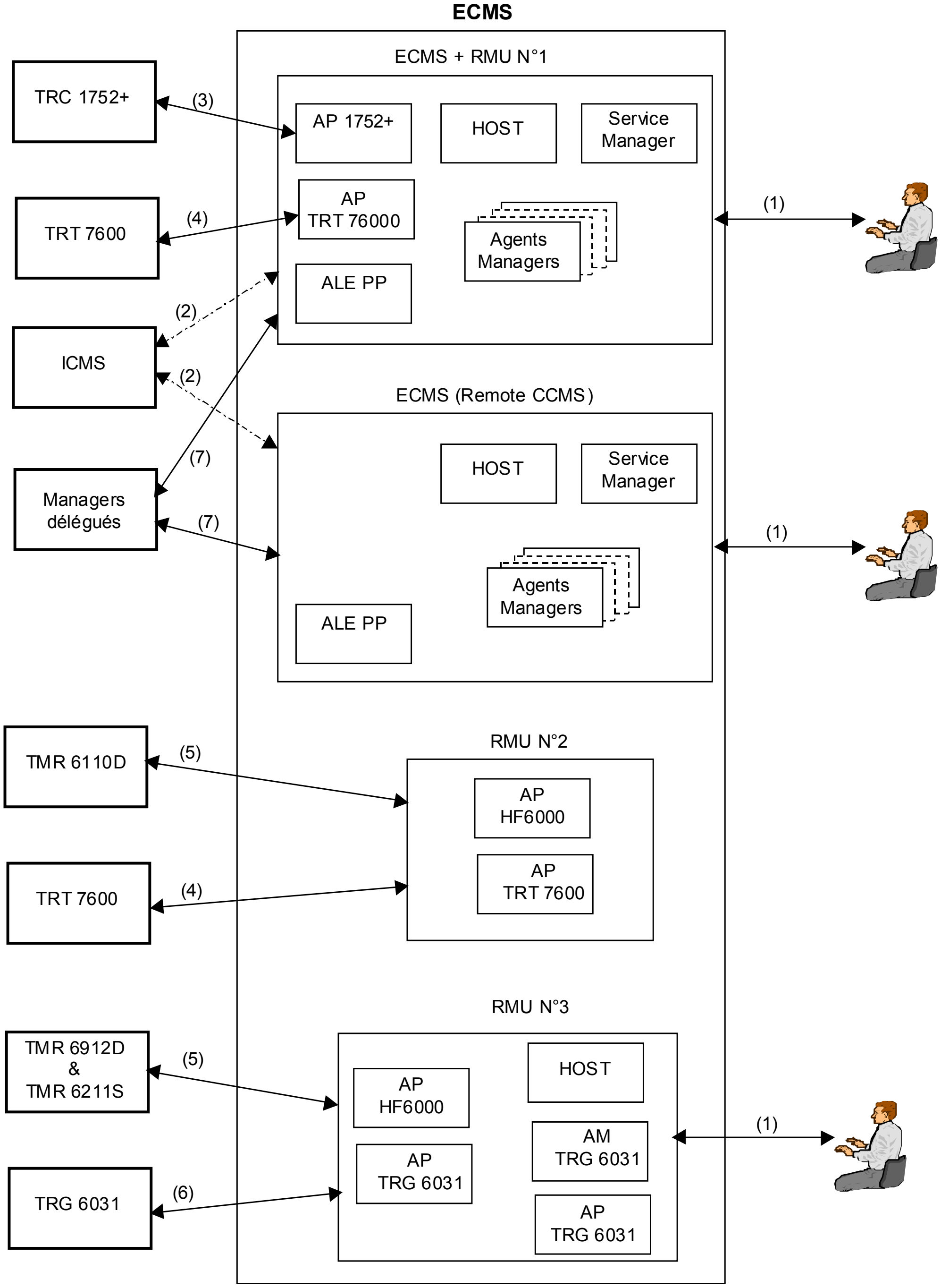

**Figure 2-1: ECMS Host system**

## 2.2 Detailed Description

### 2.2.1 Software Components

The TOE software is written in C++.

### 2.2.2 External Interfaces

The TOE has the following external interfaces:

- Operator interface – the interface between the operator and the ECMS. This is a graphical user interface which is installed on the CCMS NT workstations;
- Radio equipment interface – this interface allows the ECMS to exchange information with the radio equipment;
- CCMS workstation interface – the interface to the CCMS workstation's NT operating system;
- ICMS interface – the interface to the ICMS application. This allows the ECMS to exchange monitoring information and commands controlling the radio services, emission control and voice terminal/radio chain allocation.

### 2.2.3 Architecture

The ECMS Host application runs on a PC under the Windows NT operating system. Users interface with the ECMS Host application via the PC's keyboard and display. The figure below shows the components that make up the ECMS core and the communications devices that are controlled by the ECMS. The red box denotes the ECMS Core or Logical Component. The Host application, or physical component controls all the other applications (e.g. Service Manager, Agent Managers) and is denoted by the black outer box.

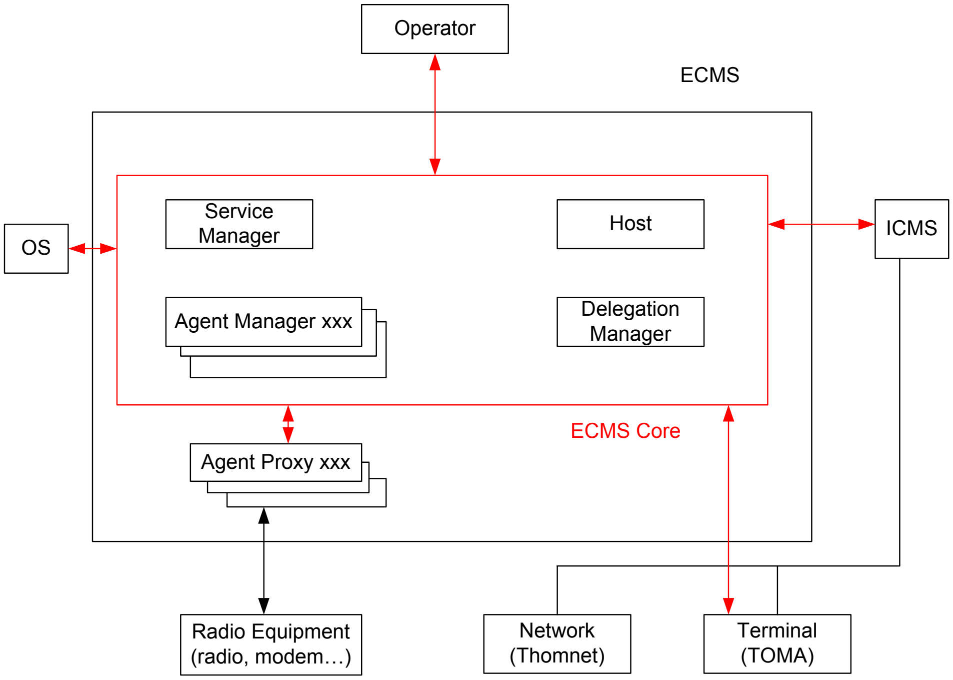

Figure 2-2: ECMS Core system

### 2.2.4 Scope of the Evaluation

The scope of this evaluation covers the Host application and its interface with the user. The operating system on which the Host application resides is not included within this evaluation.

#### 2.2.4.1 The Physical Scope

The upper inner box in Figure 2-1 marked as "ECMS + RMU No 1" describes the physical scope. It covers the Agent Manager, Service Manager and Host modules, the AP1752+, AP TRT7600 and ALE PP modules as well as interfaces to other systems.

#### 2.2.4.2 Logical Scope

The inner red line in Figure 2-2 defines the logical scope as the ECMS Core. It encompasses the Service Manager, Host, Agent Manager and Delegation Manager.

### 2.2.5 Security Functions and Services

The TOE security services under evaluation are:

- Enforcement of the ECMS Discretionary Access Control Policy;

- Audit of specified security events.

### 2.2.6 Security Roles

The following roles are supported by the TOE:

- Operator (O),
- Chief Operator (C) and
- Administrator (A).

The specific responsibilities and privileges of the Chief Operator and Operators are a subset of those of the Administrator.

User rights are assigned according to the role. Users are able to “handover” their role to another user or to “swap” their role for another role.

### 2.2.7 Hardware and Software Requirements

The ECMS Host application runs on a Microsoft Windows NT4 PC.

The following software is used by the ECMS Host application:

- JDK 1.2.2
- EXCEED
- Microsoft Windows NT4 Service Pack 6a
- INGRES II

# 3 TOE SECURITY ENVIRONMENT

The statement of TOE security environment describes the security aspects of the environment in which the TOE is intended to be used, and the manner in which it is expected to be employed.

The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the method of use for the product; defines the threats that the product is designed to counter; and defines the organisational security policies with which the product is designed to comply.

## 3.1 Assumptions

The list of assumptions regarding the security aspects of the environment in which the TOE is intended to be used is presented in the following subsections.

### 3.1.1 Physical Assumptions

It is assumed that the following physical conditions will exist in the environment of the TOE:

**A.LOCATE** The TOE will be located within controlled access facilities which will prevent unauthorised physical access.

**A.PROTECT** The TOE hardware and software will be protected from unauthorised physical modification.

### 3.1.2 Personnel Assumptions

It is assumed that the following personnel conditions will be enforced by the organisation in control of the environment of the TOE:

**A.MANAGE** There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

**A.NO_EVIL_ADM**

The system administrative personnel are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

**A.COOP** Authorised users possess the necessary authorisation to access at least some of the information managed by the

TOE and are expected to act in a cooperating manner in a benign environment.

**A.PASSWORD** Authorised users will choose a password that conforms to the length and complexity rules stated in the user guidance. These rules will be consistent with a SOF medium claim for the TOE.

### 3.1.3 Connectivity Assumptions

The following connectivity conditions are assumed:

**A.PEER** Any other system with which the TOE communicates is assumed to be under the same management control and operate under the same security policy constraints.

**A.CONNECT** All connections to peripheral devices reside within the controlled access facilities. Internal communication paths to access points such as terminals are assumed to be adequately protected.

**A.OS** The underlying operating system shall ensure that any information contained in a protected resource is not released when the resource is recycled; protect the TOE software from unauthorised modification and prevent the TSFs from being bypassed.

## 3.2 Threats

There are no explicit threats identified for the TOE. The security objectives are derived from the statement of Organisational Security Policy contained in Section 3.3.

## 3.3 Organisational Security Policies

The organisational security policies are described below.

**P.AUTHORISED_USERS**

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

**P.NEED_TO_KNOW**

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

**P.ACCOUNTABILITY**

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

# 4 SECURITY OBJECTIVES

## 4.1 TOE Security Objectives

The Security Objectives of the TOE comprise the following:

**O.AUTHORISATION**

The TSF must ensure that only authorised users gain access to the TOE and its resources.

**O.DAC** The TSF must control access to resources based on identity of users. The TSF must allow authorised users to specify which users may access which resources.

**O.AUDITING** The TSF must record the security relevant actions of users of the TOE. The TSF must present this information to authorised administrators.

**O.MANAGE** The TSF must provide all the functions and facilities necessary to support the authorised administrators that are responsible for the management of TOE security.

## 4.2 Environmental Security Objectives

### 4.2.1 IT Environmental Security Objectives

The IT security objectives for the environment comprise the following:

**O.RESIDUAL_INFORMATION**

The underlying operating system must ensure that any information contained in a protected resource is not released when the resource is recycled.

**O.NO_MOD** The underlying operating system must protect the TOE software from unauthorised modification.

**O.NO_BYPASS** The underlying operating system must prevent the TSFs from being bypassed.

### 4.2.2 Non-IT Environmental Security Objectives

The non-IT Environmental Security Objectives comprise the following:

**O.INSTALL** Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security objectives.

**O.PHYSICAL** Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security objectives, and by siting the TOE network environment in an adequately protected location. All connections to peripheral devices must reside within the controlled access facilities and internal communication paths to access points such as terminals are protected by their physical location.

**O.CREDEN** Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users in a manner that maintains IT security objectives. In addition, users should ensure that their passwords conform to the length and complexity rules stated in the user guidance. These rules will be consistent with a SOF medium claim for the TOE.

# 5 IT SECURITY REQUIREMENTS

## 5.1 Security Functional Requirements

### 5.1.1 Statement of Security Functional Requirements for the TOE

This section contains the security functional requirements for the TOE. The following CC Part 2 components are referenced. Completed definition text (i.e. added text not defined by the CC) is indicated below by *italics*.

#### 5.1.1.1 Security Audit (FAU)

##### 5.1.1.1.1 Audit Data Generation (FAU_GEN.1)

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

(a) Start-up and shutdown of the audit functions;

(b) *The auditable events listed in Table 5-1 (Auditable Events).*

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

(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, *any additional information specified in the "Details" column of Table 5-1 (Auditable Events).*

**Table 5-1: Auditable Events**

| SFR | Event | Details |
|---|---|---|
| FAU_STG.3 | Actions taken due to exceeding of a threshold. | |
| FDP_ACF.1 | All requests to perform an operation on an object covered by the SFP. | |
| FIA_UAU.1 | All *successful and unsuccessful* use of the authentication mechanism. | |
| FIA_UID.2 | All *successful* use of the user identification mechanism including the user identity provided. | |

#### 5.1.1.1.2 User Identity Association (FAU_GEN.2)

The TSF shall be able to associate each auditable event with the identity of the user that caused the event. $_{\text{FAU\_GEN.2.1}}$

#### 5.1.1.1.3 Audit Review (FAU_SAR.1)

The TSF shall provide *all users* with the capability to read *all audit information* from the audit records. $_{\text{FAU\_SAR.1.1}}$

The TSF shall provide the audit records in a manner suitable for the user to interpret the information. $_{\text{FAU\_SAR.1.2}}$

#### 5.1.1.1.4 Selectable Audit Review (FAU_SAR.3)

The TSF shall provide the ability to perform *searches* of audit data based on *the following attributes*: $_{\text{FAU\_SAR.3.1}}$

*(a) type of event;*

*(b) date.*

#### 5.1.1.1.5 Protected Audit Trail Storage (FAU_STG.1)

The TSF shall protect the stored audit records from unauthorised deletion. $_{\text{FAU\_STG.1.1}}$

The TSF shall be able to *prevent* modifications to the audit records. $_{\text{FAU\_STG.1.2}}$

#### 5.1.1.1.6 Action in Case of Possible Audit Data Loss (FAU_STG.3)

The TSF shall *generate an alarm to the authorised administrator* if the audit trail exceeds *80%*. $_{\text{FAU\_STG.3.1}}$

#### 5.1.1.1.7 Prevention of Audit Data Loss (FAU_STG.4)

The TSF shall *overwrite the oldest stored audit records (excluding alarms that have not been cleared)* if the audit trail is full. $_{\text{FAU\_STG.4.1}}$

### 5.1.1.2 User Data Protection (FDP)

#### 5.1.1.2.1 Discretionary Access Control Policy (FDP_ACC.1)

The TSF shall enforce the *Discretionary Access Control Policy* on *all processes acting on the behalf of users*. FDP_ACC.1.1

#### 5.1.1.2.2 Discretionary Access Control Functions (FDP_ACF.1)

The TSF shall enforce the *Discretionary Access Control Policy* to objects based on *the user identity associated with a subject*. FDP_ACF.1.1

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

*(a) a rule for each operation which uses either the user identity or the role of a subject as the basis of allowing or denying access.*

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

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

### 5.1.1.3 Identification and Authentication (FIA)

#### 5.1.1.3.1 User Attribute Definition (FIA_ATD.1)

The TSF shall maintain the following list of security attributes belonging to individual users: FIA_ATD.1.1

*(a) User Name;*

*(b) Role;*

(c) *Password.*

#### 5.1.1.3.2 Authentication (FIA_UAU.1)

The TSF shall allow *the user identification* on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.1

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on the behalf of that user. FIA_UAU.1.2

#### 5.1.1.3.3 Protected Authentication Feedback (FIA_UAU.7)

The TSF shall provide only *obscured feedback* to the user while the authentication is in progress. FIA_UAU.7

#### 5.1.1.3.4 Identification (FIA_UID.2)

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

#### 5.1.1.3.5 User-Subject Binding (FIA_USB.1)

The TSF shall associate the appropriate user security attributes with subjects acting on the behalf of that user: FIA_USB.1.1

### 5.1.1.4 Security Management (FMT)

#### 5.1.1.4.1 Static Attribute Initialisation (FMT_MSA.3)

The TSF shall enforce *the Discretionary Access Control Policy* to provide *restrictive* default values for security attributes that are used to enforce the SFP. FMT_MSA.3.1

The TSF shall allow *nobody* to specify alternative initial values to override the default values when an object or information is created. FMT_MSA.3.2

#### 5.1.1.4.2 Security Management Roles (FMT_SMR.1)

The TSF shall maintain the roles: FMT_SMR.1.1

*(a) Operator (O);*

*(b) Chief Operator (C);*

*(c) Administrator (A).*

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

### 5.1.2 Statement of Security Functional Requirements for the IT Environment

This section contains the security functional requirements for the IT environment. The following CC Part 2 components are referenced. Completed definition text (i.e. added text not defined by the CC) is indicated below by *italics*.

#### 5.1.2.1 User Data Protection

##### 5.1.2.1.1 Subset Residual Information Protection (FDP_RIP.1)

The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource* from the following objects: *the TOE application*. $_{\text{FDP\_RIP.1.1}}$

#### 5.1.2.2 Protection of the TSF

##### 5.1.2.2.1 Non-bypassability of the TSP (FPT_RVM.1)

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. $_{\text{FPT\_RVM.1.1}}$

##### 5.1.2.2.2 TSF Domain Separation (FPT_SEP.1)

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. $_{\text{FPT\_SEP.1.1}}$

The TSF shall enforce separation between the security domains of subjects in the TSC. $_{\text{FPT\_SEP.1.2}}$

##### 5.1.2.2.3 Reliable Time Stamps (FPT_STM.1)

The TSF shall be able to provide reliable time stamps for its own use. $_{\text{FPT\_STM.1.1}}$

## 5.2 Security Assurance Requirements

### 5.2.1 Statement of Security Assurance Requirements

The following security assurance requirements are claimed in accordance with the EAL3 requirements stated in [CC] Part 3.

**Table 5-2: Security Assurance Requirements**

| | |
|---|---|
| ACM_CAP.3 | Authorisation controls |
| ACM_SCP.1 | TOE CM coverage |

| | |
|---|---|
| ADO_DEL.1 | Delivery procedures |
| ADO_IGS.1 | Installation, generation, and start-up procedures |
| ADV_FSP.1 | Informal functional specification |
| ADV_HLD.2 | Security enforcing high-level design |
| ADV_RCR.1 | Informal correspondence demonstration |
| AGD_ADM.1 | Administrator guidance |
| AGD_USR.1 | User guidance |
| ALC_DVS.1 | Identification of security measures |
| ATE_COV.2 | Analysis of coverage |
| ATE_DPT.1 | Testing: high-level design |
| ATE_FUN.1 | Functional testing |
| ATE_IND.2 | Independent testing - sample |
| AVA_MSU.1 | Examination of guidance |
| AVA_SOF.1 | Strength of TOE security function evaluation |
| AVA_VLA.1 | Developer vulnerability analysis |

### 5.2.2 Statement of Strength of TOE Security Function

Strength of function, as a CC concept, applies to probabilistic or permutational mechanisms that are non-cryptographic in nature. This ST claims AVA_SOF.1 applicability for the user identification and authentication SFRs: FIA_UID.2 and FIA_UAU.1 through the user password entry function and its mechanism.

The minimum strength of function level for the password entry mechanism is SOF medium. This is achieved through procedural means i.e. the user guidance will inform the user that they have to choose a password of sufficient length and complexity to satisfy a SOF medium rating.

# 6 TOE SUMMARY SPECIFICATION

## 6.1 TOE Security Functions

The TOE IT Security Functions and their specifications are listed as follows.

**AUDIT** The TOE performs audit functions by recording all events listed in Table 5-1.

**DAC** The TOE controls access by an identified and authenticated user to those processes whose owner attribute is identical to that of the currently authenticated user.

**USER_LOGIN** The TOE requires the user to identify and authenticate via a user login.

The overall strength of function of the TOE IT security functions is SOF medium. Only the USER_LOGIN function is realised by a probabilistic mechanism and the strength of this function is SOF medium on the assumption that the users will choose passwords of sufficient length and complexity to be consistent with this claim.

## 6.2 Assurance Measures

The assurance measures that are provided by the TOE are described below:

**ACM_CAP** TOE releases are uniquely identified with the version number and model identifier. All Configuration Items that comprise the TOE are under Configuration Management and are included on a Configuration List and uniquely identified by part number.

**ACM_SCP** TOE Configuration Management coverage analysis is provided.

**ADO_DEL** The TOE delivery procedures ensure that secure delivery of the TOE is achieved.

**ADO_IGS** Automated installation procedures are adequate to ensure that the user starts the TOE within a secure configuration.

**ADV_FSP** An informal functional specification is supplied for the TOE.

**ADV_HLD** The TOE High Level Design documentation addresses the requirements of ADV_HLD.2

**ADV_RCR** A representational correspondence is supplied.

**AGD_ADM** The administrator's guide is adequate to provide administrators with the required knowledge to securely configure and maintain the TOE within the environment.

**AGD_USR** The User guidance is adequate to provide the user with the required knowledge to correctly perform login procedures and to provide security awareness of the TOE and its policies.

**ALC_DVS** Identification of security measures in the life cycle documentation is provided.

**ATE_COV** The analysis of coverage for testing is provided to assure completeness of coverage in testing of the TOE.

**ATE_DPT** Testing with respect to the High Level Design is provided.

**ATE_FUN** Functional testing of all security functions is provided in the referenced test plan.

**ATE_IND** The functional testing was performed by an independent third party.

**AVA_MSU** Examination of guidance is provided.

**AVA_SOF** The TOE Strength of Function Analysis addresses the requirements of AVA_SOF.1.

**AVA_VLA** The TOE vulnerability analysis addresses the requirements of AVA_VLA.1.

# 7 RATIONALE

## 7.1 Security Objectives Rationale and Traceability

The purpose of this section is to show that the security objectives of the TOE are appropriate to the security problem defined in the security environment section (see Section 1.2). This is accomplished through a set of tables that cross-reference threats, security policies and assumptions against the security objectives that address them. Each threat, policy or assumption is addressed by one or more security objective. Each security objective of the TOE (described in Section 4.1) addresses at least one threat, policy or assumption. An informal argument is provided to show, for each threat, policy or assumption, why the identified security objective provides an effective countermeasure that prevents an attack or mitigates risk to acceptable levels.

### 7.1.1 Security Objectives Rationale for Environmental Assumptions

The following table shows the mapping for each of the security objectives for the environment to the environmental assumptions.

**Table 7-1: Mapping for each of the Security Objectives**

| Security Objectives<br>Environmental Assumptions | O.INSTALL | O.PHYSICAL | O.CREDEN | O.RESIDUAL_INFORMATION | O.NO_MOD | O.NO_BYPASS |
|---|---|---|---|---|---|---|
| A.MANAGE | X | | | | | |
| A.NO_EVIL_ADM | X | | | | | |
| A.COOP | | | X | | | |
| A.LOCATE | | X | | | | |
| A.PASSWORD | | X | | | | |
| A.PROTECT | | X | | | | |
| A.PEER | X | | | | | |
| A.CONNECT | | X | | | | |
| A.OS | | | | X | X | X |

It is clear from the above representation that each environmental security objective addresses at least one environmental assumption and that each environmental assumption is addressed by at least one environmental security objective.

The rationale for the environmental assumptions against the environmental security objectives is given in the table below. For each assumption a list of security objectives for the environment is given, followed by an argument stating how each security objective enforces the assumption in question.

**Table 7-2: Environmental Assumptions Against the Environmental Security Objectives**

| Assumption | Security Objective | Rationale |
|---|---|---|
| **A.MANAGE** | O.INSTALL | O.INSTALL ensures that the secure state of the system is achieved on initialisation and that management of the system can proceed from a secure state. |
| **A.NO_EVIL_ADM** | O.INSTALL | O.INSTALL ensures that those responsible for the system will ensure the installation and management and operation are consistent with IT security objectives. This precludes the actions of a hostile administrator or supervisor. |
| **A.PEER** | O.INSTALL | O.INSTALL addresses A.PEER by ensuring that all other systems with which the TOE is connected are under the same management control and operate under the same security policy. |
| **A.LOCATE** | O.PHYSICAL | O.PHYSICAL provides for the requirements of A.LOCATE by ensuring that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security objectives through siting in an adequately protected location. |
| **A.PROTECT** | O.PHYSICAL | O.PHYSICAL directly addresses A.PROTECT by ensuring that the TOE hardware and software critical to security policy enforcement will be protected from unauthorised physical modification. |
| **A.CONNECT** | O.PHYSICAL | O.PHYSICAL directly addresses A.CONNECT by ensuring that all connections to peripheral devices reside within the controlled access facilities, and that internal communication paths to access points such as terminals are protected by their physical location. |
| **A.COOP** | O.CREDEN | O.CREDEN addresses A.COOP by ensuring that authorised users possess the necessary authorisation to access at least some of the information managed by the |

| Assumption | Security Objective | Rationale |
|---|---|---|
| | | TOE and are expected to act in a cooperating manner in a benign environment. This includes the requirement that all access credentials, such as passwords or other authentication information, are protected by the users in a manner that maintains IT security objectives. |
| **A.PASSWORD** | O.CREDEN | O.CREDEN addresses A.PASSWORD by ensuring that authorised users will select a password conforming to the required length and complexity requirements consistent with a SOF medium claim for the TOE. |
| **A.OS** | O.RESIDUAL_INFORMATION<br>O.NO_MOD<br>O.NO_BYPASS | The O.RESIDUAL_INFORMATION, O.NO_MOD and O.NO_BYPASS<br>address the assumptions that the IT environment security objectives and the underlying operating system will ensure that information contained in a protected resource is not released when the resource is recycled, that no unauthorised modifications are made to the TOE software and that the TSF cannot be bypassed. The password policy is as specified in the SOF manual. |

### 7.1.2 Organisational Policy Rationale

The mapping between the organisational policies enforced in the TOE Environment and the IT Security Objectives is shown in the table below.

**Table 7-3: Organisational Policy Rationale**

| **Security Objectives**<br>**Policies** | **O.AUTHORISATION** | **O.MANAGE** | **O.DAC** | **O.AUDITING** | **O.RESIDUAL_INFORMATION** | **O.NO_MOD** | **O.NO_BYPASS** |
|---|---|---|---|---|---|---|---|
| **P.AUTHORISED_USERS** | X | X | | | | X | X |
| **P.NEED_TO_KNOW** | | X | X | | X | X | X |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **P.ACCOUNTABILITY** | | X | | X | | | | |

The rationale for the policies against the IT security objectives is given in the table below. For each policy a list of IT security objectives is given, followed by an argument stating how each security objective satisfies the policy in question.

**Table 7-4: Organisational Policy**

| Organisational Policy | Security Objective | Rationale |
|---|---|---|
| **P.AUTHORISED_USERS** | **O.AUTHORISATION**<br>**O.MANAGE**<br>**O.NO_MOD**<br>**O.NO_BYPASS** | P.AUTHORISED_USERS states that only those users authorised to access the information assets of the system may access the system. The policy is implemented by O.AUTHORISATION, and supported by O.MANAGE by requiring authorised administrators to be able to manage the functions. O.NO_MOD and O.NO_BYPASS ensure that the TOE security objectives meeting P.AUTHORISED_USERS cannot be tampered with or bypassed. |
| **P.NEED_TO_KNOW** | **O.MANAGE**<br>**O.DAC**<br>**O.RESIDUAL_INFORMATION**<br>**O.NO_MOD**<br>**O.NO_BYPASS** | P.NEED_TO_KNOW states that the system must limit access to, modification of, and destruction of information to those authorised users having a need-to-know. O.DAC implements this policy. O.MANAGE supports the policy by requiring authorised administrators to manage the functions. O.RESIDUAL_INFORMATION ensures that information is not given to users without a need-to-know when resources are reused. O.NO_MOD and O.NO_BYPASS ensure that the TOE security objectives meeting P.NEED_TO_KNOW cannot be tampered with or bypassed. |
| **P.ACCOUNTABILITY** | **O.MANAGE**<br>**O.AUDITING** | P.ACCOUNTABILITY requires users of the system to be held accountable for their actions in the system. This policy is implemented by O.AUDITING in |

| Organisational Policy | Security Objective | Rationale |
|---|---|---|
| | | requiring the recording of actions in an audit trail. O.MANAGE supports this by requiring the secure management of the audit trail. |

## 7.2 Security Requirements Rationale

### 7.2.1 TOE Security Functional Requirements (SFRs) Rationale

The mapping between the SFRs and the Security Objectives is shown in the table below. The SFRs appear on the left for each row, and corresponding Security Objectives are indicated by an 'X' in the appropriate column.

**Table 7-5: TOE Security Functional Requirements**

| SFR | Description | O.AUTHORISATION | O.DAC | O.AUDITING | O.MANAGE |
|---|---|---|---|---|---|
| FAU_GEN.1 | Audit Data Generation | | | X | |
| FAU_GEN.2 | User Identity Association | | | X | |
| FAU_SAR.1 | Audit Review | | | X | X |
| FAU_SAR.3 | Selectable Audit Review | | | X | X |
| FAU_STG.1 | Protected Audit Trail Storage | | | X | |
| FAU_STG.3 | Action in Case of Possible Audit Data Loss | | | X | X |
| FAU_STG.4 | Prevention of Audit Data Loss | | | X | X |
| FDP_ACC.1 | Discretionary Access Control Policy | | X | | |
| FDP_ACF.1 | Discretionary Access Control Functions | | X | | |
| FIA_ATD.1 | User Attribute Definition | X | X | | |
| FIA_UAU.1 | Authentication | X | | | |
| FIA_UAU.7 | Protected Authentication Feedback | X | | | |
| FIA_UID.2 | Identification | X | | | |
| FIA_USB.1 | User-Subject Binding | | X | X | |

| SFR | Description | O.AUTHORISATION | O.DAC | O.AUDITING | O.MANAGE |
|---|---|---|---|---|---|
| FMT_MSA.3 | Static Attribute Initialisation | | X | | |
| FMT_SMR.1 | Security Management Roles | | | | X |
| FAU_GEN.1 | Audit Data Generation | | | X | |
| FAU_GEN.2 | User Identity Association | | | X | |
| FAU_SAR.1 | Audit Review | | | X | X |
| FAU_SAR.3 | Selectable Audit Review | | | X | X |
| FAU_STG.1 | Protected Audit Trail Storage | | | X | |
| FAU_STG.3 | Action in Case of Possible Audit Data Loss | | | X | X |
| FAU_STG.4 | Prevention of Audit Data Loss | | | X | X |
| FDP_ACC.1 | Discretionary Access Control Policy | | X | | |
| FDP_ACF.1 | Discretionary Access Control Functions | | X | | |
| FIA_ATD.1 | User Attribute Definition | X | X | | |
| FIA_UAU.1 | Authentication | X | | | |
| FIA_UAU.7 | Protected Authentication Feedback | X | | | |
| FIA_UID.2 | Identification | X | | | |
| FIA_USB.1 | User-Subject Binding | | X | X | |
| FMT_MSA.3 | Static Attribute Initialisation | | X | | |
| FMT_SMR.1 | Security Management Roles | | | | X |

The rationale for the SFRs against the security objectives of the TOE is given in the table below. For each security objective of the TOE, a list of assigned SFRs is given, followed by an argument stating how each SFR addresses or satisfies the security objective in question.

**Table 7-6: TOE SFR security objective**

| Security Objective | SFR | Rationale |
|---|---|---|
| **O.AUTHORISATION** | FIA_ATD.1<br>FIA_UAU.1<br>FIA_UAU.7<br>FIA_UID.2 | FIA_ATD.1 provides that the TSF maintain the user identifiers, roles, passwords that enable identification and authentication of users. |

| Security Objective | SFR | Rationale |
|---|---|---|
| | | FIA_UAU.1 allows only the user identification on behalf of the user to be performed before the user is authenticated.<br>FIA_UAU.7 prevents the disclosure of user password information during login.<br>FIA_UID.2 allows no other actions to be taken by the user prior to user identification.<br>These requirements collectively ensure that only authorised users gain access to the TOE and its resources. |
| **O.DAC** | FDP_ACC.1<br>FDP_ACF.1<br>FIA_ATD.1<br>FIA_USB.1<br>FMT_MSA.3 | FDP_ACC.1 provides that the TOE Discretionary Access Control Policy is enforced and allows authorised users to forward messages to other authorised users, thereby providing discretionary access and ownership transfer between users.<br>FDP_ACF.1 provides that each user identity/role is associated with a controlled subject/object and that protections are carried with it, whenever that subject/object is read, written, deleted and released.<br>FIA_ATD.1 provides that the TSF maintain the user identifiers, roles, passwords that enable identification and authentication of users.<br>FIA_USB.1 associates appropriate user security attributes with subjects acting on the behalf of that user.<br>FMT_MSA.3 enforces discretionary access control by provide restrictive default values for users on creation. |
| **O.AUDITING** | FAU_GEN.1<br>FAU_GEN.2<br>FAU_SAR.1<br>FAU_SAR.3<br>FAU_STG.1<br>FAU_STG.3<br>FAU_STG.4<br>FIA_USB.1<br>FPT_STM.1 | FAU_GEN.1 and FAU_GEN.2 provide that audit records will be generated for selected events and that the TSF shall be able to associate each auditable event with the identity of the user that caused the event.<br>FAU_SAR.1 provides that the TSF shall provide authorised administrators with the capability to read all audit information from the audit records.<br>FAU_SAR.3 provides that the TSF shall provide the ability to perform searches of specified types on the audit records.<br>FAU_STG.1 provides that the TSF shall protect the stored audit records from unauthorised deletion, and to prevent modifications to the audit records. Thus the integrity of audit records is guaranteed.<br>FAU_STG.3 provides that the TSF shall generate an alarm to the authorised administrator if the audit trail exceeds 80%.<br>FAU_STG.4 ensures that the latest audit records are maintained.<br>FIA_USB.1 associates appropriate user security attributes with subjects acting on the behalf of that user.<br>FPT_STM.1 provides a reliable time stamp to the audit generation, ensuring the accuracy of the time appeared in audit records. |
| **O.MANAGE** | FAU_SAR.1<br>FAU_SAR.3 | FAU_SAR.1 provides that the TSF shall provide authorised administrators with the capability to read all audit information |

| Security Objective | SFR | Rationale |
|---|---|---|
| | FAU_STG.3<br>FAU_STG.4<br>FMT_SMR.1 | from the audit records.<br>FAU_SAR.3 provides that the TSF shall provide the ability to perform searches of specified types on the audit records.<br>FAU_STG.3 provides that the TSF shall generate an alarm to the authorised administrator if the audit trail exceeds 80%.<br>FAU_STG.4 ensures that the latest audit records are maintained.<br>FMT_SMR.1 provides that the TSF maintain roles and that the roles can be associated by the TSF with users |

The coverage of the above table against the SFRs satisfies the following properties:

- for every security objective of the TOE, there is at least one SFR that satisfies it;
- for every SFR, there is at least one security objective of the TOE that it addresses; and
- for every security objective of the TOE, an informal argument as to why the identified SFRs are sufficient to meet it is provided.

### 7.2.2 IT environment Security Functional Requirements (SFRs) Rationale

The mapping between the SFRs and the Security Objectives is shown in the table below. The SFRs appear on the left for each row, and corresponding Security Objectives are indicated by an 'X' in the appropriate column.

**Table 7-7: IT environment Security Functional Requirements**

| SFR | Description | O.RESIDUAL_INFORMATION | O.NO_MOD | O.NO_BYPASS | O.AUDITING |
|---|---|---|---|---|---|
| FDP_RIP.1 | Subset Residual Information Protection | X | | | |
| FPT_RVM.1 | Non-bypassability of the TSP | | | X | |
| FPT_SEP.1 | TSF Domain Separation | | X | | |
| FPT_STM.1 | Reliable Time Stamp | | | | X |

The rationale for the SFRs against the security objectives of the IT environment is given in the table below. For each security objective of the IT environment, a list of assigned SFRs is given, followed by an argument stating how each SFR addresses or satisfies the security objective in question.

Table 7-8: SFR security objective

| Security Objective | SFR | Rationale |
|---|---|---|
| **O.RESIDUAL_INFORMATION** | FDP_RIP.1 | FDP_RIP.1 provides that the IT environment would protect residual information contained in resources to be recycled. |
| **O.NO_MOD** | FPT_SEP.1 | FPT_SEP.1 provides that the IT environment would maintain the TOE in a secure domain protected from modification. |
| **O.NO_BYPASS** | FPT_RVM.1 | FPT_RVM.1 provides that the IT environment would ensure successful invoking of the TSP enforcement functions. |

### 7.2.3 SFR Dependency Rationale

The following table shows the dependency analysis of the claimed SFRs for the TOE and the IT environment. The traceability of an SFR dependency is confirmed by selecting an SFR from the left-hand column and noting the columns in which an ‘X’ appears. Each such column determines an SFR that should be included in the claims of Section 5 by way of a dependency rule specified in the CC, Part 2. In the case where an alternative is specified in the CC, at least one of the alternative SFRs has been chosen.

By confirming that each column SFR is also a row SFR in the matrix, the property of closure under dependencies is established for Section 5.

> **Note:** In this TOE FMT_MSA.3 does not depend on FMT_MSA.1 because role defaults are established by the developer and cannot be amended by users or Administrators.

Table 7-9: SFR Dependency Rationale

| SFR | FAU_GEN.1 | FAU_SAR.1 | FAU_STG.1 | FDP_ACC.1 | FDP_ACF.1 | FDP_RIP.1 | FIA_ATD.1 | FIA_UAU.1 | FIA_UID.2 | FMT_MSA.3 | FMT_SMR.1 | FPT_RVM.1 | FPT_SEP.1 | FPT_STM.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **FAU_GEN.1** | | | | | | | | | | | | | | X |

| SFR | FAU_GEN.1 | FAU_SAR.1 | FAU_STG.1 | FDP_ACC.1 | FDP_ACF.1 | FDP_RIP.1 | FIA_ATD.1 | FIA_UAU.1 | FIA_UID.2 | FMT_MSA.3 | FMT_SMR.1 | FPT_RVM.1 | FPT_SEP.1 | FPT_STM.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FAU_GEN.2 | X | | | | | | | | X | | | | | |
| FAU_SAR.1 | X | | | | | | | | | | | | | |
| FAU_SAR.3 | | X | | | | | | | | | | | | |
| FAU_STG.1 | X | | | | | | | | | | | | | |
| FAU_STG.3 | | | X | | | | | | | | | | | |
| FAU_STG.4 | X | | | | | | | | | | | | | |
| FDP_ACC.1 | | | | | X | | | | | | | | | |
| FDP_ACF.1 | | | | X | | | | | | | | | | |
| FDP_RIP.1 | | | | | | | | | | | | | | |
| FIA_ATD.1 | | | | | | | | | | | | | | |
| FIA_UAU.1 | | | | | | | | | X | | | | | |
| FIA_UAU.7 | | | | | | | | X | | | | | | |
| FIA_UID.2 | | | | | | | | | | | | | | |
| FIA_USB.1 | | | | | | | X | | | | | | | |
| FMT_MSA.3 | | | | | | | | | | | X | | | |
| FMT_SMR.1 | | | | | | | | | X | | | | | |
| FPT_RVM.1 | | | | | | | | | | | | | | |
| FPT_SEP.1 | | | | | | | | | | | | | | |
| FPT_STM.1 | | | | | | | | | | | | | | |

### 7.2.4 Security Assurance Requirements Rationale (SARs)

Given the statement of security environment and security objectives contained in this ST, an assurance level of EAL3 is appropriate to capture the moderate level of independently assured protection provided by the TOE. For environments that have an adequate security policy and set of security procedures that address the issues raised in the environmental assumptions (see Section 3.1), the services of the TOE will provide secure discretionary access control and audit services.

The vulnerability analysis required by AVA_VLA.1 and strength of function analysis required by AVA_SOF.1 are appropriate for the level of protection claimed by this TOE, and is provided, as referenced in Section 6.2 (see also Section 5.2.2 for claim).

## 7.3 TOE Summary Specification Rationale

### 7.3.1 IT Security Functions Rationale (SFRs)

The mapping between the IT security functions and the SFRs is shown in the table below.

**Table 7-10: IT Security Functions Rationale**

| SFR | AUDIT | DAC | USER_LOGIN |
|---|---|---|---|
| FAU_GEN.1 | X | | |
| FAU_GEN.2 | X | | |
| FAU_SAR.1 | X | | |
| FAU_SAR.3 | X | | |
| FAU_STG.1 | X | | |
| FAU_STG.3 | X | | |
| FAU_STG.4 | X | | |
| FDP_ACC.1 | | X | |
| FDP_ACF.1 | | X | |
| FIA_ATD.1 | | X | |
| FIA_UAU.1 | | | X |
| FIA_UAU.7 | | | X |
| FIA_UID.2 | | | X |
| FIA_USB.1 | | | X |
| FMT_MSA.3 | | X | |
| FMT_SMR.1 | | X | |

The IT security functions appear on the left for each row and the corresponding SFRs are indicated by an ‘X’ in the appropriate column.

The detailed traceability of the TSF to the Security Function Requirements follows. The TOE IT Security Functions are referenced to the list of SFRs, described in Section 5, that are provided by the defined IT Security Function. Specifications of IT Security Functions are provided in Section 6.1. A Coverage Mapping is included to describe how the IT Security Functions covers the referenced SFR.

**Table 7-11: IT Security Functions**

| Security Functional Requirement | IT Security Function | IT Security Function to SFR Coverage Mapping |
|---|---|---|
| FAU_GEN.1 | AUDIT | AUDIT creates audit records satisfying the FAU_GEN.1 requirements for auditable events. |
| FAU_GEN.2 | AUDIT | AUDIT creates audit records satisfying the FAU_GEN.2 requirements for association of auditable events with user name. |
| FAU_SAR.1 | AUDIT | AUDIT provides everybody with the capability of reading all audit records and presents the records in a manner suitable to interpret. |
| FAU_SAR.3 | AUDIT | AUDIT provides the ability to perform searches for audit events using event-type and/or dates as keys. |
| FAU_STG.1 | AUDIT | AUDIT protects audit records from deletion and modification. |
| FAU_STG.3 | AUDIT | AUDIT generates an alarm to the administrator if the audit trail exceeds 80%. |
| FAU_STG.4 | AUDIT | AUDIT overwrites the oldest audit records (excluding any alarms that have not been acknowledged) when the audit log is full and generate an alarm to say that it has done so. |
| FDP_ACC.1 | DAC | DAC provides the TOE DAC policy on all user subjects, message objects and operations between subjects and objects. |
| FDP_ACF.1 | DAC | DAC enforces the DAC policies specified in FDP_ACF.1. |
| FIA_ATD.1 | DAC | DAC maintains the required user attributes necessary to correctly mediate all DAC policies. |
| FIA_UAU.1 | USER_LOGIN | USER_LOGIN does not permit user actions other than user identification to be performed prior to user authentication. |
| FIA_UAU.7 | USER_LOGIN | USER_LOGIN does not provide explicit feedback to the user while authentication is in progress. |
| FIA_UID.2 | USER_LOGIN | USER_LOGIN does not permit user actions prior to authentication with the exception of user identification. |
| FIA_USB.1 | USER_LOGIN | USER_LOGIN provides a binding between user name and auditable events and discretionary access control mediations. |
| FMT_MSA.3 | DAC | DAC enforces discretionary access control to provide restrictive default values for users on creation. |
| FMT_SMR.1 | DAC | DAC enforces the security roles: a) Operator; b) Chief Operator & c) Administrator. |

The combined aggregate of the TOE security functions satisfies the set of identified TOE SFRs as shown above. Provided the configuration and maintenance of the TOE is carried out in accordance with organisational policy, environmental assumptions the TOE security functional claims are valid.

# 8 REFERENCES

**CC** Common Criteria for Information Technology Security Evaluation, August 1999, Version 2.1, CCIMB-99-032

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