EADS
CASA

DOCUMENTO TECNICO
TECHNICAL DOCUMENT

Documento nº/Document no.	Avión/Aircraft
DT-T-MEE44-10001	General

Título/Title

EADS GROUND SEGMENT SYSTEMS PROTECTION PROFILE

Realizado/Prepared	Firma/Signature	
	Nombre/Name	Sergio Torralba Urrutia
	Cargo/Position	Information Security Engineer
Comprobado/Checked	Firma/Signature	Montse Herrera
	Nombre/Name	Montserrat Herrera Esparrach
	Cargo/Position	Head of System Accreditation
Aprobado/Approved	Firma/Signature	
	Nombre/Name	Miguel Ángel Gil Jiménez
	Cargo/Position	Head of Engineering Processes, Tools and Accreditation

Fecha 1ª edición 1st issue date	July 2010
Clas. Acceso Access class.	P1

REGISTRO DE REVISIONES/REVISIONS RECORD

Revisión	Motivo de Modificación/Change reason	Realiz./Prep.	Compr/Check	Aprobado/App.
Fecha/Date	Capítulos, Secciones, Hojas afectadas/Chapters, Sections, Sheets affected	Firma/Sign.	Firma/Sign.	Firma/Sign.
Issue A	Initial Release	Sergio Torralba Urrutia	Montserrat Herrera Esparrach	Miguel Ángel Gil Jiménez
July 2010	Initial Release			
Issue B	INTA Comments. Title Doc.: PP Ground Systems Observations Report. Doc.: PPG-COM-2035-001-INTA.	Sergio Torralba Urrutia	Montserrat Herrera Esparrach	Miguel Ángel Gil Jiménez
September 2010	All the document			

INDEX

Título/Title **Página/Page**

0. PREFACE

0.1 Related Documents

Reference	Document Related
[CC_Part1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, CCMB-2009-07-001, v3.1 Release 3, Final, July 2009.
[CC_Part2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2009-07-002, v3.1 Release 3, Final, July 2009.
[CC_Part3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2009-07-003, v3.1 Release 3, Final, July 2009.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, CCMB-2009-07-004, v3.1 Release 3, Final, July2009.
[CCRA]	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, May 2000.
[NATO]	ROADMAP to NATO Security Policy, Supporting Directives, Documents and Guidance for the Communication and Information Systems (CIS). Version 1.5. 13 June 2007.

Table 1. Related Documents

0.2 ACRONYMS AND DEFINITIONS

0.2.1 Acronyms

Term	Description
CC	Common Criteria for Information Technology Security Evaluation.
CIS	Communication and Information System.
DOB	Deployed Operating Base.
ISM	Installation Security Manager.
MOB	Main Operating Base.
OSP	Organisational Security Policy.
PP	Protection Profile.
SFR	Security Functional Requirement.
ST	Security Target.
SyOPs	Security Operating Procedures.

Term	Description
TOE	Target Of Evaluation.
UAV	Unmanned Aircraft Vehicle.

Table 2. Acronyms

0.2.2 Definitions

Term	Definition
Adverse Action	Actions performed by a threat agent on an asset. [CC_Part1].
Assurance	Grounds for confidence that a TOE meets the SFRs. [CC_Part1].
Evaluation	Assessment of a PP, an ST or a TOE, against defined criteria. [CC_Part1].
Protection Profile	Implementation-independent statement of security needs for a TOE type. [CC_Part1].
Security Objective	Statement of an intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions. [CC_Part1].
Security Problem	Statement which in a formal manner defines the nature and scope of the security that the TOE is intended to address. [CC_Part1].
Security Requirement	Requirement, stated in a standardised language, which is meant to contribute to achieving the security objectives for a TOE. [CC_Part1].
Security Target	Implementation-dependent statement of security needs for a specific identified TOE. [CC_Part1].
Target Of Evaluation	Set of software, firmware and/or hardware possibly accompanied by guidance. [CC_Part1].
Threat	A threat consists of an adverse action performed by a threat agent on an asset. [CC_Part1].
Threat Agent	Entity that can adversely act on assets. [CC_Part1].

Table 3. Definitions

1. PP INTRODUCTION (APE_INT)

This section describes de TOE in a narrative way providing identification material for the PP and describing it briefly.

1.1 PP Reference

Title: EADS Ground Segment Systems Protection Profile.

Version: Issue B.

Common Criteria Version: 3.1 Release 3 Final.

Author: EADS-CASA. EADS Defence & Security Division. Military Air Systems Business Unit.

Publication Date: 06-09-2010

1.2 TOE Type

This TOE reference to a military-purpose Ground Segment Systems which allows to prepare, to manage and to upload mission data to an aircraft previously a mission.

1.3 TOE Overview

Ground Segment Systems are these systems used by the aircraft crew to manage all the classified or unclassified data related to the aircraft (mission data, health data, etc.).

Ground Segment Systems are located in a Main Operating Base (MOB) or in a Deployed Operating Base (DOB) and should include among others the following functionality:

- Mission Management: mission plan data preparation and re-planning.
- Mission Briefing/Debriefing.
- Payloads data exploitation.
- Data Recording.

The TOE is a software solution, usually composed by two domains, with the possibility to include hardware, but there are some hardware components out of the TOE where the TOE relies to run on (this hardware could be laptops, workstations, servers or even real time platforms if the aircraft is an UAV).

2. CONFORMANCE CLAIMS (APE_CCL)

This section of a PP describes how the PP conforms with other PPs and with packages.

2.1 Common Criteria Conformance Claim

This Protection Profile is Common Criteria for Information Technology Security Evaluation version 3.1 Release 3 Final:

- Part 1 [CC_Part1] conformant.
- Part 2 [CC_Part2] extended.
  - Anti-Virus Actions (FAV_ACT_EXP.1).
  - Anti-Virus Alerts (FAV_ALR_EXP.1).
- Part 3 [CC_Part3] conformant.

2.2 Protection Profile Claim

This Protection Profile is not based on any other Protection Profile.

2.3 Package Conformance Claim

This Protection Profile conforms to Common Criteria Evaluation Assurance Level (EAL) 4.

2.4 Conformance Rationale

As this PP does not claim conformance to another PP, this section is not applicable.

2.5 Conformance statement

The conformance required for this PP is **demonstrable**.

3. SECURITY PROBLEM DEFINITION (APE_SPD)

This section defines the security problem that is to be addressed.

The main security problem is to protect the information stored and managed by the Ground Segment Systems, as well as the confidentiality, integrity or availability of which could be compromised.

3.1 Threats

This section of the security problem definition shows the threats that are to be countered by the TOE, its operational environment, or a combination of the two.

The types of threats can be described, generically, by the nature of the intentionality of the cause which may impact on the System, as follows:

- **Accidental or casual:** It states unintentional cause or unknowing damage. Combination of circumstances that cannot be avoided or foreseen.
- **Deliberate or intentional:** It is intended in terms of conscious design or purpose with premeditation or intention; "intentional damage" or "a knowing attempt to defraud"

Threats can also be categorised by the type the impact on the System:

- **Availability:** The property of information being accessible and usable upon demand by an authorized individual or entity
- **Integrity:** The property that information (including data) has not been altered or destroyed in an unauthorized manner.
- **Confidentiality:** The property that information is not made available or disclosed to unauthorized individuals or entities

The actuation of a threat, of a deliberate nature, would be in the form of an attack on a CIS by a threat agent, through exploitation of any vulnerability(s).

The definition of the type and cause of a threat is essential for the impact (severity) or for its feasibility (opportunity) which it can have on the system.

The type of threats can be classified as:

- **Natural:** This term is intended to cover all those events or incidents caused by the action of nature forces such as earthquakes, water, winds or storms.
- **Human:** This term encompasses all those threats where the human factor is the factor of trigger for the event. It can be caused by omission (passive subject) or action (active subject).
- **Environmental:** It is considered all those threats where the condition of the situation and location of the system in a particular moment, might trigger and materialize the threats and cause an impact on the subject system. This can take the form of theft from insecure facilities. In addition, this threat type also addresses power surges, power failures or other environmental damage.

According to the reference [NATO], the term threat agents can be split into three general types, as follows:

- **Adversarial threats:** Individuals, groups, organisations and nation states with the intent, motivation, capabilities, and resources to exploit the vulnerabilities of an information system to further their objectives. This includes malicious hackers, often referred to as "crackers";

- **Non-adversarial threats:** Individuals, groups, organisations and, in some circumstances, nation states that have no objectives, motivations, or intentions to cause harm to a system. This includes authorised users' errors and recreational hackers. Although there is no intention to cause harm, they have the capability of doing the wrong thing at the wrong time and causing a level of harm that sometimes surpasses that of an adversary with intent to harm; and

- **Natural and technological disasters:** This includes weather and geological phenomenon such as tornadoes, floods and earthquakes, as well as technological disasters such as toxic spills and power or telephone failures.

Threats are stated below:

Threat	Definition
T.ABUSE	**An attacker from inside or outside the organisation** with special rights (network administration) **modifies** the operating characteristics of the **resources** without informing the users.
T.DATA_CORRUPTION	**An attacker from inside or outside the organisation** gains access to the equipment of the information system and **corrupts or delete the sensitive information** in an unauthorised manner.
T.DOS	**Users** due to a misuse can cause an **IT assets** (hardware, software, network, etc.) **overload**.
T.EQUIPMENT_THEFT	**Someone inside or outside the organisation** accessing equipment located on the premises or transported outside **steals** the **equipment**.
T.IMPERSONATION	**A person assumes the identity of a different person** in order to use his/her access rights to the **information system**, commit a fraud, etc.
T.INFORMATION_DISCLOSURE	**Someone inside the organisation** who, through negligence, **passes information** to others in the organisation who have no need to know or to the outside.
T.INFORMATION_THEFT	**Someone inside or outside the organisation** accessing digital media with the intention of **stealing** and using the **information** on them.
T.UNAUTHORIZED_USE	**An attacker from inside or outside the organisation** accesses the **information system** and uses one of its services to **penetrate** it, **runs unauthorised operations** or **steal** information.
T.UNTRUSTWORTHY_DATA	**Outside sources send false data** or unsuitable equipment being used inside the organisation compromising the **system**.

Table 4. Threats

3.2 Organisational Security Policies

This section of the security problem definition shows the OSPs that are to be enforced by the TOE, its operational environment, or a combination of the two.

Organisational Security Policies are sated below:

Organizational Security Policy	Definition
P.ACCOUNTABILITY	The users of the TOE shall be held accountable for their actions within the TOE.
P.AUTHORISED_USERS	Only those users who have been authorised access to information within the system may access the TOE.
P.AUTOMATIC_SCAN	The TOE must be able to initiate automatic virus scans of removable media (e.g. USB pen drives, CD/DVD) when introduced into the workstation before accessing any data on the removable media.
P.EXTERNAL	The TOE must be able to prevent attacks from external systems.
P.NEED_TO_KNOW	The TOE must limit the access to, modification of, and deletion of the objects to those authorised users which have a "need to know" for that information. The access rights to specific data objects are determined by the owner of the object, the role of the subject attempting access, and the implicit and explicit access rights to the object granted to the role by the object owner.

Table 5. Organisational Security Policies

3.3 Assumptions

This section of the security problem definition shows the assumptions that are made on the operational environment in order to be able to provide security functionality. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may not be able to provide all of its security functionality anymore. Assumptions can be on physical, personnel and connectivity of the operational environment.

Assumptions are sated below:

Assumptions	Definition
A.ACCESS	The rights for users to gain access and perform operations on information are based on their user profile. The user profile is created by the TOE administrator according to the users allowed access and operations.
A.AUDIT_REVIEW	The ISM shall inspect the security audit and accounting log(s) on a regular and sufficiently frequent basis to detect any patterns of user behaviour that may be a threat to security.
A.DEVELOPEMENT	All in-service software development, modification, maintenance and testing shall be carried out on a physically separate system which shall be electronically isolated from the TOE.
A.INSTALL	Procedures shall exist to ensure that the system is installed in a secure manner.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

Assumptions	Definition
A.NO_EVIL_ADMIN	The system administrative personnel are not careless, will fully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
A.PROTECT	TOE hardware and software critical to security policy enforcement will be protected from unauthorised physical modification including unauthorised modifications by potentially hostile outsiders. It is assumed that all software and hardware, including network and peripheral cabling is approved for the transmittal of the protectively marked data held by the system. Such items are assumed to be physically protected against threats to the confidentiality and integrity of the data transmitted.
A.SEC_OPERATION	Security Operating Procedures (SyOPs) shall exist to ensure that the system is operated in a secure manner.
A.SYOPS	All users will be trained in accordance with their duties and will read, understand, and obey all the relevant Security Operating Procedures (SyOPs).
A.USER_ID	Each individual user shall be identified unequivocally by IT functions or by organisational procedures.

Table 6. Assumptions

4. SECURITY OBJETIVES (APE_OBJ)

This section states the security objectives which are divided into two part wise solutions. These part wise solutions are called the security objectives for the TOE and the security objectives for the operational environment. This reflects that these part wise solutions are to be provided by two different entities: the TOE, and the operational environment.

4.1 Security Objectives for the TOE

Security Objectives for the TOE are sated below:

Security Objectives	Definition
O.AUDITING	The TOE must record the security relevant actions of users of the TOE. The TOE must present this information to authorised administrators. The TOE must provide the means of recording security relevant events in sufficient detail to help an administrator of the TOE detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.
O.I&A	The TOE must ensure that only authenticated users gain access to the TOE and its resources, associating in addition an identity to the authenticated user. It shall control user issues related to identification and authentication as failures, verification of secrets, timing of authentication and identification, and authentication feedback.
O.DAC	The TOE must control access to resources based on identity of users. The TOE must allow authorised users to specify which users may access which resources controlling the access and controlling the user credentials.
O.VIRUS	The TOE must check data received from external sources to be protected from malicious code.
O.MANAGE	The TOE must allow administrators to effectively manage the TOE and its Security Functionality, and must ensure that only authorised administrators are able to access such functionality. It includes to control the management of audit data, security attributes, TSF data,
O.RESIDUAL_INFO	The TOE must ensure that any information contained in a protected resource is not released when the resource is recycled or reused.
O.SECURITY_POLICY	The TOE must ensure that information sent to sources is limited to that defined by the security policy.

Table 7. Security Objectives for the TOE

4.2 Security Objectives for the operational environment

Security Objectives for the operational environment are sated below:

Security Objectives	Definition
O. E_ACCESS	Those responsible for the administration must ensure that the rights for users to gain access and perform operations on information are based on their user profile. The user profile is created by the TOE administrator and it accurately reflects the user's job function.
O.E_ACCOUNTABLE	Those responsible for the TOE must ensure that: • The TOE is configured such that only the approved users may access the system. • Each individual user is assigned a unique user ID or identified unequivocally.
O.E_ADMIN	Those responsible for the administration of the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
O.E_AUDITDATA	Those responsible for the TOE must ensure that the audit functionality is used and managed effectively. In particular: • Procedures must exist to ensure that the audit trail for the product (i.e., all networked components containing an audit trail) is regularly analysed and archived, to allow retrospective inspection. • The auditing system must be configured such that the loss of audit data is minimised upon planned or unplanned shutdown or lack of available audit storage. • The media on which audit data is stored must not be physically removable from the platform by unauthorised users.
O.E_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 which maintains IT security objectives. Those responsible for the TOE must ensure that user authentication data is stored securely and not disclosed to unauthorised individuals. In particular: • Procedures must 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. • The media on which authentication data is stored must not be physically removable from the system by unauthorised users. • Users must not disclose their passwords to other individuals.

O.E_EXTERNAL_SYS	Those responsible for the TOE must establish and implement procedures to ensure that the users: • Review the classification of the information prior to dissemination assuring that users know the security mark and • Ensuring that the protective marking of the TOE information is consistent with the external system to which the information is being sent.
O.E.HW&SW_INSTALL	The installation of those parts of the TOE critical to security policy (e.g. servers, firewall, DMZ) is protected from physical attack which might compromise IT security objectives.
O.E_INSTALL	Those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the system are installed and configured in a secure manner.
O.E_LOCATE	The operational environment must ensure that the TOE shall be located within controlled access facilities of the MOB which will prevent unauthorised physical access. The physical controls at the MOB will alert the system authorities to the physical presence of attackers within the controlled space where the TOE is located.
O.E_PROTECT	The operational environment must ensure that the TOE hardware and software critical to security policy enforcement shall be protected from unauthorised physical modification including unauthorised modifications by potentially hostile outsiders. This includes all software and hardware, including network and peripheral cabling is approved for the transmittal of the protectively marked data held by the system.
O.E_SECOP	Those responsible for the TOE must establish and implement procedures to ensure that the users will be trained in accordance with their duties and will read, understand, and obey all relevant Security Operating Procedures (SecOPs).
O.E_SW_LIFECYCLE	The software development, modification, maintenance and testing shall be carried out on a physically separate system which shall be electronically isolated from the TOE.

Table 8. Security Objectives for the operational environment

4.3 Security objectives rationale

This section trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective, and trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

Threats, policies, and assumptions	Objectives																		
	O.AUDITING	O.I&A	O.DAC	O.VIRUS	O.MANAGE	O.RESIDUAL_INFO	O.SECURITY_POLICY	O. E_ACCESS	O.E_ACCOUNTABLE	O.E_ADMIN	O.E_AUDITDATA	O.E_CREDEN	O.E_EXTERNAL_SYS	O.E.HW&SW_INSTALL	O.E_INSTALL	O.E_LOCATE	O.E_PROTECT	O.E_SECOP	O.E_SW_LIFECYCLE
T.ABUSE	✓																		
T.DATA_CORRUPTION		✓	✓																
T.DOS					✓		✓										✓		
T.EQUIPMENT_THEFT		✓															✓		
T.IMPERSONATION	✓	✓	✓																
T.INFORMATION_DISCLOSURE													✓						
T.INFORMATION_THEFT		✓															✓		
T.UNAUTHORIZED_USE	✓	✓	✓																
T.UNTRUSTWORTHY_DATA				✓			✓												
P.ACCOUNTABILITY	✓																		
P.AUTHORISED_USERS			✓																
P.AUTOMATIC_SCAN				✓															
P.EXTERNAL							✓												
P.NEED_TO_KNOW			✓		✓	✓													
A.ACCESS								✓											
A.AUDIT_REVIEW											✓								
A.DEVELOPEMENT																			✓
A.INSTALL														✓	✓				
A.LOCATE																✓			
A.MANAGE										✓									
A.NO_EVIL_ADMIN										✓									
A.PROTECT																	✓		
A.SEC_OPERATION											✓		✓					✓	
A.SYOPS												✓	✓					✓	
A.USER_ID									✓										

Table 9. Security Objectives Rationale

Security Objective **O.AUDITING** directly counters Threats **T.ABUSE** and mitigates **T.IMPERSONATION** and **T.UNAUTHORIZED_USE** by recording all security relevant actions. In addition it directly enforces OSP **P.ACCOUNTABILITY**.

Security Objective **O.I&A** directly counters Threats **T.DATA_CORRUPTION**, **T.EQUIPMENT_THEFT** by controlling the access to the sensitive information stored in hardware, **T.IMPERSONATION**, **T.INFORMATION_THEFT**, and **T.UNAUTHORIZED_USE** by controlling the access to TOE and its resources.

Security Objective **O.DAC** by controlling the access to resources directly counters Threats **T.IMPERSONATION** and **T.DATA_CORRUPTION** and **T.UNAUTHORIZED_USE**. In addition it directly enforces OSP **P.AUTHORISED_USERS**, and OSP **P.NEED_TO_KNOW** by allowing authorized users to specify which users may access which resources.

Security Objective **O.VIRUS** directly counters Threat **T.UNTRUSTWORTHY_DATA** by checking the data received from external sources. In addition it directly enforces OSP **P.AUTOMATIC_SCAN** by forcing the checking of the removable media.

Security Objective **O.MANAGE** directly counters Threat and **T.DOS** by allowing administrator carry out security administration avoiding any overload. In addition it directly enforces OSP **P.NEED_TO_KNOW** by allowing the administrator to manage user security attributes.

Security Objective **O.RESIDUAL_INFO** directly enforces OSP **P.NEED_TO_KNOW** by erasing in a secure way all the sensitive data contained in a resource data which is going to be use by other users.

Security Objective **O.SECURITY_POLICY** directly counters Threats **T.DOS** by forcing users to use well-formed data and **T.UNTRUSTWORTHY_DATA**. In addition it directly enforces OSP **P.EXTERNAL** by restricting the sources which can exchange information.

Security Objective **O. E_ACCESS** directly upholds Assumptions **A.ACCESS**.

Security Objective **O.E_ACCOUNTABLE** directly upholds Assumption **A.USER_ID** by ensuring that individual user is assigned a unique user ID.

Security Objective **O.E_ADMIN** directly upholds Assumptions **A.MANAGE** and **A.NO_EVIL_ADMIN**.

Security Objective **O.E_AUDITDATA** directly upholds Assumptions **A.AUDIT_REVIEW** by ensuring quality logs to be inspected by the ISM and **A.SEC_OPERATION** by ensuring that procedures related to audit will exist.

Security Objective **O.E_CREDEN** directly upholds Assumption **A.SYOPS** by teaching users how to deal with their credentials.

Security Objective **O.E_EXTERNAL_SYS** directly counters Threat **T.INFORMATION_DISCLOSURE** by implanting procedures to check the classification of the information. In addition directly upholds Assumption **A.SYOPS** by teaching users checking classification of the information procedures.

Security Objective **O.E.HW&SW_INSTALL** directly upholds Assumption **A.INSTALL**.

Security Objective **O.E_INSTALL** directly upholds Assumption **A.INSTALL**.

Security Objective **O.E_LOCATE** directly upholds Assumptions **A.LOCATE**.

Security Objective **O.E_PROTECT** directly counters Threats **T.DOS** by avoiding software modifications, **T.EQUIPMENT_THEFT** and **T.INFORMATION_THEFT** by protecting the security policy enforcement hardware and software. In addition directly upholds Assumption **A.PROTECT**.

Security Objective **O.E_SECOP** directly upholds Assumptions **A.SEC_OPERATION** and **A.SYOPS**.

Security Objective **O.E_SW_LIFECYCLE** directly upholds Assumption **A.DEVELOPEMENT**.

5. EXTENDED COMPONENTS DEFINITION (APE_ECD)

In many cases the security requirements in a PP are based on components in [CC_Part2] or [CC_Part3]. However, in some cases, there may be requirements in a PP that are not based on components in [CC_Part2] or [CC_Part3]. In this case, new components (extended components) must be defined, and this definition should be done in the Extended Components Definition.

5.1 Extended Components Definition

Majority of the security requirements contained in this PP are based on the components in [CC_Part2] or [CC_Part3]. However, there are some security requirements which are applicable to the TOE, e.g. virus scanning, integrity checks based in the bespoke application, are not defined in CC. In this case extended components have been defined.

5.2 Anti-Virus (FAV)

Anti-virus FAV class helps to satisfy the security objectives related with the checking of the data that comes from the TOE external interfaces in order to protect it from the virus threats.

This class contains families specifying requirements related to antivirus checks of viruses and the Antivirus alerts that are produced with these checks.

This Common Criteria Extended Class is split into two groups of families (listed below):

- Anti-Virus Actions (FAV_ACT_EXP)
- Anti-Virus Alerts (FAV_ALR_EXP)

5.2.1 Anti-Virus Actions (FAV_ACT_EXP)

5.2.1.1 Family behaviour

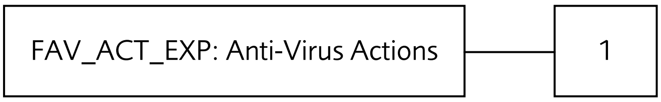
This family defines the actions that should be enforced when a virus is detected during the importation of data into system from external sources.

These external sources could be but not limited to CDROM devices, floppy devices, USB devices, Firewire devices and also data imported from the external network interfaces.

The different types of viruses that the TSF will detect are based on:

- The well-know definitions included in the virus signature file or,
- Suspicious chains that the powerful heuristic analysis tools could be reveal as virus.

5.2.1.2 Component levelling



FAV_ACT_EXP: Anti-Virus Actions

1

5.2.1.3 Management: FAV_ACT_EXP

NONE.

5.2.1.4 Audit: FAV_ACT_EXP

The following actions will be audited:

a. The detection of attempts of virus infections and the actions that the Anti-virus TSF take in order to stop the threat.

5.2.1.5 Anti-Virus Actions (FAV_ACT_EXP.1)

Hierarchical to: No other components.

Dependencies: No other components.

FAV_ACT_EXP.1.1: Upon detection based on known signatures of a memory based virus, the TSF shall prevent the virus from further execution.

FAV_ACT_EXP.1.2: Upon detection based on known signatures of a file-based virus, the TSF shall perform the action(s) specified by the authorised administrator. Actions are administratively configurable on a per-workstation basis and consist of:

a. Clean the virus from the file

b. Quarantine the file,

c. Delete the file,

d. No other actions.

e. [assignment: *other configurable actions*].

5.2.2 Anti-Virus Alerts (FAV_ALR_EXP)

5.2.2.1 Family behaviour

This family defines the alerts that will be used to inform the users when a virus is detected.

The TSF shows the following alerts:

- An alert on the screen of the workstations on which the virus is detected. The alert shall identify the virus that was detected and the action taken by the TOE and,

- continue to display the alerts on the screen of the workstation until they are acknowledged by the user of the workstation, or the user session ends.

5.2.2.2 Component leveling

FAV_ALR_EXP: Anti-Virus Alerts
1

5.2.2.3 Management: FAV_ALR_EXP

NONE.

5.2.2.4 Audit: FAV_ALR_EXP

The following actions will be audited:

a. The detection of attempts of virus infections and the actions that the Anti-virus TSF take in order to stop the threat.

5.2.2.5 Anti-Virus Alerts (FAV_ALR_EXP.1)

Hierarchical to: No other components.

Dependencies: No other components.

FAV_ALR_EXP.1.1: Upon detection of a virus, the TSF shall display an alert on the screen of the workstations on which the virus is detected. The alert shall identify the virus that was detected and the action taken by the TOE.

FAV_ALR_EXP.1.2: The TSF shall continue to display the alerts on the screen of the workstation until they are acknowledged by the user of the workstation, or the user session ends.

6. SECURITY REQUIREMENTS (APE_REQ)

The security requirements consist of two groups of requirements:

a) the security functional requirements (SFRs): a translation of the security objectives for the TOE into a standarised language.

b) the security assurance requirements (SARs): a description of how assurance is to be gained that the TOE meets the SFRs.

6.1 Security Functional Requirements

The following table states the Security Functional Requirements included in this Protection Profile.

Component	Name	Operations			
		A	S	R	I
FAU_GEN.1	Audit Data Generation		X		
FAU_GEN.2	User Identity Association				
FAU_SAR.1	Audit Review	X			
FAU_SAR.2	Restricted Audit Review				
FAU_SAR.3	Selectable Audit Review				
FAU_STG.1	Protected Audit Trail Storage		X		
FAU_STG.4	Prevention of Audit Data Loss	X	X		
FDP_ACC.1	Subset Access Control				
FDP_ACF.1	Security Attribute Based Access Control				
FDP_RIP.2	Full Residual Information Protection		X		
FIA_AFL.1	Authentication Failure Handling	X	X		
FIA_ATD.1	User Attribute Definition				
FIA_SOS.1	Verification of Secrets	X			
FIA_UAU.1	Timing of Authentication	X			
FIA_UAU.7	Protected authentication feedback	X			
FIA_UID.1	Timing of Identification	X			
FIA_USB.1	User-subject binding				
FMT_MOF.1	Management of security functions behaviour				
FMT_MSA.1	Management of Security Attributes				
FMT_MSA.2	Secure security attributes	X			
FMT_MSA.3	Static Attribute Initialisation				
FMT_MTD.1	Management of TSF Data				
FMT_MTD.2	Management of limits on TSF data	X			
FMT_SAE.1	Time-limited authorisation	X			
FMT_SMF.1	Specification of Management Functions				
FMT_SMR.1	Security Roles	X			
FMT_SMR.3	Assuming Roles	X			
FPT_STM.1	Reliable Time stamps				
FAV_ACT_EXP.1	Anti-Virus Actions				
FAV_ALR_EXP.1	Anti-Virus Alerts				

Table 10. Security Functional Requirements

6.1.1 Class FAU: Security audit

6.1.1.1 Security audit data generation (FAU_GEN)

6.1.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps.

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) All auditable events for the BASIC level of audit; and

c) [assignment: *other specifically defined auditable events*].

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 (if applicable), 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, [assignment: *other audit relevant information*].

6.1.1.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies:

- FAU_GEN.1 Audit data generation.
- FIA_UID.1 Timing of identification.

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.2 Security audit review (FAU_SAR)

6.1.1.2.1 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation.

FAU_SAR.1.1 The TSF shall provide AUTHORISED ADMINISTRATORS with the capability to read ALL AUDIT INFORMATION from the audit records.

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

6.1.1.2.2 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review.

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.2.3 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review.

FAU_SAR.3.1 The TSF shall provide the ability to apply [assignment: *methods of selection and/or ordering*] of audit data based on [assignment: *criteria with logical relations*].

6.1.1.3 Security audit event storage (FAU_STG)

6.1.1.3.1 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation.

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to PREVENT unauthorised modifications to the stored audit records in the audit trail.

6.1.1.3.2 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss.

Dependencies: FAU_STG.1 Protected audit trail storage.

FAU_STG.4.1 The TSF shall PREVENT AUDITED EVENTS, EXCEPT THOSE TAKEN BY THE AUTHORISED USER WITH SPECIAL RIGHTS and GENERATE AN ALARM TO THE AUTHORISED ADMINISTRATOR if the audit trail is full.

6.1.2 Class FDP: User data protection

6.1.2.1 Access control policy (FDP_ACC)

6.1.2.1.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control.

FDP_ACC.1.1 The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

6.1.2.2 Access control functions (FDP_ACF)

6.1.2.2.1 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control.
- FMT_MSA.3 Static attribute initialisation.

FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

6.1.2.3 Residual information protection (FDP_RIP)

6.1.2.3.1 FDP_RIP.2 Full residual information protection

Hierarchical to: FDP_RIP.1 Subset residual information protection.

Dependencies: No dependencies.

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the ALLOCATION OF THE RESOURCE TO all objects.

6.1.3 Class FIA: Identification and authentication

6.1.3.1 Authentication failures (FIA_AFL)

6.1.3.1.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_AFL.1.1 The TSF shall detect when AN ADMINISTRATOR CONFIGURABLE POSITIVE INTEGER WITHIN A RANGE OF VALUES ACCEPTABLE TO THE ADMINISTRATOR unsuccessful authentication attempts occur related to USER LOGON.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been SURPASSED, the TSF shall DISABLE THE USER ACCOUNT FOR AN AUTHORISED ADMINISTRATOR SPECIFIED DURATION.

6.1.3.2 User attribute definition (FIA_ATD)

6.1.3.2.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.1.3.3 Specification of secrets (FIA_SOS)

6.1.3.3.1 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet:

- **FOR EACH ATTEMPT TO USE THE AUTHENTICATION MECHANISM, THE PROBABILITY THAT A RANDOM ATTEMPT WILL SUCCEED IS LESS THAN ONE IN 2 X 1015;**
- **FOR MULTIPLE ATTEMPTS TO USE THE AUTHENTICATION MECHANISM DURING A ONE MINUTE PERIOD, THE PROBABILITY THAT A RANDOM ATTEMPT DURING THAT MINUTE WILL SUCCEED IS LESS THAN ONE IN 25 X 1012;**
- **ANY FEEDBACK GIVEN DURING AN ATTEMPT TO USE THE AUTHENTICATION MECHANISM WILL NOT REDUCE THE PROBABILITY BELOW THE ABOVE METRICS; AND**
- **THE AUTHENTICATION MECHANISM MUST PROVIDE A DELAY BETWEEN ATTEMPTS, SUCH THAT THERE CAN BE NO MORE THAN TEN ATTEMPTS PER MINUTE.**

6.1.3.4 User authentication (FIA_UAU)

6.1.3.4.1 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1 The TSF shall allow ACCESS TO THE AUTHENTICATION SERVER on behalf of the user to be performed before the user is authenticated.

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

6.1.3.4.2 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_UAU.7.1 The TSF shall provide only OSCURE FEEDBACK to the user while the authentication is in progress.

6.1.3.5 User identification (FIA_UID)

6.1.3.5.1 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow ACCESS TO THE AUTHENTICATION SERVER on behalf of the user to be performed before the user is identified.

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

6.1.3.6 User-subject binding (FIA_USB)

6.1.3.6.1 FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

6.1.4 Class FMT: Security management

6.1.4.1 Management of functions in TSF (FMT_MOF)

6.1.4.1.1 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies:

- FMT_SMR.1 Security roles.
- FMT_SMF.1 Specification of Management Functions.

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of*, *disable*, *enable*, *modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

6.1.4.2 Management of security attributes (FMT_MSA)

6.1.4.2.1 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control, **or** FDP_IFC.1 Subset information flow control.
- FMT_SMR.1 Security roles.
- FMT_SMF.1 Specification of Management Functions.

FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP(s)*, *information flow control SFP(s)*] to restrict the ability to [selection: *change_default*, *query*, *modify*, *delete*, *[assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

6.1.4.2.2 FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control, **or** FDP_IFC.1 Subset information flow control.
- FMT_MSA.1 Management of security attributes.
- FMT_SMR.1 Security roles.

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for PASSWORD SECURITY ATTRIBUTES.

6.1.4.2.3 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies:

- FMT_MSA.1 Management of security attributes.
- FMT_SMR.1 Security roles.

FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP*, *information flow control SFP*] to provide [selection, choose one of: *restrictive*, *permissive*, *[assignment: other property]*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.3 Management of TSF data (FMT_MTD)

6.1.4.3.1 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies:

- FMT_SMR.1 Security roles.
- FMT_SMF.1 Specification of Management Functions.

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default*, *query*, *modify*, *delete*, *clear*, *[assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

6.1.4.3.2 FMT_MTD.2 Management of limits on TSF data

Hierarchical to: No other components.

Dependencies:

- FMT_MTD.1 Management of TSF data.
- FMT_SMR.1 Security roles.

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for FOR THE UNSUCCESSFUL AUTHENTICATION ATTEMPTS THRESHOLD to AUTHORISED ADMINISTRATORS.

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: THE TSF SHALL DISABLE THE USER ACCOUNT FOR AN AUTHORISED ADMINISTRATOR SPECIFIED DURATION.

6.1.4.4 Security attribute expiration (FMT_SAE)

6.1.4.4.1 FMT_SAE.1 Time-limited authorisation

Hierarchical to: No other components.

Dependencies:

- FMT_SMR.1 Security roles.
- FPT_STM.1 Reliable time stamps.

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for AUTHENTICATION DATA to AUTHORISED ADMINISTRATORS.

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to LOCK OUT THE ASSOCIATED USER ACCOUNT after the expiration time for the indicated security attribute has passed.

6.1.4.5 Specification of Management Functions (FMT_SMF)

6.1.4.5.1 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

6.1.4.6 Security management roles (FMT_SMR)

6.1.4.6.1 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles:

a) AUTHORIZED ADMINISTRATOR;

b) USERS AUTHORIZED BY THE DISCRETIONARY ACCESS CONTROL POLICY TO MODIFY OBJECT SECURITY ATTRIBUTES;

c) USERS AUTHORIZED TO MODIFY THEIR OWN AUTHENTICATION DATA AND UNLOCK THE LOCAL USER SESSION; AND

d) OBJECT CREATOR - USERS THAT CREATE OBJECTS.

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

6.1.4.6.2 FMT_SMR.3 Assuming roles

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles.

FMT_SMR.3.1 The TSF shall require an explicit request to assume the following roles: ANY ROLE.

6.1.5 Class FPT: Protection of the TSF

6.1.5.1 Time stamps (FPT_STM)

6.1.5.1.1 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.1.6 Class FAV: Antivirus

6.1.6.1 Anti-Virus Actions (FAV_ACT_EXP)

6.1.6.1.1 FAV_ACT_EXP.1 Anti-Virus Actions

Hierarchical to: No other components.

Dependencies: No other components.

FAV_ACT_EXP.1.1: Upon detection based on known signatures of a memory based virus, the TSF shall prevent the virus from further execution.

FAV_ACT_EXP.1.2: Upon detection based on known signatures of a file-based virus, the TSF shall perform the action(s) specified by the authorised administrator. Actions are administratively configurable on a per-workstation basis and consist of:

a) Clean the virus from the file

b) Quarantine the file,

c) Delete the file,

d) No other actions.

e) [assignment: *other configurable actions*].

6.1.6.2 Anti-Virus Alerts (FAV_ALR_EXP)

6.1.6.2.1 FAV_ALR_EXP.1 Anti-Virus Alerts

Hierarchical to: No other components.

Dependencies: No other components.

FAV_ALR_EXP.1.1: Upon detection of a virus, the TSF shall display an alert on the screen of the workstations on which the virus is detected. The alert shall identify the virus that was detected and the action taken by the TOE.

FAV_ALR_EXP.1.2: The TSF shall continue to display the alerts on the screen of the workstation until they are acknowledged by the user of the workstation, or the user session ends.

6.2 Security Assurance Requirements

The evaluation assurance level of this protection profile is EAL-4. The following table states the Security Assurance Requirements included in the Evaluation Assurance Level 4.

Assurance Class	Assurance Component
ADV: Development	ADV_ARC.1 Security architecture description.
	ADV_FSP.4 Complete functional specification.
	ADV_IMP.1 Implementation representation of the TSF.
	ADV_TDS.3 Basic modular design.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance.
	AGD_PRE.1 Preparative procedures.
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation.
	ALC_CMS.4 Problem tracking CM coverage.
	ALC_DEL.1 Delivery procedures.
	ALC_DVS.1 Identification of security measures.
	ALC_LCD.1 Developer defined life-cycle model.
	ALC_TAT.1 Well-defined development tools.
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims.
	ASE_ECD.1 Extended components definition.
	ASE_INT.1 ST introduction.
	ASE_OBJ.2 Security objectives.
	ASE_REQ.2 Derived security requirements.
	ASE_SPD.1 Security problem definition.
	ASE_TSS.1 TOE summary specification.
ATE: Tests	ATE_COV.2 Analysis of coverage.
	ATE_DPT.1 Testing: basic design.
	ATE_FUN.1 Functional testing.
	ATE_IND.2 Independent testing – sample.
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Table 11. Security Functional Requirements

6.3 Security Requirements Rationale

This section states the Security Requirements (Security Functional Requirements and Security Assurance Requirements) Rationale.

6.3.1 Security Functional Requirements Rationale

The following table provides the correspondence mapping between IT Security Objectives for the TOE and the requirements that satisfy them.

Security Functional Requirements	Security Objectives for the TOE						
	O.AUDITING	O.I&A	O.DAC	O.VIRUS	O.MANAGE	O.RESIDUAL_INFO	O.SECURITY_POLICY
FAU_GEN.1	✓						
FAU_GEN.2	✓						
FAU_SAR.1	✓				✓		
FAU_SAR.2	✓				✓		
FAU_SAR.3	✓				✓		
FAU_STG.1	✓						
FAU_STG.4	✓				✓		
FDP_ACC.1			✓				✓
FDP_ACF.1			✓				✓
FDP_RIP.2						✓	
FIA_AFL.1		✓			✓		
FIA_ATD.1		✓	✓				
FIA_SOS.1		✓					
FIA_UAU.1		✓					
FIA_UAU.7		✓					
FIA_UID.1		✓					

Security Functional Requirements	Security Objectives for the TOE						
	O.AUDITING	O.I&A	O.DAC	O.VIRUS	O.MANAGE	O.RESIDUAL_INFO	O.SECURITY_POLICY
FIA_USB.1	✓		✓				
FMT_MOF.1	✓	✓			✓		
FMT_MSA.1			✓		✓		
FMT_MSA.2		✓			✓		
FMT_MSA.3			✓		✓		
FMT_MTD.1	✓	✓			✓	✓	
FMT_MTD.2	✓	✓			✓		
FMT_SAE.1					✓		
FMT_SMF.1					✓		
FMT_SMR.1					✓		
FMT_SMR.3					✓		
FPT_STM.1	✓						
FAV_ACT_EXP.1				✓			
FAV_ALR_EXP.1				✓			

Table 12. Security Functional Requirements

O.AUDITING

FAU_GEN.1, FAU_GEN.2, FIA_USB.1, FPT_STM.1, and FMT_MTD.1 define the events that must be auditable and ensures that each event shall identify the user that caused the event and the time the event occurred.

FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.4 FMT_MTD.1and FMT_MTD.2 ensure that the audit trail is complete and that audit events can be selected and reviewed by only the authorized administrator, and that the audit log (security log) can be managed appropriately by the authorized administrator.

FMT_MOF.1 ensures the authorized administrator can manage the audit function and the function to protect TSF data during transmission.

FPT_STM.1 provides a reliable Time Stamp for all the accounting events.

Each of the above requirements together ensure the generation of audit records, the adequacy of the content of audit records, and that the audit records are available to and managed by the authorized administrator.

O.I&A

FIA_ATD.1 and FMT_MTD.1 define data to be used for authentication per user and restrict the ability to initialize authentication data to only authorized administrator, and the ability to modify authentication to authorized administrators and authorized users.

FIA_UAU.1 and FIA_UAU.7 will ensure successful user authentication.

FIA_UID.1 require a user to be identified and authenticated before any other TSF-mediation action on their behalf, with the exception of the authentication server access, is allowed and prevent the user requesting access from receiving insightful authentication feedback during the authentication.

FMT_MSA.2 ensures that only secure values are accepted for password security attributes.

FIA_AFL.1, FMT_MTD.1 and FMT_MTD.2 allow the authorized administrator the ability to set thresholds on the amount of attempts to logon that can be made before a user is locked out and the duration the account locked out.

FIA_SOS.1 defines a metric the authentication mechanism must meet.

FMT_MOF.1 allows the authorized user to manage the security configuration attributes.

FMT_MTD.1 allows the authorized user to manage the security configuration attributes TSF data.

They allow the authorized administrator the ability to modify the minimum password length and set an expiration limit on authentication data that upon the expiration time the user is prevented from logging on.

These requirements together restrict access to the TOE by enforcing authentication and identification of users based on the user accounts including user attributes and limits defined by the authorized administrator

O.DAC

FDP_ACC.1 and FDP_ACF.1 define several discretionary Security Functional Policies (SFPs), each identifies the subjects and objects which the policy covers, the security attributes that access to objects is based upon, and the rules of access between subjects and objects. The discretionary SFPs allows for the control of access to resources based on the user identity.

FIA_ATD.1 and FIA_USB.1 define the security attributes associated with users that used to enforce the SFPs.

FMT_MSA.1 and FMT_MSA.3 restrict the ability to modify object security attributes to authorized users, ensures that the default values are known (permissive or restrictive) for the security attributes used to enforce the SFPs, and ensures that only authorized users can revoke the security attributes used to enforce the SFPs.

These requirements together allow the users the ability to specify, modify, and revoke how objects they are authorized to control can be shared; ensures that the system enforces the sharing specified; and that the security attributes of the users cannot be modified by other than the authorized administrator.

Each of the above requirements together ensure that access is controlled to resources based on user identity and allow authorized users to specify which resources may be accessed by which users

O.VIRUS

This objective is covered by requirements which ensure that the TOE takes action against viruses once they are detected and which ensure that the user is made aware that a virus was detected FAV_ACT_EXP.1 and FAV_ALR_EXP.1.

O.MANAGE

FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.4 and FMT_MTD.1 ensure the authorized administrator can manage audit records.

FMT_MSA.1, FMT_MSA.3 and FMT_MTD.1 ensure the authorized administrator can manage attributes used to enforce the SFPs.

FMT_MSA.2 ensures that only secure values are accepted for password security attributes.

FIA_AFL.1, FMT_MTD.1, FMT_MTD.2, FMT_MOF.1 and FMT_SAE.1 ensure the authorized administrator can manage authentication related data.

FMT_MTD.1 restricts the ability to modify TSF data (including the password complexity requirements).

FMT_MTD.1 prevents all users (including the authorized administrator) from reading passwords.

FMT_SMR.1 and FMT_SMR.3 ensure the role of the authorized administrator is enforced.

FMT_SMF.1 ensures the authorized administrator is provided the capability to change and maintain security relevant data (e.g. audit policy, account policy, etc).

FMT_MOF.1 ensures the authorized administrator can manage the audit function and the function to protect TSF data during transmission.

FMT_MOF.1 ensures the authorized administrator can manage the group policy calculation functions.

Together the above requirements ensure that the administrator can manage data (audit records, attributes used to enforce the SFPs), manage functions, and ensure that the authorized user and administrator roles are enforced.

Each of the above requirements contributes to and together ensures that the authorized administrator can manage the TOE securely

O.RESIDUAL_INFO

This objective is covered by requirements which ensure that any previous information content of a resource is made unavailable FDP_RIP.2 and by requirements which ensure that only authorised users to manage TSF data FMT_MTD.1.

O.SECURITY_POLICY

This objective is covered by requirements which ensure that information exchanged with sources is limited to that defined by the security policies FDP_ACC.1 and FDP_ACF.1.

6.3.2 Security Assurance Requirements Rationale

The Security Assurance Requirements have been chosen due to they are included in the **Evaluation Assurance Level 4**.