CASSIDIAN
AN EADS COMPANY

DOCUMENTO TECNICO
TECHNICAL DOCUMENT

Documento nº/Document no.	Avión/Aircraft
DT-T-MEP24-10002	General

Título/Title

EADS AIR SEGMENT SYSTEMS PROTECTION PROFILE

Realizado/Prepared	**Firma/Signature**	
	Nombre/Name	Sergio Torralba Urrutia
	Cargo/Position	Information Security Engineer
Comprobado/Checked	**Firma/Signature**	
	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	December 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	See cover	See cover	See cover
December 2010	Initial Release	See cover	See cover	See cover
Issue B	EAL modification INTA Comments. Title Doc.: EADS Air Segment Systems Protection Profile Observations Report. Doc.: PPA-COM-2035-001-INTA	Sergio Torralba Urrutia	Montserrat Herrera Esparrach	Miguel Ángel Gil Jiménez
February 2011	All the document			

TABLE OF CONTENTS

Título/Title **Página/Page**

LIST OF TABLES

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.
EAL	Evaluation Assurance Level.
ISM	Installation Security Manager.
MOB	Main Operating Base.
OSP	Organisational Security Policy.
PP	Protection Profile.
RDBMS	Relational Database Management System.
RTOS	Real Time Operating System.

Term	Description
SFR	Security Functional Requirement.
ST	Security Target.
SyOPs	Security Operating Procedures.
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 Air Segment Systems Protection Profile.

Version: Issue B.

Common Criteria Version: 3.1 Release 3 Final.

Author: EADS-CASA. Cassidian Division. Cassidian Air Systems Business Unit.

Publication Date: 28-02-2011

1.2 TOE Type

This TOE reference to a military-purpose Air Segment Systems which allows to fly the aircraft, to manage the mission data and to use data links.

1.3 TOE Overview

Air Segment Systems are these systems used by the aircraft crew or by the aircraft computers and sensors to store, record or manage information during mission.

Air Segment Systems are systems located in the aircraft and are used on-flight and on-ground.

The typical Air Mission Systems functionality is functionality related to:

- general purpose, which includes such hydraulic system; fuel system; etc.(excluded of the security problem).
- management, which includes flight control and management functions; navigation systems; etc.
- mission, which includes mission monitoring and control; payload management; data recorders; etc.
- communication, which includes dialog with traffic air control; interconnection with other allied aircrafts; etc.

Depending on the type of aircraft the TOE will need other software, in example, if the aircraft is a manned aircraft, the TOE could require operating systems as Microsoft Windows or Linux; or RDBMS as Microsoft SQL Server or Oracle. However if the aircraft is an unmanned aircraft it will require a RTOS.

These systems shall implement security functions to protect the sensitive information from unauthorized disclosure based on cryptography, identification and authentication, access control or secure erase, as well as an integrity control of the information.

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] conformant.
- 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) 3.

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 Air 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.

Threats are stated below:

Threat	Definition
T.CAPTURE	**Hostile forces** capture the equipment while combat, transport or accessing premises and **steal information**.
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.EAVESDROPPING	**Someone inside or outside the organisation** connects a sniffer device to the network to **store and analyse** transmitted **information**.
T.INFORMATION_THEFT	**Someone inside or outside the organisation** accessing digital media with the intention of **stealing** and using the **information** on them.
T.REMANANCE	**An attacker recovers information** from removed electronic media.
T.TELECOM_FAILURE	**An attacker**, through sabotage or disturbance of the telecom installation, **gains access** to the **telecommunications equipment**.
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** 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 in the following table:

Organizational Security Policy	Definition
P.ACCOUNTABILITY	The users of the TOE shall be held accountable for their actions within the TOE.

Organizational Security Policy	Definition
P.AUTHORISED_USERS	Only those users who have been authorised access to information within the system may access the TOE.
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.CLEARANCE	All persons requiring access to the Aircraft TOE which manage sensitive data shall have a clearance that dominates the protecting marking of that data, prior to any authorised access.
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.CRYPTO_MANAGE	Information marked as 'CRYPTO' shall always be handled and stored in accordance with its Protective Marking and Caveat.
A.INSTALL	All software or hardware installed in the Aircraft TOE equipment shall be subjected to rigorous configuration management procedures, stringent quality control and comprehensive testing.
A.PHYSICAL_ACCESS	In controlled areas and/or scenarios all personnel accessing the Aircraft where the TOE is located shall be reliably identified before access is granted.
A.TAMPER_SEALS	Tamper seals shall be fitted to Aircraft TOE equipment dependent on the design and as deemed necessary by the Security Accreditation Authority.
A.SYOPS	All users will be trained in accordance with their duties and will read, understand, and obey all the relevant Security Operating Procedures.
A.USER_CONFIDENCE	Privileged users shall be trusted not to abuse their privilege.

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 generate, record and present the security relevant actions in the TOE.
O.DAC	The TOE must control access to information and resources.
O.ENCRYPTION	The TOE must encrypt all appropriate equipments which stores and processes sensitive data.
O.I&A	The TOE must ensure that only authenticated users gain access to the TOE and its resources.
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 (i.e.: access to audit data).
O.SECURE_TRANSFER	The TOE must ensure data confidentiality and integrity in transmissions.
O.ZEROISE	The TOE must have the capability to null, zeroise or purge all data and information Protectively Marked above from the appropriate Aircraft systems which stores such data in the Non-Volatile memory.

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_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.

Security Objectives	Definition
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_AWARE	The personnel must be made accountable and informed of possible sanctions. The personnel must be made aware of the obligation of professional secrecy and discretion. The system user shall be informed about the accounting of their activities in the system.
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	While not flying or being transported, 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_NO_KEYS_LEAK	To avoid sensitive data compromise the crypto keys must be correctly managed.
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.
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).

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.ENCRYPTION	O.MANAGE	O.SECURE_TRANSFER	O.ZEROISE	O.E_ADMIN	O.E_AUDITDATA	O.E_AWARE	O.E_INSTALL	O.E_LOCATE	O.E_NO_KEYS_LEAK	O.E_PROTECT	O.E_SECOP
T.CAPTURE		✓		✓	✓		✓					✓			
T.DATA_CORRUPTION		✓	✓		✓										
T. EAVESDROPPING						✓						✓			
T.INFORMATION_THEFT	✓	✓	✓		✓									✓	
T. REMANANCE				✓			✓								
T.TELECOM_FAILURE						✓									
T.UNAUTHORIZED_USE	✓	✓	✓		✓										
T.UNTRUSTWORTHY_DATA						✓									
P.ACCOUNTABILITY	✓	✓			✓										
P.AUTHORISED_USERS		✓	✓		✓										
P.NEED_TO_KNOW			✓	✓	✓		✓								
A.CLEARENCE								✓		✓			✓		
A.AUDIT_REVIEW									✓						
A.CRYPTO_MANAGE										✓					
A.INSTALL											✓		✓		
A.PHYSICAL_ACCESS												✓			
A.TAMPER_SEALS											✓			✓	
A.SYOPS										✓					✓
A.USER_CONFIDENCE								✓							

Table 9. Security Objectives Rationale

Security Objective **O.AUDITING** directly counters threats **T.INFORMATION_THEFT** and mitigates **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.CAPTURE** and **T.DATA_CORRUPTION** by controlling the access to the sensitive information; **T.INFORMATION_THEFT**, and **T.UNAUTHORIZED_USE** by controlling that only authenticated users access to TOE and its resources. In addition it directly enforces OSPS **P.ACCOUNTABILITY** AND **P.AUTHORISED_USERS** by authenticating users.

Security Objective **O.DAC** by controlling the access to resources directly counters threats **T. INFORMATION_THEFT, 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.ENCRYPTION** directly counters threats **T.CAPTURE** and **T.REMANANCE** by the encryption of sensitive data and directly enforces OSP **P.NEED_TO_KNOW** by encrypting with non-commonly-known keys all the sensitive data contained in a resource data.

Security Objective **O.MANAGE** directly counters threats **T.CAPTURE**, **T.DATA_CORRUPTION**, **T.INFORMATION_THEFT** and **T.UNAUTHORIZED_USE** by allowing administrator carry out security administration to protect the TOE. In addition it directly enforces OSPs **P.ACCOUNTABILITY**, **P.AUTHORISED_USERS** and **P.NEED_TO_KNOW** by allowing the administrator to manage user security attributes.

Security Objective **O.SECURE_TRANSFER** directly counters threat **T.EAVESDROPPING**, **T.TELECOM_FAILURE** and **T.UNTRUSTWORTHY_DATA** by assuring data confidentiality and integrity.

Security Objective **O.ZEROISE** directly counters threats **T.CAPTURE** and **T.REMANANCE** by the allowing a secure erase of sensitive data and 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.E_ADMIN** directly upholds assumptions **A.CLEARANCE** and **A.USER_CONFIDENCE.**

Security Objective **O.E_AUDITDATA** directly upholds assumption **A.AUDIT_REVIEW** by ensuring quality logs to be inspected.

Security Objective **O.E_AWARE** directly upholds assumptions **A.CLEARANCE**, **A.CRYPTO_MANAGE** and **A.SYOPS** by teaching users.

Security Objective **O.E_INSTALL** directly upholds assumptions **A.INSTALL** and **A.TAMPER_SEALS**.

Security Objective **O.E_LOCATE** mitigates threats **T.CAPTURE** and **T.EVESDROPPING** by assuring that during on ground it will be located in a in a controlled access facilities. Security Objective **O.E_NO_KEYS_LEAK** directly upholds assumptions **A.CLEARANCE** and **A.INSTALL**.

Security Objective **O.E_PROTECT** directly counters threat **T.INFORMATION_THEFT** by protecting the security policy enforcement hardware and software. In addition directly upholds assumption **A.TAMPER_SEALS**.

Security Objective **O.E_SECOP** directly upholds assumption **A.SYOPS**.

5. 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.

5.1 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_SAR.1	Audit Review	X			
FAU_SAR.2	Restricted audit review				
FCS_CKM.4	Cryptographic key destruction				
FCS_COP.1	Cryptographic operation	X			
FDP_ACC.1	Subset access control				
FDP_ACF.1	Security attribute based access control				
FDP_IFC.1	Subset information flow control				
FDP_IFF.1	Simple security attributes				
FDP_ITC.1	Import of user data without security attributes				
FDP_RIP.1	Subset residual information protection	X		X	
FDP_UCT.1	Basic data exchange confidentiality	X			X
FDP_UIT.1	Data exchange integrity	X			X
FIA_UAU.1	Timing of Authentication	X			
FIA_UAU.7	Protected authentication feedback	X			
FIA_UID.1	Timing of Identification	X			
FMT_MSA.1	Management of security attributes				
FMT_MSA.3	Static Attribute Initialisation				
FMT_SMF.1	Specification of Management Functions				
FMT_SMR.1	Security roles				
FPT_STM.1	Reliable Time stamps				

Table 10. Security Functional Requirements

5.1.1 Class FAU: Security audit

5.1.1.1 Security audit data generation (FAU_GEN)

5.1.1.1.1 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*].

5.1.1.2 Security audit review (FAU_SAR)

5.1.1.2.1 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.

5.1.1.2.2 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.

5.1.2 Class FCS: Cryptographic support

5.1.2.1 Access control policy (FCS_CKM)

5.1.2.1.1 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: FDP_ITC.1 Import of user data without security attributes, **or** FDP_ITC.2 Import of user data with security attributes, **or** FCS_CKM.1 Cryptographic key generation.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

5.1.2.2 Cryptographic operation (FCS_COP)

5.1.2.2.1 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies:

- FDP_ITC.1 Import of user data without security attributes, **or** FDP_ITC.2 Import of user data with security attributes, **or** FCS_CKM.1 Cryptographic key generation.
- FCS_CKM.4 Cryptographic key destruction.

FCS_COP.1.1 The TSF shall perform DATA ENCRYPTION in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

5.1.3 Class FDP: User data protection

5.1.3.1 Access control policy (FDP_ACC)

5.1.3.1.1 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*].

5.1.3.2 Access control functions (FDP_ACF)

5.1.3.2.1 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*].

5.1.3.3 Information flow control policy (FDP_IFC)

5.1.3.3.1 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes.

FDP_IFC.1.1 The TSF shall enforce the [assignment*: information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].

5.1.3.4 Information flow control functions (FDP_IFF)

5.1.3.4.1 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies:

- FDP_IFC.1 Subset information flow control.
- FMT_MSA.3 Static attribute initialisation.

FDP_IFF.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].

FDP_IFF.1.3 The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorise information flows*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].

5.1.3.5 Import from outside of the TOE (FDP_ITC)

5.1.3.5.1 FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control, **or** FDP_IFC.1 Subset information flow control.

- FMT_MSA.3 Static attribute initialisation.

FDP_ITC.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment*: additional importation control rules*].

5.1.3.6 Residual information protection (FDP_RIP)

5.1.3.6.1 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable BY ZEROISING upon the ALLOCATION OF THE RESOURCE to the following objects: [assignment: list of objects].

5.1.3.7 Inter-TSF user data confidentiality transfer protection (FDP_UCT)

5.1.3.7.1 FDP_UCT.1(a) Basic data exchange confidentiality (Transmit)

Hierarchical to: No other components.

Dependencies:

- FTP_ITC.1 Inter-TSF trusted channel, **or** FTP_TRP.1 Trusted path.
- FDP_ACC.1 Subset access control, **or** FDP_IFC.1 Subset information flow control.

FDP_UCT.1.1(a) The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to TRANSMIT user data in a manner protected from unauthorised disclosure.

5.1.3.7.2 FDP_UCT.1(b) Basic data exchange confidentiality (Receive)

Hierarchical to: No other components.

Dependencies:

- FTP_ITC.1 Inter-TSF trusted channel, **or** FTP_TRP.1 Trusted path.
- FDP_ACC.1 Subset access control, **or** FDP_IFC.1 Subset information flow control.

FDP_UCT.1.1(b) The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to RECEIVE user data in a manner protected from unauthorised disclosure.

5.1.3.8 Inter-TSF user data integrity transfer protection (FDP_UIT)

5.1.3.8.1 FDP_UIT.1(a) Data exchange integrity (Transmit)

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control, **or** FDP_IFC.1 Subset information flow control.
- FTP_ITC.1 Inter-TSF trusted channel, **or** FTP_TRP.1 Trusted path.

FDP_UIT.1.1(a) The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to TRANSMIT user data in a manner protected from [selection: *modification*, *deletion*, *insertion*, *replay*] errors.

FDP_UIT.1.2(a) The TSF shall be able to determine on receipt of user data, whether [selection: *modification*, *deletion*, *insertion*, *replay*] has occurred.

5.1.3.8.2 FDP_UIT.1(b) Data exchange integrity (Receive)

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control, **or** FDP_IFC.1 Subset information flow control.
- FTP_ITC.1 Inter-TSF trusted channel, **or** FTP_TRP.1 Trusted path.

FDP_UIT.1.1(b) The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to RECEIVE user data in a manner protected from [selection: *modification*, *deletion*, *insertion*, *replay*] errors.

FDP_UIT.1.2(b) The TSF shall be able to determine on receipt of user data, whether [selection: *modification*, *deletion*, *insertion*, *replay*] has occurred.

5.1.4 Class FIA: Identification and authentication

5.1.4.1 User authentication (FIA_UAU)

5.1.4.1.1 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 USER IDENTIFICATION 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.

5.1.4.1.2 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.

5.1.4.2 User identification (FIA_UID)

5.1.4.2.1 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.

5.1.5 Class FMT: Security management

5.1.5.1 Management of security attributes (FMT_MSA)

5.1.5.1.1 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*].

5.1.5.1.2 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.

5.1.5.2 Specification of Management Functions (FMT_SMF)

5.1.5.2.1 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*].

5.1.5.3 Security management roles (FMT_SMR)

5.1.5.3.1 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 [assignment: *the authorised identified roles*].
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.6 Class FPT: Protection of the TSF

5.1.6.1 Time stamps (FPT_STM)

5.1.6.1.1 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.

5.2 Security Assurance Requirements

The evaluation assurance level of this protection profile is EAL-3. The following table states the Security Assurance Requirements included in the Evaluation Assurance Level 3.

Assurance Class	Assurance Component
ADV: Development	ADV_ARC.1 Security architecture description.
	ADV_FSP.3 Functional specification with complete summary.
	ADV_TDS.2 Architectural design.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance.
	AGD_PRE.1 Preparative procedures.
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls.
	ALC_CMS.3 Implementation representation CM coverage.
	ALC_DEL.1 Delivery procedures.
	ALC_DVS.1 Identification of security measures.
	ALC_LCD.1 Developer defined life-cycle model.
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.2 Vulnerability analysis.

Table 11. Security Functional Requirements

5.3 Security Requirements Rationale

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

5.3.1 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.ENCRYPTION	O.MANAGE	O.SECURE_TRANSFER	O.ZEORISE
FAU_GEN.1	✔						
FAU_SAR.1	✔				✔		
FAU_SAR.2	✔				✔		
FCS_CKM.4				✔			
FCS_COP.1				✔			
FDP_ACC.1			✔				
FDP_ACF.1			✔				
FDP_IFC.1						✔	
FDP_IFF.1						✔	
FDP_ITC.1				✔			
FDP_RIP.1							✔
FDP_UCT.1(a)						✔	
FDP_UCT.1(b)						✔	
FDP_UIT.1(a)						✔	
FDP_UIT.1(b)						✔	
FIA_UAU.1		✔					
FIA_UAU.7		✔					
FIA_UID.1		✔					
FMT_MSA.1			✔		✔		

Security Functional Requirements	Security Objectives for the TOE						
	O.AUDITING	O.I&A	O.DAC	O.ENCRYPTION	O.MANAGE	O.SECURE_TRANSFER	O.ZEORISE
FMT_MSA.3			✔		✔		
FMT_SMF.1					✔		
FMT_SMR.1					✔		
FPT_STM.1	✔						

Table 12. Security Functional Requirements

O.AUDITING

FAU_GEN.1 and FPT_STM.1 define the events that must be auditable and the time the event occurred.

FAU_SAR.1 and FAU_SAR.2 ensure that the audit trail could be read and that audit events can reviewed by only the authorized users.

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_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.

These requirements restrict access to the TOE by enforcing authentication and identification of users.

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.

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.

Each of the above requirements ensures that access is controlled to resources allow authorized users to specify which resources may be accessed by which users

O.ENCRYPTION

FCS_COP.1 allows the cryptographic operation of encrypt the sensitive data.

FDP_ITC.1 allows the import of the cryptographic key and FCS_CKM.1 requires the cryptographic key destruction.

These requirements allow to encrypt sensitive data and manage the cryptographic key.

O.MANAGE

FAU_SAR.1 and FAU_SAR.2 ensure the authorized administrator can access audit records.

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

FMT_SMR.1 ensures the role of the authorized administrator is enforced.

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

Each of the above requirements contributes to ensure that the authorized administrator can manage the TOE securely

O.SECURE_TRANSFER

FDP_IFC.1 and FDP_IFF.1 control the information flow.

FDP_UCT.1(a), FDP_UCT.1(b) FDP_UIT.1(a) and FDP_UIT.1(b) control the confidentiality and the integrity respectively.

These requirements ensure data transmission confidentially and integrity.

O.ZEROISE

This objective is covered by requirements which ensure that any previous sensitive information content of a resource is made unavailable FDP_RIP.1 by zeorising.

5.3.2 Security Assurance Requirements Rationale

The Security Assurance Requirements have been chosen due to they are included in the **Evaluation Assurance Level 3**.