Security Target

XFER Service V 2.0

Authors:	**Ove Hølland, Teleplan** **Remi J Hauge, Secode**
Created:	**13.02.2004**
Updated:	**30.06.2008 12:38**
Version:	**1.7**

Foreword

This Security Target (ST) has been written in order to achieve an EAL 4 certification of the File Transfer Service (XFER Service) which is used to transfer files between two different partitions on a transfer server.

Comments to this ST can be addressed to:

Norwegian Defence Communication and Information Services Division
Postmottak
2617 Lillehammer

Telephone: +47 03003
Telefax: +47 67 86 23 09
E-mail: forsvaret@mil.no

Date	Version	Changes	Author
17.10.05	1.0	New document	Ove Hølland, Teleplan Remi J Hauge, Norconsult
27.01.06	1.1	Updated according to EOR 1-1, 1-2, 1-3, 1-4 and 1-5	Ove Hølland, Teleplan Remi J. Hauge, Norconsult
16.02.06	1.2	FMT_SMR.1 is deleted from the TOE functional requirements. Header description in Table 7 and 15 is changed. Updated references in table 8.	Ove Hølland, Teleplan Remi J. Hauge, Norconsult
23.05.06	1.3	Uppdated according to EOR 1-6, 1-7, 1-8, 1-10 and 4-5.	Ove Hølland, Teleplan Remi J. Hauge, Norconsult
25.09.06	1.4	Modified A.Certified_FW and A.Certified_OS Added FPT_RCV.1. Changed requirement text in FPT_FLS.1 Removed reference to SAT Updated according to EOR 1-11 Changed requirement text in FMT_MTD.1 according to EOR 4-9	Ove Hølland, Teleplan Remi J. Hauge, Norconsult
21.12.06	1.5	Changes made according to EOR 1-11 and EOR 7-7	Ove Hølland, Teleplan Remi J. Hauge, Norconsult
03.07.07	1.6	Declassified the document Deleted ref [18] DAT Report	Ove Hølland, Teleplan Remi J. Hauge, Secode
30.06.08	1.7	Updated TOE version	Ove Hølland, Teleplan

Table of Contents

List of Tables

List of Figures

Terminology

Administrators	Microsoft's definition: Built-in user group for administering the computer/domain
Enterprise Domain Controllers	Microsoft's definition: A computer group that includes all domain controllers in a forest that uses an Active Directory service
Event log	Microsoft Event log
Flow control policy	A policy set by the system owner in accordance with the security authority, deciding • Legal file types (extensions) to transfer • Legal classification labels
Partitioned mode of operation	A data system consisting of two System High partitions with different classification levels. A user is cleared and authorized for at least one level but not necessarily cleared or authorized for both.
Server administrator	Common definition for all administrators for the TOE environment: • Administrators • Enterprise Domain Controllers
System Administrator	Common definition for all administrators for the TOE: • XFER Service Admins • XFER Service Auditors • XFER High Operators • XFER Low Operators • XFER Service Enterprise Admins

User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
XFER HIGH Operators	The (high partition) users having access to administer (add/remove) members of the XFER HIGH to LOW Source Users and XFER LOW to HIGH Target Users groups.
XFER LOW Operators	The (low partition) users having access to administer (add/remove) members of the XFER LOW to HIGH Source Users and XFER HIGH to LOW Target Users.
XFER Service Admins	The users responsible for administering the XFER Server.
XFER Service Auditors	The users responsible for review and backing up the XFER servers Content Archive, Event log and Schedlgu.txt.
XFER Service Enterprise Admins	Distribute approved filtering rules and security label configuration of the TOE.
XFER Service	The product that comprises the TOE: ■ The two processes in the file transfer mechanism (referred to as the XFER services). ■ The scripts for creating and deleting user transfer areas ■ Scripts for verifying the configuration of the TOE environment
XFER services	The two processes in the file transfer mechanism (note the difference between the XFER Service and the XFER services).

Table 1 Terminology

Document Organisation

Chapter 1 – Introduction – provides the introductory material for the ST.

Chapter 2 – TOE Description – provides general purpose, TOE description and defines the physical and logical boundaries of the TOE.

Chapter 3 – TOE Security Environment – provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware or software or through the environmental controls. The threats are prefixed as follows:

- TA –Threat Agent
- TE – Threats to the Environment
- TT – Threat to the TOE

Chapter 4 – Security Objectives – defines the security objectives for both the TOE and the TOE environment. The security objectives reflects the stated intent, counters all identified threats and covers all identified organisational security policies and assumptions.

The objectives are prefixed as follows:

- O – Objective for the TOE
- OE – Objective for the TOE environment

Chapter 5 – IT Security Requirements – contains functional and assurance requirements derived from the Common Criteria, Part 2 [2] and 3 [3], respectively, which must be satisfied by the TOE. The text is conformant with CC Part 2 [2]. The underlined text is the chosen parameters, derived from I-02 [26].

Chapter 6 – TOE Summary Specification – demonstrates how each of the functional requirements is implemented in the TOE and it's environment referring to the documents where the implementation is described. This chapter also states how the assurance requirements are covered by referring to the documentation.

Chapter 7 – Protection Profile Claim – states that there are no PP claims.

Chapter 8 - Rationale – provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the assumptions, policies and threats. Arguments are provided for the coverage of each assumption, policy and threat. The chapter then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next Chapter 8 provides a set of arguments that address dependency analysis, and the internal consistency and mutual supportiveness of the ST requirements. It concludes with demonstrating how the TOE security functions satisfy the security function requirements.

Chapter 9 – A reference section is provided to identify background material.

Appendix A – Acronym list to define frequently used acronyms.

1 Introduction

1.1 Identification

ST Title:	XFER Service Security Target
CC Version:	2.3
TOE name:	XFER service
TOE version:	2.0.1

1.2 Security Target Overview

This ST describes the IT security requirements for the proposed file transfer mechanism for partitioned mode of operation. The cross-partition file transfer service (XFER Service) shall perform and control file exchange between associated end-user accounts in high and low partitions.

1.3 CC Conformance Claim

The XFER Service Security Target has been developed using the Common Criteria (CC) Version 2.3 (Evaluation Criteria for Information Technology Security; Part 1: Introduction and general model [1], Part 2: Security functional requirements [2], and Part 3: Security assurance requirements [3]).

The XFER Service Security Target is Part 2 conformant and Part 3 conformant.

2 TOE Description

2.1 Overview of the file transfer mechanism

The TOE is a software system to transfer files between partitions that have different classifications. Specifically, the system shall be used to transfer files between two partitions with different classifications. These files will contain information which not all users on both partitions of the system are cleared and authorised for, and will hence be marked with the actual classification level. Only files with classification level releasable to the target domain can be transferred.

The design and security requirements are based on I-02 [26].

In the following text, the **low partition** denotes a partition with a lower classification than the **high partition**.

The mechanism is based on EAL 4 certified MS Windows 2003, and as much functionality as possible is implemented by standard Windows 2003 Server security functions, to make the functionality of the TOE as small as possible. The two transfer areas are installed on two different servers, one in each partition, separated by an EAL 4 certified firewall. The transfer service is installed on a third server, separated from the two partitions with the same firewall. This server contains the XFER domain, the transfer areas, the Event log, Schedlgu.txt and the content archive. All transferred files between the high and low partition will go through this server. The firewall, Schedlgu.txt and Event log is part of the TOE environment.

A typical usage scenario of TOE and TOE environment is depicted in Figure 1.

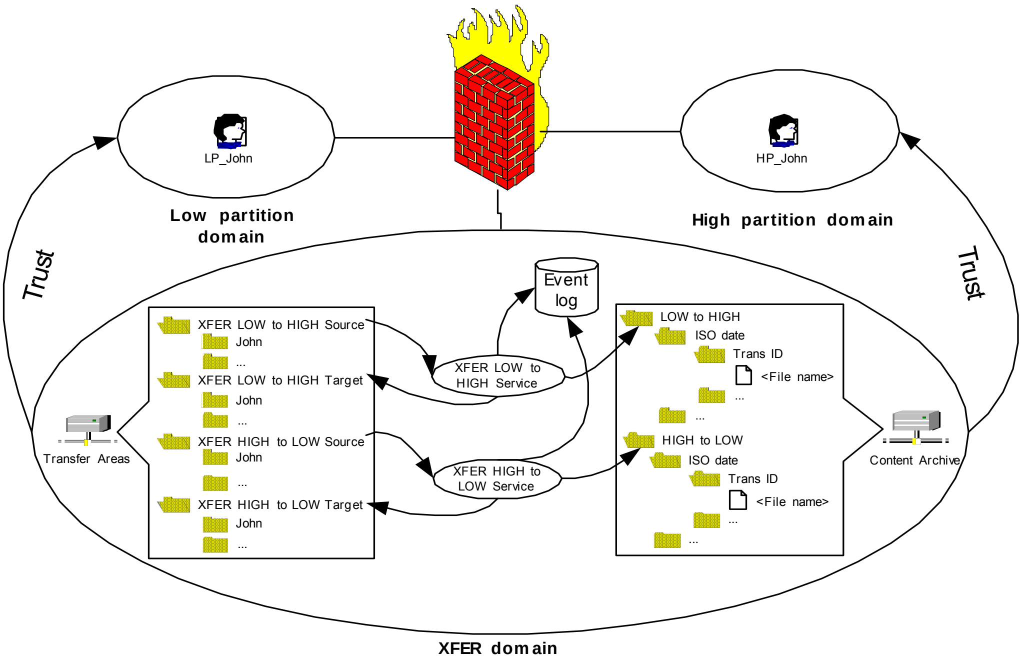

Figure 1 An overview of the TOE and TOE environment

The figure shows three different domains; low partition, high partition and the XFER domain that contains the transfer service. A user (John) has one user account in the high partition and one user account in the low partition (HP_John and LP_John, respectively). The transfer service enables John to transfer data from the low to the high partition, and vice versa. In the low partition, LP_John has access to the **John** directory on the following shares:

- **XFER LOW to HIGH Source**. To transfer a file to the high partition, LP_John has to put the file(s) in the **John** subdirectory of this share.

- **XFER HIGH to LOW Target**. The **John** subdirectory in this share contains the file(s) transferred from the high partition to the low partition.

    - Correspondingly, HP_John has access to the **John** directory on the following shares:

- **XFER HIGH to LOW Source**. To transfer a file to the low partition, HP_John has to put the file(s) in the **John** subdirectory of this share.

- **XFER LOW to HIGH Target**. The **John** subdirectory in this share contains the file(s) transferred from the low partition to the high partition.

A similar directory structure exists for all users that have access to transfer files between the partitions. The criterion for having access to the shares is that the user must be defined with one account in each partition (low and high).

All transfers are always logged to the system Event log. The figure also shows the Content Archive share, which contains a copy of the data transferred (optional for data from the low to the high partition, mandatory for data from the high partition to the low partition). The files are saved in a directory structure with direction (LOW to HIGH or HIGH to LOW), date, Transaction ID (generated and saved in the corresponding Event log item) and the file that has been moved.

To implement the functionality described here, the TOE consists of the following main parts:

- **The file transfer mechanism**. This is the “XFER HIGH to LOW Service” and “XFER LOW to HIGH Service” processes shown in the figure.

- Scripts for creating and deleting user transfer areas.

- Scripts for verifying the configuration of users, groups and ACLs.

2.2 The file transfer mechanism

The file transfer mechanism is the two processes that do the actual file transfer. Both processes have the same functionality, and will be the same program, but with different start-up options.

The “XFER LOW to HIGH Service” process will watch for changes in the XFER LOW to HIGH Source directory and subdirectories to find files to transfer to the high partition. When a file is found, the process will proceed through the following steps. (For each step in the list, the following rules apply; if the step is successful, continue to the next step. If a step in the main flow is not successful, the service will undo this step and all steps above this step (except step 5 and 7, if these steps have been performed) and log the error.)

1) **Lock the file**. The service will open the file with the write flag set, to prevent other processes or users to lock the file.

2) **Check the file location**. Check if the file is in a valid location for transfer:

3) **Check the file type**. Check if the file type is valid for transfer according to filtering rules.

4) **Check the file classification**. Check if the file classification is valid for transfer according to Flow control policy.

5) **Generate a Transaction ID**. The transaction ID is a 32-bit number that is incremented for every file transfer. The number must be persistent between every file transfer and between each stop and start of the XFER Service.

6) **(Optional) Make a copy of the file transferred**. If the Log flag value is true, the file must be copied to a new subdirectory below the **ArchiveDir** directory as described in reference. All parts of the file will be copied (security attributes, file attributes, all alternate data streams).

7) **Remove any streams from the file**. All streams will be removed from the file. The contents of the :Marking and :OriginalOwner streams will be saved for logging.

8) **Move the file**. The file will be moved to the corresponding subdirectory in the XFER LOW to HIGH Target directory. Only data, filename, owner and attributes will be moved, security attributes will not be moved and the default security attributes for <TargetDir> will be used.

9) **Write to the event log**. Write information about the transfer, including the Transaction ID.

The “XFER HIGH to LOW Service” process has equal functionality, with the following changes:

- Replace all references in the text to “LOW to HIGH” with “HIGH to LOW”

- Replace all references in the text to “low partition” with “high partition”, and vice versa.

- Step 6 is not optional, but must always be performed, e.g. Log flag must always be true for this service.

2.3 Scripts for creating and deleting user transfer areas

All administration of the directories mentioned earlier, are to be automatic. This means that when a user is created, changed or deleted, a script must be run to create or delete the corresponding directories in the transfer area.

When a user is created and/or given membership in certain user groups, the script must:

- Create a directory for the user (if it not already exists) on the XFER LOW to HIGH Source/XFER HIGH to LOW Target shares or the XFER HIGH to LOW Source/XFER LOW to HIGH Target shares, depending on which partition the user belongs to.

- Set correct ACLs on all created directories.

When a user is blocked, deleted or removed from certain user groups, the script must:

- Delete the directory for the user (including all subdirectories) on the XFER LOW to HIGH Source/XFER HIGH to LOW Target shares or the XFER HIGH to LOW

Source/XFER LOW to HIGH Target shares, depending on which partition the user belongs to.

The script is running as a scheduled task and can also be initiated by an administrator.

2.4 Scripts for verifying the configuration of TOE environment

As the TOE is heavily dependent on the Windows 2003 Server security functions, much of the security of the TOE is implemented by strict settings for users, group memberships and ACLs. If these settings get compromised, the security of the TOE also gets compromised. Therefore, the TOE includes a script to verify that the settings on the XFER server are correct. This script is derived from requirements in I-02 [26] and will run continually or can be initiated by XFER Service Admins. If any errors are found, the script will log the error and perform shutdown of the XFER services. A restart of the XFER services will require intervention by system administrator.

2.5 TOE boundaries

2.5.1 Logical and physical boundaries

The physical scope and deployment environment is defined in Table 2.

Logical boundaries / Part of TOE	Physical boundaries / Deployment environment
The two processes in the file transfer mechanism	A server in the XFER domain with EAL 4 certified MS Windows Server 2003 operating system configured according to [21, 22, 23, 26], and patch policy sufficient for stopping all known public available vulnerabilities. The server is separated from the high and low partition by an EAL4 certified firewall.
The scripts for creating and deleting user transfer areas	.NET framework 2.0, MS Windows Server 2003, Active Directory
Scripts for verifying the configuration of TOE environment	.NET framework 2.0, MS Windows Server 2003, Active Directory

Table 2 The deployment environment of the different parts of the TOE

3 TOE Security Environment

3.1 Secure Usage Assumptions

A.Acc_to_Comms: Physical protection of communications
Physical protection of the communications to the system is adequate to guard against unauthorized access or malicious modification by users.

A.Auth_Sys_Admin: Authenticated administrators
System Administrators are authenticated and held accountable for their actions.

A.Certified_FW: Certified firewall
The TOE shall use a firewall certified and configured at an EAL equal to or higher than the TOE. All communication between the partitions shall be mediated by this firewall.
The patch policy for the TOE environment must be sufficient for stopping all known, public available vulnerabilities in the TOE environment software.

A.Certified_OS: Certified operation system
The TOE shall run under an OS certified and configured at an EAL equal to or higher than the TOE.
The patch policy for the TOE environment must be sufficient for stopping all known, public available vulnerabilities in the TOE environment software.

A.Competent_Admin: Competent System Administrators
System Administrators have been given training and are competent to manage the TOE and the security of the information it contains.

A.Competent_User: Competent Users
Users have been given training and are competent to use the TOE.

A.Connection: No unauthorized connection to public networks
The TOE and TOE environment shall not have any connections, directly or indirectly, to unclassified and/or public networks, which not specifically are approved by NSM.

A.No_Abuse_By_Admin: No abusive System Administrators
System Administrators are trusted not to abuse their authority.

A.Physical_Location: Secure physical location
The TOE shall be installed in a secure physical location in accordance with P.Legislation and P.Infosec.

A.Remote_Admin: Remote administration
System Administrators have remote access and are able to view and modify security-relevant data according to their respective access rights.

3.2 Threats to Security

3.2.1 Identification of Assets

The assets within the TOE that need protection are all classified information.

3.2.2 Identification of Threat Agents

TA.Admin: Administrator
Authenticated authorized administrators of XFER Service. These threat agents may unintentionally perform unauthorized actions. The result being that they are given the ability to read, copy or modify classified information not authorised for them.

TA.User: User
Authenticated authorised user of XFER Service. These threat agents may intentionally or unintentionally perform unauthorized actions. Their intention can be to read, copy or modify classified information not authorised for them. They may be supported by organizations with “unlimited” resources.

TA.Hacker: Hacker
Personnel with no authorized access to the TOE or TOE environment. These threat agents may try to access classified information. They may have “unlimited” resource supporting them.

3.2.3 Identification of Threats to TOE Environment

TE.Admin_Err_Omit: Administrative errors of omission
The System Administrator fails to perform functions essential to security.
Threat agent: TA.Admin
Asset: Classified information
Unwanted outcome: Unauthorised personnel get access to classified information
Attack method: The system administrator forgets or fails to update the TOE environment with security patches.

TE.Audit_Trail_Loss: Loss of audit trail
Loss of audit trail (Event log).
Threat agent: TA.User, TA.Hacker
Asset: Classified information
Unwanted outcome: Threat agents get undetected access to classified information
Attack method: A threat agent will perform a large amount of transactions in order to fill the Event log and hence make audit unavailable.

TE.Exploit_Vuln: User exploits vulnerability
A user or hacker tries to exploit a vulnerability in the IT-environment to get unauthorised access to information.
Threat agent: TA.User, TA.Hacker
Asset: Classified information
Unwanted outcome: Unauthorised personnel get access to classified information
Attack method: A threat agent use hacking methods to exploit weaknesses in the TOE environment

TE.Hack_AC: Hacker gains undetected system access
A hacker gains undetected access to TOE environment due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.
Threat agent: TA.Hacker
Asset: Classified information
Unwanted outcome: Unauthorised personnel get access to classified information
Attack method: A threat agent use hacking methods to exploit missing, weak or incorrectly implemented access control in the TOE environment.

TE.Hack_Masq: Hacker masquerading as a legitimate user
A hacker masquerades as an authorized user to perform operations that will be attributed to

the authorized user or a system process.
Threat agent: TA.Hacker
Asset: Classified information
Unwanted outcome: Unauthorised personnel get access to classified information
Attack method: A hacker will use hacker methods to obtain user id and password of an authorised user to get access to classified information.

3.2.4 Identification of Threats to TOE

TT.Admin_Err_Omit: Administrative errors of omission
The System Administrator fails to perform some function essential to security.
Threat agent: TA.Admin
Asset: Classified information
Unwanted outcome: Unauthorised personnel get access to classified information.
Attack method: The system administrator stops the verification script from running or makes error in the flow control policy.

TT.Audit_Trail_Loss: Loss of audit trail
Loss of audit trail (Content Archive).
Threat agent: TA.User, TA.Hacker
Asset: Classified information
Unwanted outcome: Threat agents get undetected access to classified information
Attack method: A threat agent will perform a large amount of transactions in order to fill the Content Archive and hence make audit unavailable

TT.Buffer_overflow: User creates buffer overflow
A user creates a buffer overflow to get unauthorised access to the TOE.
Threat agent: TA.User
Asset: Classified information
Unwanted outcome: Unauthorised personnel get access to classified information
Attack method: A Threat agent creates a path too long for MS Windows or a file with large alternate streams, or with a large number of alternate streams.

TT.Exploit_vuln: User exploits vulnerability
A user or hacker tries to exploit a vulnerability in the TOE software.
Threat agent: TA.User, TA.Hacker
Asset: Classified information
Unwanted outcome: Unauthorised personnel get access to classified information
Attack method: A threat agent use hacking methods to exploit weaknesses in the TOE.

TT.Hack_AC: Hacker gains undetected system access
A hacker gains undetected access to TOE due to missing, weak and/or incorrectly implemented access rights causing potential violations of integrity, confidentiality, or availability.
Threat agent: TA.Hacker
Asset: Classified information
Unwanted outcome: Unauthorised personnel get access to classified information
Attack method: A threat agent use hacking methods to exploit missing, weak or incorrectly implemented access rights.

TT.Hack_Masq: Hacker masquerading a legitimate system process
A hacker masquerades a system process by replacing a legal process.
Threat agent: TA.Hacker
Asset: Classified information
Unwanted outcome: Unauthorised personnel get access to classified information

Attack method: A hacker will replace scripts or processes with false scripts or processes (Trojan Horse) to get access to classified information.

TT.Flow_Control_Policy_Violation: Flow control policy violation
An unauthorized user changes the configuration of the XFER Service causing violation of the TOE transfer policy.
Threat agent: TA.User
Asset: Classified information
Unwanted outcome: Unauthorised personnel get access to classified information
Attack method: A threat agent will try to gain access to the XFER Service to change the security parameters.

3.3 Organisational Security Policies

P.Accountability: Individual accountability
Individuals shall be held accountable for their actions.

P.Audit: Audit review
The TOE shall perform audit to Content Archive and initiate audit to Event log and Schedlgu.txt. Based on these logs, daily and weekly reports showing number of files and volume of files transferred during the period shall be generated:
- To high and low partitions
- To high and low partitions – summarized per user
- To low partition – summarized per release marking
- Number of files and volume of files transferred per direction per release marking per user.

P.Authorities: Notification of threats and vulnerabilities
Appropriate authorities shall be immediately notified of any threats or vulnerabilities impacting TOE or TOE environment.

P.Authorized_Use: Authorized use of information
Information shall be used only for its authorized purpose(s).

P.Infosec: C-M(2002)49
The TOE and its environment are compliant with the NATO security policy as stated in C-M(2002)49 Enclosure F [6], AC/35-D/2004 [24] and AC/35-D/2005 [25].

P.Implementation: Implementation of the TOE
Each transfer process shall be implemented as Win32 service and run under a distinct account.

P.Information_AC: Information access control
Information shall be accessed only by authorized individuals and processes.

P.Legislation: The Norwegian Security Act
The TOE and its environment are compliant with The Norwegian Security Act (Sikkerhetsloven) [4] with supportive Directive on information security (Forskrift om informasjonssikkerhet) [5].

P.Marking: Information marking
Files shall be marked with security classification by the user/owner of the file.

P.Password: Different passwords in low and high partition
Users must have different passwords in low and high partitions.

P.Sec_Label_Attributes Security label attributes
Security label attributes according to flow control policy can only be configured in the TOE by XFER Service Enterprise Admins.

4 Security Objectives

4.1 Security Objectives for TOE

O.Audit: Audit records with identity
The TOE shall perform audit to Content Archive and initiate audit to Event log and Schedlgu.txt.

O.Config_Protection Protection of flow control security configuration
Configuration of the flow control security parameters shall be protected from manipulation by unauthorised personnel.

O.Flow_Control: Flow control between partitions
The TOE shall perform a flow control to ensure that the file transfer between partitions is according to flow control policy for file transfer. Filtering rules and security label in the flow control policy can only be configured by XFER Service Enterprise Admins.

O.Sec_Env: Secure environment
The TOE shall verify the configuration of the TOE environment to secure that the TOE is operating in a secure environment. This is done by a verification script. This script is derived from requirements in I-02 [26] and will run continually or can be initiated by XFER Service Admins. If any errors are found, the script will log the error and perform shutdown of the XFER services. A restart of the XFER services will require intervention by system administrator.

4.2 Security Objectives for TOE Environment

OE.Access_Control Access Control
Access control shall be performed in the environment before users and system administrators are given access to the XFER service.

OE.Event_Log Event log
The environment shall perform audit to Event log and Schedlgu.txt.

OE.Inst_Env Installation Environment
The TOE shall be installed in a secure physical and logical environment.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

Functional Class	Functional Components
FAU	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.2, FAU_STG.3
FDP	FDP_IFC.2, FDP_IFF.1
FMT	FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1,
FPT	FPT_AMT.1, FPT_FLS, FPT_RCV.1, FPT_RVM.1, FPT_SEP.1, FPT_STM.1
FRU	FRU_FLT.1

Table 3 Functional Requirements for the TOE

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.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 detailed level of audit; and

c)- File transfer between partitions shall be logged:

- content to a distinct archive area on the XFER Server archive before the actual transfer
- Event log after transfer

- Failures shall be logged:

- Unable to start verification script
- Verification script step fails
- Service configuration missing or corrupt
- File move failed
- Content Archive fails
- Error report write fails
- XFER services out of memory (the logging of this error might fail because of lack of memory)

- Non-unique transaction id
- File name already exist in target area
- Source file not in transfer area
- File in subdirectory of transfer area
- Base account name of file owner not equal to name of transfer area
- Remove alternate data streams from file
- Unable to delete file in source area
- Verification script is unable to stop the XFER services
- Configuration script fails
- XFER services fails

- The following type of events shall be logged

  - Start of the verification script
  - Start and stop of the configuration script
  - Start and stop of the XFER Service
  - All failing checks detected by the verification script
  - All runtime errors encountered by the verification script
  - Stop of the verification script with all verifications OK
  - Stop of the verification script with runtime errors, but verification regarded as OK.$^{\text{FAU\_GEN.1.1}}$

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST,

Event log:
- Date,
- Time,
- Type (severity indicator),
- User (what user generated the event),
- Computer (on what computer did the event occur / was the Event logged),
- Source (event class / what component generated the event, e.g. XFER Service),
- Category (event sub-classing, e.g. XFER HIGH to LOW and XFER LOW to HIGH),
- Event ID (unique event indicator, relative to the source and category),
- Description (text describing the event, use = list format if multiple values).

The event Description field shall contain the following XFER Service parameters under start-up:
- Source directory
- Destination directory
- Content archival flag
- Content archival directory

The event description field shall contain the following XFER service parameter under transfer:
- File transfer transaction identifier
- End-user base account name
- Direction – File name
- File attributes (size, etc)
- Marking
- Archived file contents (relative path or «N/A» if not applicable)
- Data (binary data describing the event, optional)

Content Archive:
- File transfer transaction identifier
- End-user base account name
- Direction
- File name
- File attributes (size, etc)
- Marking
- Archived file contents (relative path or «N/A» if not applicable[FAU_GEN.1.2]

5.1.1.2 User identity association (FAU_GEN.2)

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

5.1.1.3 Audit review (FAU_SAR.1)

The TSF shall provide XFER Service Auditors and XFER Service Admins with the capability to read:
- Content Archive
- Event log
- Schedlgu.txt
from the audit records.[FAU_SAR.1.1]

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

5.1.1.4 Restricted audit review (FAU_SAR.2)

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

5.1.1.5 Guarantees of audit data availability (FAU_STG.2)

The TSF shall protect the stored audit records from unauthorised deletion.[FAU_STG.2.1]

The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.[FAU_STG.2.2]

The TSF shall ensure that all audit records will be maintained when the following conditions occur: Audit storage exhaustion failure.[FAU_STG.2.3]

5.1.1.6 Action in case of possible audit data loss (FAU_STG.3)

The TSF shall take action to perform service shut down if the audit trail exceeds the storage limit.[FAU_STG.3.1]

5.1.2 User data protection (FDP)

Complete information flow control (FDP_IFC.2)

The TSF shall enforce the XFER information flow control SFP on
List of subjects:
- User
- Personal transfer areas
List of information:

- Information in files
and all operations that cause that information to flow to and from subjects covered by the SFP.[FDP_IFC.2.1]

The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.[FDP_IFC.2.2]

5.1.2.1 Simple security attributes (FDP_IFF.1)

The TSF shall enforce the XFER information flow control SFP
based on the following types of subject and information security attributes:
List of subjects:
- User
- Personal transfer areas

List of information:
- Information in files

List of security attributes:
- User id
- File type
- Security label
- Log flag.[FDP_IFF.1.1]

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: XFER information flow control SFP.[FDP_IFF.1.2]

The TSF shall enforce the additional information flow: none.[FDP_IFF.1.3]

The TSF shall provide the following additional information flow: none.[FDP_IFF.1.4]

The TSF shall explicitly authorise an information flow based on the following rules: none.[FDP_IFF.1.5]

The TSF shall explicitly deny an information flow based on the following rules: none.[FDP_IFF.1.6]

5.1.3 Security management (FMT)

5.1.3.1 Management of security attributes (FMT_MSA.1)

The TSF shall enforce the XFER access control SFP to restrict the ability to change_default, modify and delete the security attributes filtering rules, security label and content archive from low to high file transfer to XFER Service Enterprise Admins.[FMT_MSA.1.1]

5.1.3.2 Static attribute initialisation (FMT_MSA.3)

The TSF shall enforce the XFER access control SFP to provide restrictive default values for security attributes that are used to enforce the SFP.[FMT_MSA.3.1]

The TSF shall allow the XFER Service Enterprise Admins to specify alternative initial values to override the default values when an object or information is created.[FMT_MSA.3.2]

5.1.3.3 Management of TSF data (FMT_MTD.1)

The TSF shall restrict the ability to

- query, modify, clear and add the security attributes to XFER Service Enterprise Admins
- query the security attributes to the XFER services user accounts and the verification script user account. FMT_MTD.1.1

5.1.3.4 Specification of Management Functions (FMT_SMF.1)

The TSF shall be capable of performing the following security management functions:
- Start and stop of script for creating and deleting user transfer areas
- Start and stop of script for verifying the configuration of the TOE environment
- Modification of the flow control policy
- Modification of the configuration script configuration file
- Modification of the verification script configuration file
- Changing the password for the user accounts that the configuration and/or the verification script uses to read the information from the high, low and XFER partition domains.
- Start and stop of the XFER services
- Read the audited events
- Modification of last transactionID for the XFER services.
- Modification of general registry settings for the XFER services. FMT_SMF.1.1

5.1.4 Protection of the TOE Security Functions (FPT)

5.1.4.1 Abstract machine testing (FPT_AMT.1)

The TSF shall run a suite of tests during initial start-up and periodically during normal operation to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. FPT_AMT.1.1

5.1.4.2 Failure with preservation of secure state (FPT_FLS.1)

The TSF shall preserve a secure state when the following types of failures occur:
- Configuration scripts fails and shuts down
- Runtime errors occurs in the verification script
- Non-unique transaction id
- File name already exists in target area
- Source file not in transfer area
- File in subdirectory of transfer area
- Base account name of file owner not equal to name of transfer area
- Error in removal of alternate data streams from file
- Unable to delete file in source area FPT_FLS.1.1

5.1.4.3 Manual recovery (FPT_RCV.1)

After:
- Verification script fails
- Event log fails
- Service configuration missing or corrupt
- File move failed because of full disk
- Content Archive fails because of full disk
- Error report write fails because of full disk
- XFER services fails
- Service out of memory

The TSF shall enter a maintenance mode where the ability to return to a secure state is provided. FPT_RCV.1.1

5.1.4.4 Non-bypassability of the TSP (FPT_RVM.1)

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

5.1.4.5 TSF domain separation (FPT_SEP.1)

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

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

5.1.4.6 Reliable time stamps (FPT_STM.1)

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

5.1.5 Resource utilisation (FRU)

5.1.5.1 Degraded fault tolerance (FRU_FLT.1)

The TSF shall ensure the operation of XFER services and verification script when the following failures occur:
- Configuration scripts fails and shuts down
- Runtime errors occurs in the verification script
- Non-unique transaction id
- File name already exists in target area
- Source file not in transfer area
- File in subdirectory of transfer area
- Base account name of file owner not equal to name of transfer area
- Error in removal of alternate data streams from file
- Unable to delete file in source area. $^{\text{FRU\_FLT.1.1}}$

5.2 TOE Security Assurance Requirements

Assurance Class	Assurance Components
ACM	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2
ADO	ADO_DEL.2 ADO_IGS.1
ADV	ADV_FSP.2 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 ADV_RCR.1 ADV_SPM.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.1 ALC_LCD.1 ALC_TAT.1

ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_MSU.2 AVA_SOF.1 AVA_VLA.2

Table 4 Assurance Requirements: EAL (4)

5.2.1 Configuration management (ACM)

5.2.1.1 Partial CM automation (ACM_AUT.1)

The developer shall use a CM system.$^{\text{ACM\_AUT.1.1D}}$

The developer shall provide a CM plan.$^{\text{ACM\_AUT.1.2D}}$

The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.$^{\text{ACM\_AUT.1.1C}}$

The CM system shall provide an automated means to support the generation of the TOE.$^{\text{ACM\_AUT.1.2C}}$

The CM plan shall describe the automated tools used in the CM system.$^{\text{ACM\_AUT.1.3C}}$

The CM plan shall describe how the automated tools are used in the CM system.$^{\text{ACM\_AUT.1.4C}}$

5.2.1.2 Generation support and acceptance procedures (ACM_CAP.4)

The developer shall provide a reference for the TOE.$^{\text{ACM\_CAP.4.1D}}$

The developer shall use a CM system.$^{\text{ACM\_CAP.4.2D}}$

The developer shall provide CM documentation.$^{\text{ACM\_CAP.4.3D}}$

The reference for the TOE shall be unique to each version of the TOE.$^{\text{ACM\_CAP.4.1C}}$

The TOE shall be labelled with its reference.$^{\text{ACM\_CAP.4.2C}}$

The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.$^{\text{ACM\_CAP.4.3C}}$

The configuration list shall uniquely identify all configuration items that comprise the TOE.$^{\text{ACM\_CAP.4.4C}}$

The configuration list shall describe the configuration items that comprise the TOE.$^{\text{ACM\_CAP.4.5C}}$

The CM documentation shall describe the method used to uniquely identify the configuration items.$^{\text{ACM\_CAP.4.6C}}$

The CM system shall uniquely identify all configuration items.$^{\text{ACM\_CAP.4.7C}}$

The CM plan shall describe how the CM system is used.$^{\text{ACM\_CAP.4.8C}}$

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.$^{\text{ACM\_CAP.4.9C}}$

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.[ACM_CAP.4.10C]

The CM system shall provide measures such that only authorised changes are made to the configuration items.[ACM_CAP.4.11C]

The CM system shall support the generation of the TOE.[ACM_CAP.4.12C]

The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.[ACM_CAP.4.13C]

5.2.1.3 Problem tracking CM coverage (ACM_SCP.2)

The developer shall provide a list of configuration items for the TOE.[ACM_SCP.2.1D]

The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.[ACM_SCP.2.1C]

5.2.2 Delivery and operation (ADO)

5.2.2.1 Detection of modification (ADO_DEL.2)

The developer shall document procedures for delivery of the TOE or parts of it to the user.[ADO_DEL.2.1D]

The developer shall use the delivery procedures.[ADO_DEL.2.2D]

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.[ADO_DEL.2.1C]

The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.[ADO_DEL.2.2C]

The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.[ADO_DEL.2.3C]

5.2.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.[ADO_IGS.1.1D]

The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.[ADO_IGS.1.1C]

5.2.3 Development (ADV)

5.2.3.1 Fully defined external interfaces (ADV_FSP.2)

The developer shall provide a functional specification.[ADV_FSP.2.1D]

The functional specification shall describe the TSF and its external interfaces using an informal style.[ADV_FSP.2.1C]

The functional specification shall be internally consistent.[ADV_FSP.2.2C]

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.[ADV_FSP.2.3C]

The functional specification shall completely represent the TSF.[ADV_FSP.2.4C]

The functional specification shall include rationale that the TSF is completely represented.[ADV_FSP.2.5C]

5.2.3.2 Security enforcing high-level design (ADV_HLD.2)

The developer shall provide the high-level design of the TSF.[ADV_HLD.2.1D]

The presentation of the high-level design shall be informal.[ADV_HLD.2.1C]

The high-level design shall be internally consistent.[ADV_HLD.2.2C]

The high-level design shall describe the structure of the TSF in terms of subsystems.[ADV_HLD.2.3C]

The high-level design shall describe the security functionality provided by each subsystem of the TSF.[ADV_HLD.2.4C]

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.[ADV_HLD.2.5C]

The high-level design shall identify all interfaces to the subsystems of the TSF.[ADV_HLD.2.6C]

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.[ADV_HLD.2.7C]

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.[ADV_HLD.2.8C]

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems. [ADV_HLD.2.9C]

5.2.3.3 Subset of the implementation of the TSF (ADV_IMP.1)

The developer shall provide the implementation representation for a selected subset of the TSF.[ADV_IMP.1.1D]

The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.[ADV_IMP.1.1C]

The implementation representation shall be internally consistent.[ADV_IMP.1.2C]

5.2.3.4 Descriptive low-level design (ADV_LLD.1)

The developer shall provide the low-level design of the TSF.[ADV_LLD.1.1D]

The presentation of the low-level design shall be informal.[ADV_LLD.1.1C]

The low-level design shall be internally consistent.[ADV_LLD.1.2C]

The low-level design shall describe the TSF in terms of modules.[ADV_LLD.1.3C]

The low-level design shall describe the purpose of each module.[ADV_LLD.1.4C]

The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.[ADV_LLD.1.5C]

The low-level design shall describe how each TSP-enforcing function is provided.[ADV_LLD.1.6C]

The low-level design shall identify all interfaces to the modules of the TSF.[ADV_LLD.1.7C]

The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.[ADV_LLD.1.8C]

The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.[ADV_LLD.1.9C]

The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.[ADV_LLD.1.10C]

5.2.3.5 Informal correspondence demonstration (ADV_RCR.1)

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.[ADV_RCR.1.1D]

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.[ADV_RCR.1.1C]

5.2.3.6 Informal TOE security policy model (ADV_SPM.1)

The developer shall provide a TSP model.[ADV_SPM.1.1D]

The developer shall demonstrate correspondence between the functional specification and the TSP model.[ADV_SPM.1.2D]

The TSP model shall be informal.[ADV_SPM.1.1C]

The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modelled.[ADV_SPM.1.2C]

The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modelled.[ADV_SPM.1.3C]

The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.[ADV_SPM.1.4C]

5.2.4 Guidance documents (AGD)

5.2.4.1 Administrator guidance (AGD_ADM.1)

The developer shall provide administrator guidance addressed to system administrative personnel.$^{\text{AGD\_ADM.1.1D}}$

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.$^{\text{AGD\_ADM.1.1C}}$

The administrator guidance shall describe how to administer the TOE in a secure manner.$^{\text{AGD\_ADM.1.2C}}$

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.$^{\text{AGD\_ADM.1.3C}}$

The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.$^{\text{AGD\_ADM.1.4C}}$

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.$^{\text{AGD\_ADM.1.5C}}$

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.$^{\text{AGD\_ADM.1.6C}}$

The administrator guidance shall be consistent with all other documentation supplied for evaluation.$^{\text{AGD\_ADM.1.7C}}$

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.$^{\text{AGD\_ADM.1.8C}}$

5.2.4.2 User guidance (AGD_USR.1)

The developer shall provide user guidance.$^{\text{AGD\_USR.1.1D}}$

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE. $^{\text{AGD\_USR.1.1C}}$

The user guidance shall describe the use of user-accessible security functions provided by the TOE.$^{\text{AGD\_USR.1.2C}}$

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.$^{\text{AGD\_USR.1.3C}}$

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.$^{\text{AGD\_USR.1.4C}}$

The user guidance shall be consistent with all other documentation supplied for evaluation.$^{\text{AGD\_USR.1.5C}}$

The user guidance shall describe all security requirements for the IT environment that are relevant to the user.$^{\text{AGD\_USR.1.6C}}$

5.2.5 Life cycle support (ALC)

5.2.5.1 Identification of security measures (ALC_DVS.1)

The developer shall produce development security documentation.[ALC_DVS.1.1D]

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.[ALC_DVS.1.1C]

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.[ALC_DVS.1.2C]

5.2.5.2 Developer defined life-cycle model (ALC_LCD.1)

The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.[ALC_LCD.1.1D]

The developer shall provide life-cycle definition documentation.[ALC_LCD.1.2D]

The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.[ALC_LCD.1.1C]

The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.[ALC_LCD.1.2C]

5.2.5.3 Well-defined development tools (ALC_TAT.1)

The developer shall identify the development tools being used for the TOE.[ALC_TAT.1.1D]

The developer shall document the selected implementation-dependent options of the development tools.[ALC_TAT.1.2D]

All development tools used for implementation shall be well-defined.[ALC_TAT.1.1C]

The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.[ALC_TAT.1.2C]

The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.[ALC_TAT.1.3C]

5.2.6 Tests (ATE)

5.2.6.1 Analysis of coverage (ATE_COV.2)

The developer shall provide an analysis of the test coverage.[ATE_COV.2.1D]

The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.[ATE_COV.2.1C]

The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete. [ATE_COV.2.2C]

5.2.6.2 Testing: high-level design (ATE_DPT.1)

The developer shall provide the analysis of the depth of testing.ATE_DPT.1.1D

The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.ATE_DPT.1.1C

5.2.6.3 Functional testing (ATE_FUN.1)

The developer shall test the TSF and document the results.ATE_FUN.1.1D

The developer shall provide test documentation.ATE_FUN.1.2D

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.ATE_FUN.1.1C

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.ATE_FUN.1.2C

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.ATE_FUN.1.3C

The expected test results shall show the anticipated outputs from a successful execution of the tests.ATE_FUN.1.4C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.ATE_FUN.1.5C

5.2.6.4 Independent testing – sample (ATE_IND.2)

The developer shall provide the TOE for testing.ATE_IND.2.1D

The TOE shall be suitable for testing.ATE_IND.2.1C

The developer shall provide an equivalent set of resources to those that were used in the developer’s functional testing of the TSF. ATE_IND.2.2C

5.2.7 Vulnerability assessment (AVA)

5.2.7.1 Validation of analysis (AVA_MSU.2)

The developer shall provide guidance documentation. AVA_MSU.2.1D

The developer shall document an analysis of the guidance documentation.AVA_MSU.2.2D

The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.AVA_MSU.2.1C

The guidance documentation shall be complete, clear, consistent and reasonable.AVA_MSU.2.2C

The guidance documentation shall list all assumptions about the intended environment.AVA_MSU.2.3C

The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).[AVA_MSU.2.4C]

The analysis documentation shall demonstrate that the guidance documentation is complete.[AVA_MSU.2.5C]

5.2.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.[AVA_SOF.1.1D]

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.[AVA_SOF.1.1C]

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.[AVA_SOF.1.2C]

5.2.7.3 Independent vulnerability analysis (AVA_VLA.2)

The developer shall perform a vulnerability analysis.[AVA_VLA.2.1D]

The developer shall provide vulnerability analysis documentation.[AVA_VLA.2.2D]

The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.[AVA_VLA.2.1C]

The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.[AVA_VLA.2.2C]

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. [AVA_VLA.2.3C]

The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks. [AVA_VLA.2.4C]

5.3 Security Requirements for the IT Environment

5.3.1 Functional requirements for TOE environment

Functional Class	Functional Components
FAU	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2
FDP	FDP_ACC.2, FDP_ACF.1
FIA	FIA_UAU.2, FIA_UID.2

FMT	FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1

Table 5 Functional Requirements for the IT Environment

5.3.1.1 Security audit (FAU)

Audit data generation (FAU_GEN.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 detailed level of audit; and

c) - File transfer between partitions shall be logged:

- Event log after transfer

- Failures shall be logged:
- Unable to start verification script
- Verification script step fails
- Service configuration missing or corrupt
- File move failed
- Content Archive fails
- Error rapport write fails
- XFER services out of memory (the logging of this error might fail because of lack of memory)- Non-unique transaction id
- File name already exist in target area
- Source file not in transfer area
- File in subdirectory of transfer area
- Base account name of file owner not equal to name of transfer area
- Remove alternate data streams from file
- Unable to delete file in source area
- Verification script is unable to stop the XFER services
- Configuration script fails
- XFER services fails

- The following type of events shall be logged
- Start of the verification script
- Start and stop of the configuration script
- Start and stop of the XFER Service
- All failing checks detected by the verification script
- All runtime errors encountered by the verification script
- Stop of the verification script with all verifications OK
- Stop of the verification script with runtime errors, but verification regarded as OK..[FAU_GEN.1.1]

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST:

Event log:
- Date,
- Time,
- Type (severity indicator),
- User (what user generated the event),
- Computer (on what computer did the event occur / was the Event logged),
- Source (event class / what component generated the event, e.g. XFER Service),
- Category (event sub-classing, e.g. XFER HIGH to LOW and XFER LOW to HIGH),
- Event ID (unique event indicator, relative to the source and category),
- Description (text describing the event, use = list format if multiple values).

The event Description field shall contain the following XFER Service parameters under start-up:
- Source directory
- Destination directory
- Content archival flag
- Content archival directory

The event description field shall contain the following XFER service parameter under transfer:
- File transfer transaction identifier
- End-user base account name
- Direction – File name
- File attributes (size, etc)
- Marking
- Archived file contents (relative path or «N/A» if not applicable)
- Data (binary data describing the event, optional)

Schedlgu.txt:
- Date,
- Time,
- User (what user started or stopped the scheduled task).[FAU_GEN.1.2]

User identity association (FAU_GEN.2)

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

Audit review (FAU_SAR.1)

The TSF shall provide XFER Service Auditors and XFER Service Admins with the capability to read:
- Event log
- Schedlgu.txt

from the audit records.[FAU_SAR.1.1]

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

Restricted audit review (FAU_SAR.2)

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

5.3.1.2 Identification and authentication (FIA)

User authentication before any action (FIA_UAU.2)

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

User identification before any action (FIA_UID.2)

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

5.3.1.3 User data protection (FDP)

Complete access controle (FDP_ACC.2)

The TSF shall enforce the XFER access control SFP on

list of subjects:
- Users

list of objects
- Files
- Transfer areas
- Content archive
- Event log
- Registry
- Services
- Schedlgu.txt

and all operations among subjects and objects covered by the XFER access control SFP. FDP_ACC.2.1

The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP. FDP_ACC.2.2

Security attribute based access control (FDP_ACF.1)

The TSF shall enforce the XFER access control SFP to objects based on the following:

List of subjects:
- Users

List of objects:
- Files
- Transfer areas
- Content archive
- Event log
- Registry
- Services
- Schedlgu.txt

Access control attributes associated with an subject:
- identity, group membership(s) and privileges associated with a subject

Access control attributes associated with an object:
- Object owner

- A discretionary Access Control List (DACL) that can be either absent, empty, or consist of a list of one or more entries. Each DACL entry has a:
- Type (allow or deny)
- User or group identifier
- Specific object access right bitmasks

The defaults for allowed or denied operations are:
- If a DACL is absent, the object is not protected and all access is granted.
- If a DACL is present but empty, no access is granted $^{\text{FDP\_ACF.1.1}}$

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: Object access is allowed if at least one of the following conditions is true:
- A DACL entry explicitly grants access to a user, and the access has not been denied by a previous entry in the DACL
- A DACL entry explicitly grants access to a group of which the subject is a direct or indirect member, and the access has not been denied by a previous entry int the DACL
- A DACL is not present. $^{\text{FDP\_ACF.1.2}}$

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: None. $^{\text{FDP\_ACF.1.3}}$

The TSF shall explicitly deny access of subjects to objects based on theObject access is explicitly denied if at least one of the below conditions is true:
- A DACL entry explicitly denies access for a user, and the access has not been granted by a previous entry in the DACL
- A DACL entry explicitly denies access for the group of which the user is a direct or indirect member, and the access has not been granted by a previous entry in the DACL. $^{\text{FDP\_ACF.1.4}}$

5.3.1.4 Security management (FMT)

Management of security attributes (FMT_MSA.1)

The TSF shall enforce the XFER access control SFP to restrict the ability to modify and delete the security attributes access control attributes associated with a named object to XFER Service Admins.$^{\text{FMT\_MSA.1.1}}$

Static attribute initialisation (FMT_MSA.3)

The TSF shall enforce the XFER access control SFP to provide restrictive default values for security attributes that are used to enforce the XFER access control SFP.$^{\text{FMT\_MSA.3.1}}$

The TSF shall allow the XFER Service admins to specify alternative initial values to override the default values when an object or information is created.$^{\text{FMT\_MSA.3.2}}$

Specification of management functions (FMT_SMF.1)

The TSF shall be capable of performing the following security management functions:
- Modify access control attributes associated with an object
- Read the audited events
- Modify the audit log size
- Changing the password for the user accounts that the configuration script, verification script and/or XFER services uses
- Add and remove users to/from the XFER Service $^{\text{FMT\_SMF.1.1}}$

Security roles (FMT_SMR.1)

The TSF shall maintain the roles XFER HIGH to LOW Source Users, XFER HIGH to LOW Target Users, XFER LOW to HIGH Source Users, XFER LOW to HIGH Target Users, XFER Service Auditors, XFER HIGH Operators, XFER LOW Operators, XFER Service Admins, XFER Service Enterprise Admins, Administrators and Enterprise Domain Controllers.$^{\text{FMT\_SMR.1.1}}$

The TSF shall be able to associate users with roles.$^{\text{FMT\_SMR.1.2}}$

5.3.2 Assurance requirements for TOE environment

Assurance Class	Assurance Components
ADO	ADO_IGS.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.1

Table 6 Assurance Requirements for the IT Environment

5.3.2.1 Delivery and operation (ADO)

Installation, generation, and start-up procedures (ADO_IGS.1)

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.$^{\text{ADO\_IGS.1.1D}}$

The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.$^{\text{ADO\_IGS.1.1C}}$

5.3.2.2 Guidance documents (AGD)

Administrator guidance (AGD_ADM.1)

The developer shall provide administrator guidance addressed to system administrative personnel.$^{\text{AGD\_ADM.1.1D}}$

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.$^{\text{AGD\_ADM.1.1C}}$

The administrator guidance shall describe how to administer the TOE in a secure manner.$^{\text{AGD\_ADM.1.2C}}$

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.$^{\text{AGD\_ADM.1.3C}}$

The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.$^{\text{AGD\_ADM.1.4C}}$

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.$^{\text{AGD\_ADM.1.5C}}$

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.$^{\text{AGD\_ADM.1.6C}}$

The administrator guidance shall be consistent with all other documentation supplied for evaluation.$^{\text{AGD\_ADM.1.7C}}$

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.$^{\text{AGD\_ADM.1.8C}}$

User guidance (AGD_USR.1)

The developer shall provide user guidance.$^{\text{AGD\_USR.1.1D}}$

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE. $^{\text{AGD\_USR.1.1C}}$

The user guidance shall describe the use of user-accessible security functions provided by the TOE.$^{\text{AGD\_USR.1.2C}}$

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.$^{\text{AGD\_USR.1.3C}}$

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.$^{\text{AGD\_USR.1.4C}}$

The user guidance shall be consistent with all other documentation supplied for evaluation.$^{\text{AGD\_USR.1.5C}}$

The user guidance shall describe all security requirements for the IT environment that are relevant to the user.$^{\text{AGD\_USR.1.6C}}$

5.3.2.3 Life cycle support (ALC)

Identification of security measures (ALC_DVS.1)

The developer shall produce development security documentation.$^{\text{ALC\_DVS.1.1D}}$

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.$^{\text{ALC\_DVS.1.1C}}$

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.$^{\text{ALC\_DVS.1.2C}}$

5.4 Minimum strength of function (SOF) for TOE

CC part 1, chapter 2.6 require a statement about the minimum strength level for the TOE security functions realized by probabilistic or permutational mechanisms. In this TOE there are no security functions realized by probabilistic or permutational mechanisms. Accordingly there is not a SOF-claim for any SFR of the TOE in this ST.

6 TOE Summary Specification

The TOE summary specification gives a high-level description of the security functions and assurance measures, and traces them to the TOE Functional and Assurance requirements. The security functions claimed to meet the functional requirements are shown in table 7. The assurance measures taken to meet the assurance requirements are shown in table 8.

6.1 Functional requirements

TOE Security Functions	Requirement	Implementation description	Reference
SF.Audit	FAU_GEN.1	The XFER services are shut down if audit generation fails (for example if audit generation is shut down). Audit generation is performed at start-up and shut-down of the XFER Service. File transfer is audited in Content Archive and Event log. Audit generation is performed using MS Windows audit functions.	Usage Scenarios [7]
	FAU_GEN.2	Audit of file transfer is identified by the SID of the file owner. Audit of start up and shut down of the XFER Service is identified by user-ID of the user that performs the operation	Usage Scenarios [7]
	FAU_SAR.1	MS Windows access control is used to grant access to Event log, Schedlgu.txt and Content Archive to XFER Service Auditors and XFER Service Admins.	Usage Scenarios [7]
	FAU_SAR.2	MS Windows access control is used to prohibit all users read access to Event log, Schedlgu.txt and Content Archive except those users described in FAU_SAR.1	Usage Scenarios [7]
	FAU_STG.2	Event log configuration is set to “do not overwrite events”. Shut down of the XFER services is performed if the Event log or write to Content Archive fails.	Usage Scenarios [7]

TOE Security Functions	Requirement	Implementation description	Reference
	FAU_STG.3	Shut down of the XFER services is performed if the Event log or write to Content Archive fails.	Usage Scenarios [7]
SF.Flow_Control	FDP_IFC.2	Flow control policy is implemented as functionality in the XFER services. It is not possible to turn off the flow control policy using configuration.	Usage Scenarios [7]
	FDP_IFF.1	Flow control policy is implemented as functionality in the XFER services. Additional flow control policies are not allowed.	Usage Scenarios [7]
SF.Security_Management	FMT_MSA.1	Registry key is protected with MS Windows access control.	Usage Scenarios [7]
	FMT_MSA.3	MS Windows access control is used to set restrictive default values on the security attributes.	Usage Scenarios [7]
	FMT_MTD.1	MS Windows access control is used to restrict access to the security attributes only to XFER Service Enterprise Admins, the XFER services user accounts and the verification script user account.	Usage Scenarios [7]
	FMT_SMF.1	The XFER Service will contain security management functions for starting script for creating and deleting user transfer areas, start of script for verifying the configuration of the TOE environment, modify the flow control policy, modify the configuration file for the configuration and the verification scripts, changing the password for the user accounts that the configuration and/or verification script uses to read the information from the high, low and XFER partitions domains and start and stop of the XFER Service.	Usage Scenarios [7]

TOE Security Functions	Requirement	Implementation description	Reference
SF.OS_Verification	FPT_AMT.1	Verification script will run a set of tests to demonstrate the correct operation of MS Windows.	Usage Scenarios [7]
SF.Shut_Down	FPT_RCV.1	The XFER Service will perform system shut down of the services when the specified errors occur.	Usage Scenarios [7]
	FPT_RVM.1	The XFER Service will perform system shut down of the services when the specified errors occur (FPT_RCV.1).	Usage Scenarios [7]
SF.Domain_Separation	FPT_SEP.1	MS Windows access control and installation of TOE in XFER domain.	Usage Scenarios [7]
SF.Time_Stamp	FPT_STM.1	Event log, Schedlgu.txt and Content Archive use server time stamp.	
SF.Fault_Tolerance	FPT_FLS.1	The TSF shall preserve a secure state in the event of defined failures.	
	FRU_FLT.1	The TSF shall ensure the operation of XFER services and verification script in the event of defined failures.	Usage Scenarios [7]

Table 7 TOE Security Functions mapped to Functional Requirements

6.2 Assurance Measures

Requirement	TOE assurance measure	Reference
ACM_AUT.1	Partial CM automation	Development Plan [8]
ACM_CAP.4	Generation support and acceptance procedures	Development Plan [8] Configuration list [30]
ACM_SCP.2	Problem tracking CM coverage	Configuration List [30]
ADO_DEL.2	Detection of modification	Development Plan [8]
ADO_IGS.1	Installation, generation and start-up procedures	Administrator Guidance [27]

ADV_FSP.2	Fully defined external interfaces	Functional Specification [11]
ADV_HLD.2	Security enforcing high-level design	High Level Design [12]
ADV_IMP.1	Subset of the implementation of the TSF	Subset of source code [19]
ADV_LLD.1	Descriptive low-level design	Usage Scenarios [7] Physical Design [13]
ADV_RCR.1	Informal correspondence demonstration	Informal correspondence demonstration [14]
ADV_SPM.1	Informal TOE security policy model	TSP model [15] Informal correspondence demonstration [14]
AGD_ADM.1	Administrator guidance	Administrator Guidance [27]
AGD_USR.1	User guidance	User Guidance [20]
ALC_DVS.1	Identification of security measures	Master Project Plan [16] Development Plan [8]
ALC_LCD.1	Developer defined life-cycle model	Master Project Plan [16]
ALC_TAT.1	Well-defined development tools	Development Plan [8]
ATE_COV.2	Analysis of coverage	Test Plan [9] Test Specification and Test Cases [29]
ATE_DPT.1	Testing: High-level design	Test Plan [9]
ATE_FUN.1	Functional testing	Test Plan [9] Testing and Bug Report [28] Test Specification and Test Cases [29]
ATE_IND.2	Independent testing – sample	The TOE will be provided for independent testing at NDCISD
AVA_MSU.2	Validation of analysis	Usage Scenarios [7] Test Plan [9] Informal correspondence demonstration [14] User Guidance [20]

		Administrator Guidance [27]
AVA_SOF.1	Strength of TOE security function evaluation	NA. The TOE does not have any functions that need further strength of TOE security function evaluation.
AVA_VLA.2	Independent vulnerability analysis	Security Plan [10]

Table 8 Assurance Measures

7 Protection Profile Claim

There are no Protection Profile claims.

8 Rationale

This chapter provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the assumptions, policies and threats. Arguments are provided for the coverage of each assumption, policy and threat. The chapter then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next Chapter 8 provides a set of arguments that address dependency analysis, and the internal consistency and mutual supportiveness of the ST requirements. It concludes with demonstrating how the TOE security functions satisfy the security function requirements.

8.1 Security Objectives Rationale

This section shows that all assumptions, policies and threats are completely covered by security objectives.

Assumptions/Policy/Threat	**Objectives**
Security Objectives for the TOE	
P.Accountability	O.Audit
P.Audit	O.Audit
P.Authorities	O.Audit, O.Config_Protection
P.Authorized_Use	O.Flow_Control
P.Infosec	O.Config_Protection, O.Sec_Env
P.Implementation	O.Sec_Env
P.Information_AC	O.Config_Protection, O.Flow_Control
P.Legislation	O.Config_Protection, O.Sec_Env
P.Marking	O.Flow_Control
P.Password	O.Sec_Env
P.Sec_Label_Attributes	O.Config_Protection , O.Flow_Control
TT.Admin_Err_Omit	O.Audit
TT.Audit_Trail_Loss	O.Audit

TT.Buffer_Overflow	O.Flow_Control, O.Sec_Env
TT.Exploit_Vuln	O.Sec_Env
TT.Hack_AC	O.Audit, O.Flow_Control
TT.Hack_Masq	O.Audit
TT.Flow_Control_Policy_Violation	O.Config_Protection, O.Flow_Control
Security Objectives for the Environment	
A.Acc_to_Comms	OE.Access_Control, OE.Inst_Env
A.Auth_Sys_Admin	OE.Access_Control, OE.Event_Log
A.Certified_FW	OE.Inst_Env
A.Certified_OS	OE.Inst_Env
A.Competent_Admin	OE.Access_Control, OE.Event_Log
A.Competent_User	OE.Access_Control, OE.Event_Log
A.Connection	OE.Inst_Env
A.No_Abuse_By_Admin	OE.Access_Control, OE.Event_Log
A.Physical Location	OE.Inst_Env
A.Remote_Admin	OE.Access_Control, OE.Event_Log
P.Accountability	OE.Access_Control, OE.Event_Log
P.Audit	OE.Event_Log
P.Authorities	OE.Event_Log
P.Inforsec	OE.Inst_Env
P.Legislation	OE.Inst_Env
TE.Admin_Err_Omit	OE.Event_Log, OE.Inst_Env
TE.Audit_Trail_Loss	OE.Event_Log
TE.Exploit_Vuln	OE.Access_Control, OE.Event_Log,

	OE.Inst_Env
TE.Hack_AC	OE.Access_Control, OE.Event_Log, OE.Inst_Env
TE.Hack_Masq	OE.Event_Log

Table 9 Mapping assumptions, policies and threats to Security Objectives

Objectives	**Assumptions/Policy/Threat**
Security Objectives for the TOE	
O.Audit	P.Accountability, P.Audit, P.Authorities, TT.Admin_Err_Omit, TT.Audit_Trail_Loss, TT.Hack_AC, TT.Hack_Masq
O.Config_Protection	P.Authorities, P.Infosec, P.Information_AC, P.Legislation, P.Sec_Label_Attributes, TT.Flow_Control_Policy_Violation
O.Flow_Control	P.Authorized_Use, P.Information_AC, P.Marking, P.Sec_Label_Attributes , TT.Buffer_overflow, TT.Hack_AC, TT.Flow_Control_Policy_Violation
O.Sec_Env	P.Infosec, P.Implementation, P.Legislation, P.Password, TT.Buffer_Overflow, TT.Exploit_Vuln
Security Objectives for the Environment	
OE.Access_Control	A.Acc_to_Comms, A.Auth_Sys_Admin, A.Competent_Admin, A.Competent_User, A.No_Abuse_By_Admin, A.Remote_Admin, P.Accountability, TE.Exploit_Vuln, TE.Hack_AC
OE.Event_Log	A.Auth_Sys_Admin, A.Competent_Admin, A.Competent_User, A.No_Abuse_By_Admin, A.Remote_Admin, P.Accountability, P.Audit, P.Authorities, TE.Admin_Err_Omit, TE.Audit_Trail_Loss, TE.Exploit_Vuln, TE.Hack_AC, TE.Hack_Masq
OE.Inst_Env	A.Acc_to_Comms, A.Certified_FW, A.Certified_OS, A.Connection, A.Physical_Location, P.Infosec, P.Legislation, TE.Admin_Err_Omit, TE.Exploit_Vuln, TE.Hack_AC

Table 10 Tracing of Security Objectives to assumptions, policies and threats

8.1.1 Assumptions

A.Acc_to_Comms: Physical protection of communications
It is assumed that the physical protection of the communications to the system is adequate to guard against unauthorized access or malicious modification by users. The physical protection shall be according to P.Legislation and P.Infosec for the adequate classification levels.

In General, A.Acc_to_Comms is addressed by:

OE.Access_Control Access Control
Access control shall be performed in the environment before users and system administrators are given access to the XFER Service

OE.Inst_Env Installation Environment
The TOE shall be installed in a secure physical and logical environment.

A.Auth_Sys_Admin: Authenticated administrators
It is assumed that system Administrators are authenticated and held accountable for their actions.

In General, A.Auth_Sys_Admin is addressed by:

OE.Access_Control Access Control
Access control shall be performed in the environment before users and system administrators are given access to the XFER Service

OE.Event_Log Event log
The environment shall perform audit to Event log and Schedlgu.txt.

A.Certified_FW: Certified firewall
The TOE shall use a firewall certified at an EAL equal to or higher than the TOE. All communication between the partitions shall be mediated by this firewall.
The FW shall be configured according to NSM's guidances – [21, 22, 23, 26]. The patch policy for the TOE environment must be sufficient for stopping all known, public available vulnerabilities in the TOE environment software.

In General, A.Certified_FW is addressed by:

OE.Inst_Env Installation Environment
The TOE shall be installed in a secure physical and logical environment.

A.Certified_OS: Certified operation system
It is assumed that the TOE shall run under an OS certified at an EAL equal to or higher than the TOE. The OS shall be configured according to NSM's guidances - [21, 22, 23, 26]
The patch policy for the TOE environment must be sufficient for stopping all known, public available vulnerabilities in the TOE environment software.

In General, A.Certified_OS is addressed by:

OE.Inst_Env Installation Environment
The TOE shall be installed in a secure physical and logical environment.

A.Competent_Admin: Competent System Administrators
It is assumed that system Administrators have been given training and are competent to manage the TOE and the security of the information it contains.

In General, A.Competent_Admin is addressed by:

OE.Access_Control Access Control
Access control shall be performed in the environment before users and system administrators are given access to the XFER Service

OE.Event_Log Event log
The environment shall perform audit to Event log and Schedlgu.txt.

A.Competent_User Competent Users

Users have been given training and are competent to use the TOE.

In General, A.Competent_User is addressed by:

OE.Access_Control Access Control
Access control shall be performed in the environment before users and system administrators are given access to the XFER Service

OE.Event_Log Event log
The environment shall perform audit to Event log and Schedlgu.txt.

A.Connection: No unauthorized connection to public networks
The TOE and TOE environment shall not have any connections, directly or indirectly, to unclassified and/or public networks, which not specifically are approved by NSM

In General, A.Connection is addressed by:

OE.Inst_Env Installation Environment
The TOE shall be installed in a secure physical and logical environment.

A.No_Abuse_By_Admin: No abusive System Administrators
It is assumed that the system Administrators can be trusted not to abuse their authority.

In General, A.No_Abuse_By_Admin is addressed by:

OE.Access_Control Access Control
Access control shall be performed in the environment before users and system administrators are given access to the XFER Service

OE.Event_Log Event log
The environment shall perform audit to Event log and Schedlgu.txt.

A.Physical_Location Secure physical location

The TOE shall be installed in a secure physical location in accordance with P.Legislation and P.Infosec.

In General, A.Physical_Location is addressed by:

OE.Inst_Env Installation Environment
The TOE shall be installed in a secure physical and logical environment.

A.Remote_Admin: Remote administration
It is assumed that system Administrators shall have remote access and are able to view and modify security-relevant data.

In General, A.Remote_Admin is addressed by:

OE.Access_Control Access Control
Access control shall be performed in the environment before users and system administrators are given access to the XFER Service

OE.Event_Log Event log
The environment shall perform audit to Event log and Schedlgu.txt.

8.1.2 Policies

8.1.2.1 Policies addressed in TOE

P.Accountability: Individual accountability
Individuals shall be held accountable for their actions. The policy emphasizes the need for personal user accounts for users and administrators.

In General, P.Accountability is addressed by:

O.Audit: Audit records with identity
The TOE shall perform audit to Content Archive and initiate audit to Event log and Schedlgu.txt.

P.Audit: Audit review
The TOE shall generate daily and weekly reports showing number of files and volume of files transferred during the period:
- To high and low partitions
- To high and low partitions - summarized per user
- To low partition - summarized per release marking
- Number of files and volume of files transferred per direction per release marking per user

The audit log shall be reviewed to monitor the use of the XFER Service. If the audit review detects abnormal activities, the XFER Service Auditor shall perform system shutdown.

In General, P.Audit is addressed by:

O.Audit: Audit records with identity
The TOE shall perform audit to Content Archive and initiate audit to Event log and Schedlgu.txt.

P.Authorities: Notification of threats and vulnerabilities
Appropriate authorities shall be immediately notified of any threats or vulnerabilities impacting systems that process their data.

In General, P.Authorities is addressed by:

O.Audit: Audit records with identity
The TOE shall perform audit to Content Archive and initiate audit to Event log and Schedlgu.txt.

O.Config_Protection Protection of flow control security configuration
Configuration of the flow control security parameters shall be protected from manipulation by unauthorised personnel.

P.Authorized_Use: Authorized use of information
Information shall be used only for its authorized purpose(s).

In General, P.Authorized_Use is addressed by:

O.Flow_Control: Flow control between partitions
The TOE shall perform a flow control to ensure that the file transfer between partitions is according to flow control policy for file transfer. Filtering rules and security label in the flow control policy can only be configured by XFER Service Enterprise Admins.

P.Infosec: C-M(2002)49
The TOE and its environment are compliant with the NATO security policy as stated in C-M(2002)49 Enclosure F [6], AC/35-D/2004 [24] and AC/35-D/2005 [25]. The policy emphasizes the need for configuring and installing the TOE according to its NATO security classification.

In General, P.Infosec is addressed by:

O.Config_Protection Protection of flow control security configuration
Configuration of the flow control security parameters shall be protected from manipulation by unauthorised personnel.

O.Sec_Env: Secure environment
The TOE shall verify the configuration of the TOE environment to secure that the TOE is operating in a secure environment. This is done by a verification script. This script is derived from requirements in I-02 [26] and will run continually or can be initiated by XFER Service Admins. If any errors are found, the script will log the error and perform shutdown of the XFER services. A restart of the XFER Service will require intervention by system administrator.

P.Implementation: Implementation of the TOE
Each transfer process shall be implemented as Win32 service and run under a distinct account. The policy emphasizes the need for protecting the processes from unauthorised users.

In General, P.Implementation is addressed by:

O.Sec_Env: Secure environment
The TOE shall verify the configuration of the TOE environment to secure that the TOE is operating in a secure environment. This is done by a verification script. This script is derived from requirements in I-02 [26] and will run continually or can be initiated by XFER Service Admins. If any errors are found, the script will log the error and perform shutdown of the XFER services. A restart of the XFER Service will require intervention by system administrator.

P.Information_AC: Information access control
Information shall be accessed only by authorized individuals and processes.

In General, P.Information_AC is addressed by:

O.Config_Protection Protection of flow control security configuration
Configuration of the flow control security parameters shall be protected from manipulation by unauthorised personnel.

O.Flow_Control: Flow control between partitions
The TOE shall perform a flow control to ensure that the file transfer between partitions is according to flow control policy for file transfer. Filtering rules and security label in the flow control policy can only be configured by XFER Service Enterprise Admins.

P.Legislation: The Norwegian Security Act
The TOE and its environment are compliant with The Norwegian Security Act (Sikkerhetsloven) [4] with supportive Directive on information security (Forskrift om informasjonssikkerhet) [5]. The policy emphasizes the need for configuring and installing the TOE according to its national security classification.

In General, P.Legislation is addressed by:

O.Config_Protection Protection of flow control security configuration
Configuration of the flow control security parameters shall be protected from manipulation by unauthorised personnel.

O.Sec_Env: Secure environment
The TOE shall verify the configuration of the TOE environment to secure that the TOE is operating in a secure environment. This is done by a verification script. This script is derived from requirements in I-02 [26] and will run continually or can be initiated by XFER Service Admins. If any errors are found, the script will log the error and perform shutdown of the XFER services. A restart of the XFER Service will require intervention by system administrator.

P.Marking: Information marking
Information shall be appropriately marked and labelled. The policy emphasizes the need for correct marking of the security classification of the files to perform the flow control.

In General, P.Marking is addressed by:

O.Flow_Control: Flow control between partitions
The TOE shall perform a flow control to ensure that the file transfer between partitions is according to flow control policy for file transfer. Filtering rules and security label in the flow control policy can only be configured by XFER Service Enterprise Admins.

P.Password: Different passwords in low and high partition
Users must have different passwords in low and high partitions. The policy emphasizes the need for a different password in the high partition in case of compromising the password in the low partition.

In General, P.Password is addressed by:

O.Sec_Env: Secure environment
The TOE shall verify the configuration of the TOE environment to secure that the TOE is operating in a secure environment. This is done by a verification script. This script is derived from requirements in I-02 [26] and will run continually or can be initiated by XFER Service Admins. If any errors are found, the script will log the error and perform shutdown of the XFER services. A restart of the XFER services will require intervention by system administrator.

P.Sec_Label_Attributes Security label attributes

Security label attributes according to flow control policy can only be configured in the TOE by XFER Service Enterprise Admins.

In General, P.Password is addressed by:

O.Config_Protection Protection of flow control security configuration
Configuration of the flow control security parameters shall be protected from manipulation by unauthorised personnel.

O.Flow_Control:	Flow control between partitions
The TOE shall perform a flow control to ensure that the file transfer between partitions is according to flow control policy for file transfer. Filtering rules and security label in the flow control policy can only be configured by XFER Service Enterprise Admins.

8.1.2.2 Policies addressed in TOE environment

**P.Accountability:	Individual accountability**
Individuals shall be held accountable for their actions. The policy emphasizes the need for personal user accounts for users and administrators.

In General, P.Accountability is addressed by:

OE.Access_Control	Access Control
Access control shall be performed in the environment before users and system administrators are given access to the XFER Service

OE.Event_Log	Event log
The environment shall perform audit to Event log and Schedlgu.txt.

**P.Audit:	Audit review**
The TOE shall generate daily and weekly reports showing number of files and volume of files transferred during the period:
- To high and low partitions
- To high and low partitions - summarized per user
- To low partition - summarized per release marking
- Number of files and volume of files transferred per direction per release marking per user

The audit log shall be reviewed to monitor the use of the XFER Service. If the audit review detects abnormal activities, the XFER Service Auditor shall perform system shutdown.

In General, P.Audit is addressed by:

OE.Event_Log	Event log
The environment shall perform audit to Event log and Schedlgu.txt.

**P.Authorities:	Notification of threats and vulnerabilities**
Appropriate authorities shall be immediately notified of any threats or vulnerabilities impacting systems that process their data.

In General, P.Authorities is addressed by:

OE.Event_Log	Event log
The environment shall perform audit to Event log and Schedlgu.txt.

**P.Infosec:	C-M(2002)49**
The TOE and its environment are compliant with the NATO security policy as stated in C-M(2002)49 Enclosure F [6], AC/35-D/2004 [24] and AC/35-D/2005 [25]. The policy emphasizes the need for configuring and installing the TOE according to its NATO security classification.

In General, P.Infosec is addressed by:

OE.Inst_Env	Installation Environment
The TOE shall be installed in a secure physical and logical environment.

P.Legislation: The Norwegian Security Act
The TOE and its environment are compliant with The Norwegian Security Act (Sikkerhetsloven) [4] with supportive Directive on information security (Forskrift om informasjonssikkerhet) [5]. The policy emphasizes the need for configuring and installing the TOE according to its national security classification.

In General, P.Legislation is addressed by:

OE.Inst_Env Installation Environment
The TOE shall be installed in a secure physical and logical environment.

8.1.3 Threats

8.1.3.1 Threats addressed in TOE

TT.Admin_Err_Omit: Administrative errors of omission
To meet the threat of a System Administrator that fails to perform some function essential to security it sis assumed that administrator achieve training in administrating the TOE and audit will be activated in the TOE and TOE environment to monitor the TOE.

In General, TT.Admin_Err_Omit is addressed by:

O.Audit: Audit records with identity
The TOE shall perform audit to Content Archive and initiate audit to Event log and Schedlgu.txt.

TT.Audit_Trail_Loss: Loss of audit trail
To meet the threat of loss of audit trail (Content Archive), the TOE will perform shut down if audit is not possible.

In General, TT.Audit_Trail_Loss is addressed by:

O.Audit: Audit records with identity
The TOE shall perform audit to Content Archive and initiate audit to Event log and Schedlgu.txt.

TT.Buffer_overflow: User creates buffer overflow
To meet the threat of a user creating a path too long for MS Windows or a file with large alternate streams, or with a large number of alternate streams causing the service to run out of heap memory, the service will shut down if it runs out of heap memory. The TOE will only accept file transferred according to flow control policy.

In General, TT.Buffer_Overflow is addressed by:

O.Sec_Env: Secure environment
The TOE shall verify the configuration of the TOE environment to secure that the TOE is operating in a secure environment. This is done by a verification script. This script is derived from requirements in I-02 [26] and will run continually or can be initiated by XFER Service Admins. If any errors are found, the script will log the error and perform shutdown of the XFER services. A restart of the XFER services will require intervention by system administrator.

O.Flow_Control: Flow control between partitions
The TOE shall perform a flow control to ensure that the file transfer between partitions is according to flow control policy for file transfer. Filtering rules and security label in the flow control policy can only be configured by XFER Service Enterprise Admins.

TT.Exploit_vuln: Hacker exploits vulnerability
To meet the threat of a hacker that tries to exploit a vulnerability in the TOE to get unauthorised access to information, a verification script will be run periodically to ensure that the configuration of the TOE-environment is according to defined security requirements. If any errors are found, the script will perform shutdown of the XFER services.

In General, TT.Exploit_vuln is addressed by:

O.Sec_Env: Secure environment
The TOE shall verify the configuration of the TOE environment to secure that the TOE is operating in a secure environment. This is done by a verification script. This script is derived from requirements in I-02 [26] and will run continually or can be initiated by XFER Service Admins. If any errors are found, the script will log the error and perform shutdown of the XFER services. A restart of the XFER services will require intervention by system administrator.

TT.Hack_AC: Hacker gains undetected system access
To meet the threat of a hacker that gains undetected access to TOE due to missing, weak and/or incorrectly implemented access rights causing potential violations of integrity, confidentiality, or availability audit will be activated in the TOE and TOE environment to monitor the TOE.

In General, TT.Hack_AC is addressed by:

O.Audit: Audit records with identity
The TOE shall perform audit to Content Archive and initiate audit to Event log and Schedlgu.txt.

O.Flow_Control: Flow control between partitions
The TOE shall perform a flow control to ensure that the file transfer between partitions is according to flow control policy for file transfer. Filtering rules and security label in the flow control policy can only be configured by XFER Service Enterprise Admins.

TT.Hack_Masq: Hacker masquerading as a legitimate system process
To meet the threat of a hacker masquerades as a system process to perform illegal operations, audit will be activated in the TOE and TOE environment to monitor the TOE.

In General, TT.Hack_Masq is addressed by:

O.Audit: Audit records with identity
The TOE shall perform audit to Content Archive and initiate audit to Event log and Schedlgu.txt.

TT.Flow_Control_Policy_Violation: Flow control policy violation
To meet the threat of an unauthorized user or system administrator changing the configuration of the XFER Service causing violation of the TOE transfer policy, the possibility to change the configurable parameters of the flow control policy is restricted to the XFER Service Enterprise Admins.

In General, TT.Flow_Control_Policy_Violation is addressed by:

O.Config_Protection Protection of flow control security configuration
Configuration of the flow control security parameters shall be protected from manipulation by unauthorised personnel.

O.Flow_Control: Flow control between partitions
The TOE shall perform a flow control to ensure that the file transfer between partitions is

according to flow control policy for file transfer. Filtering rules and security label in the flow control policy can only be configured by XFER Service Enterprise Admins.

8.1.3.2 Threats addressed in TOE environment

TE.Admin_Err_Omit: Administrative errors of omission
To meet the threat of system Administrator that fails to perform functions essential to security it is an assumption that the system administrators have received the appropriate training. Audit will be activated in the TOE and the TOE environment to monitor the TOE.

In General, TE.Admin_Err_Omit is addressed by:

OE.Event_Log Event log
The environment shall perform audit to Event log and Schedlgu.txt.

OE.Inst_Env Installation Environment
The TOE shall be installed in a secure physical and logical environment.

TE.Audit_Trail_Loss: Loss of audit trail
To meet the threat of loss of audit trail (Event log) the TOE will perform shut down if audit is not possible.

In General, TE.Audit_Trail_Loss is addressed by:

OE.Event_Log Event log
The environment shall perform audit to Event log and Schedlgu.txt.

TE.Exploit_Vuln: Hacker exploits vulnerability
To meet the threat of a hacker that tries to exploit a vulnerability in the IT-environment to get unauthorised access to information audit will be activated in the TOE and TOE environment to monitor the TOE.

In General, TE.Exploit_Vuln is addressed by:

OE.Access_Control Access Control
Access control shall be performed in the environment before users and system administrators are given access to the XFER Service

OE.Event_Log Event log
The environment shall perform audit to Event log and Schedlgu.txt.

OE.Inst_Env Installation Environment
The TOE shall be installed in a secure physical and logical environment.

TE.Hack_AC: Hacker gains undetected system access
To meet the threat of a hacker that gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability audit will be activated in the TOE and TOE environment to monitor the TOE.

In General, TE.Hack_AC is addressed by:

OE.Access_Control Access Control
Access control shall be performed in the environment before users and system administrators are given access to the XFER Service

OE.Event_Log Event log
The environment shall perform audit to Event log and Schedlgu.txt.

OE.Inst_Env Installation Environment
The TOE shall be installed in a secure physical and logical environment.

TE.Hack_Masq: Hacker masquerading as a legitimate user
To meet the threat of a hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process, audit will be activated in the TOE environment to monitor the TOE.

In General, TE.Hack_Masq is addressed by:

OE.Event_Log Event log
The environment shall perform audit to Event log and Schedlgu.txt.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the requirements in the ST. The section demonstrates that the security objectives identified in Section 4 is met by the set of security functional requirements identified in Section 5.

8.2.1 Functional Security Requirements Rationale for TOE

The functional requirements are chosen from CC part 2 based on requirements from NSM documented in I-02 [26]. The requirements given in I-02 [26] are considered to be complete and suitable to meet the objectives for the file transfer service.

Objectives	Requirements
O.Audit	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.2, FAU_STG.3, FPT_RCV.1, FPT_RVM.1, FPT_STM.1,
O.Config_Protection	FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1
O.Flow_Control	FDP_IFC.2, FDP_IFF.1, FPT_FLS.1, FPT_RCV.1, FPT_RVM.1, FRU_FLT.1,
O.Sec_Env	FPT_AMT.1, FPT_RCV.1, FPT_RVM.1, FPT_SEP.1

Table 11 Security Objective to Functional requirement Mapping

O.Audit: Audit records with identity
The TOE will perform audit data generation to Content Archive and initiate audit data generation to Event log and Schedlgu.txt. To achieve O.Audit, the audit data will be associated to user identity, and review will be restricted to XFER server auditors. If audit data generation can't be performed, the TOE will perform shut down. Audit will be implemented in the TOE by SF.Audit, Time stamp of audit data will be implemented in the TOE by SF.Time_Stamp. Shut down of the TOE will be implemented by SF.Shut_Down.

O.Audit is implemented in the TOE by:

1. FAU_GEN.1: Audit data generation
2. FAU_GEN.2: User identity association

3.	FAU_SAR.1:	Audit review
4.	FAU_SAR.2:	Restricted audit review
5.	FAU_STG.2:	Guarantees of audit data availability
6.	FAU_STG.3:	Action in case of possible audit data loss
7.	FPT_RCV.1	Manual recovery
8.	FPT_RVM.1:	Non-bypassability of the TSP
9.	FPT_STM.1:	Reliable time stamps

O.Config_Protection: Protection of flow control security configuration
Configuration of the flow control security parameters shall be protected from manipulation by unauthorised personnel. Security management and configuration of the flow control security parameters will be implemented in the TOE by SF.Security_Management.

O.Config_Protection is implemented in the TOE by:

1.	FMT_MSA.1:	Management of security attributes
2.	FMT_MSA.3:	Static attribute initialisation
3.	FMT_MTD.1	Management of TSF data
4.	FMT_SMF.1:	Specification of management functions

O.Flow_Control: Flow control between partitions
The TOE shall perform a flow control to ensure that the file transfer between partitions is according to flow control policy for file transfer. Filtering rules and security label in the flow control policy can only be configured by XFER Service Enterprise Admins. To achieve O.Flow_Control, the flow control policy is secure by default (everything blocked), and any file type and labelling that should be allowed to be transferred must be explicitly specified in the flow control policy. Configuration of the flow control policy is restricted to the XFER Enterprice Admins. The flow control is implemented in the TOE by SF.Flow_Control.. The TOE is fault tolerant to defined failures. Fault tolerance is implemented in the TOE by SF.Fault_Tolerance.

O.Flow_Control is implemented in the TOE by:

1.	FDP_IFC.2:	Complete information flow control
2.	FDP_IFF.1:	Simple security attributes
3.	FPT_FLS.1:	Failure with preservation of secure state
4.	FPT_RCV.1:	Manually recovery
5.	FPT_RVM.1:	Non-bypassability of the TSP
6.	FRU_FLT.1:	Degraded fault tolerance

O.Sec_Env: Secure environment
The TOE shall verify the specified configuration of the TOE environment to secure that the TOE is operating in a secure environment. To achieve O.Sec_Env, the TOE will enforce domain separation between the TOE and the two partitions. Domain separation is implemented SF.Domain_Separation. The TOE will run a script to verify the configuration of the TOE environment, this script is derived from requirements in I-02 [26] and will run continually or can be initiated by XFER Service Admins. Verification of the TOE environment will be implemented in the TOE by SF.OS_Verification. If the script detects mismatch between the actual configuration of the TOE environment compared to the defined baseline, the TOE will perform system shut down. System shut down is implemented in the TOE by SF.Shut_Down. A restart of the XFER services will require intervention by system administrator.

O.Sec_Env is implemented in the TOE by:

1.	FPT_AMT.1:	Abstract machine testing
2.	FPT_RCV.1	Manual recovery
3.	FPT_RVM.1:	Non-bypassability of the TSP

4. FPT_SEP.1: TSF domain separation

8.2.2 Security requirements rationale for the TOE environment

Objectives	Requirements
OE.Access_Control	FDP_ACC.2, FDP_ACF.1, FIA_UAU.2, FIA_UID.2, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1
OE.Event_Log	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FMT_SMF.1
OE.Inst_Env	ADO_IGS.1, AGD_ADM.1, AGD_USR.1, ALC_DVS.1

Table 12 Security Objective for TOE environment to security requirement for the IT environment mapping

OE.Access_Control Access Control
Access control shall be performed and managed in the environment. Access control shall be enforced on all users and system administrators before they are given access to the objects within the XFER Service.

OE.Access_Control is implemented in the environment by:

1.	FDP_ACC.2	Complete access control
2.	FDP_ACF.1	Security attribute based access control
3.	FIA_UAU.2	User authentication before any action
4.	FIA_UID.2	User identification before any action
5.	FMT_MSA.1	Management of security attributes
6.	FMT_MSA.3	Static attribute initialisation
7.	FMT_SMF.1	Specification of management functions
8.	FMT_SMR.1	Security roles

OE.Event_Log Event log
The environment shall perform audit to Event log and Schedlgu.txt.

OE.Event_Log is implemented in the environment by:

1.	FAU_GEN.1	Audit data generation
2.	FAU_GEN.2	User identity association
3.	FAU_SAR.1	Audit review
4.	FAU_SAR.2	Restricted audit review
5.	FMT_SMF.1	Specification of management functions

OE.Inst_Env Installation Environment
The TOE shall be installed in a secure physical and logical environment.

OE.inst_Env is implemented in the environment by:

1.	ADO_IGS.1	Installation, generation, and start-up procedures
2.	AGD_ADM.1	Administrator guidance
3.	AGD_USR.1	User guidance
4.	ALC_DVS.1	Identification of security measures

8.2.3 Assurance Security Requirements Rationale

This ST contains the assurance requirements from the CC EAL4 assurance package. The TOE is initially built to satisfy NSM's requirements for a HEMMELIG / NATO SECRET system which operates in a Partitioned mode of operation. The requirement of critical parts of such systems is on EAL4. Communication between these two partitions (HEMMELIG and NATO SECRET)) is a critical part, which demands EAL4. The underlying operating system and the firewall between the two segments are both EAL4 certified. In order to have the same trust in the file transfer mechanism, EAL4 is demanded.

8.3 Dependency Rationale

Requirement	Dependencies	Dependencies Included	Dependencies covered by
Functional Requirements			
FAU_GEN.1	FPT_STM.1	Yes	
FAU_GEN.2	FAU_GEN.1	Yes	
	FIA_UID.1	No	FIA_UID.2
FAU_SAR.1	FAU_GEN.1	Yes	
FAU_SAR.2	FAU_SAR.1	Yes	
FAU_STG.2	FAU_GEN.1	Yes	
FAU_STG.3	FAU_STG.1	No	FAU_STG.2
FDP_ACC.2	FDP_ACF.1	Yes	
FDP_ACF.1	FDP_ACC.1	No	FDP_ACC.2
	FMT_MSA.3	Yes	
FDP_IFC.2	FDP_IFF.1	Yes	
FDP_IFF.1	FDP_IFC.1	No	FDP_IFC.2
	FMT_MSA.3	Yes	
FIA_UAU.2	FIA_UID.1	No	FIA_UID.2
FIA_UID.2	None		
FMT_MSA.1	FDP_IFC.1	No	FDP_IFC.2
	FMT_SMF.1	Yes	
	FMT_SMR.1	Yes	
FMT_MSA.3	FMT_MSA.1	Yes	

	FMT_SMR.1	Yes	
FMT_MTD.1	FMT_SMF.1	Yes	
	FMT_SMR.1	Yes	
FMT_SMF.1	None		
FMT_SMR.1	FIA_UID.1	No	FIA_UID.2
FPT_AMT.1	None		
FPT_FLS.1	ADV_SPM.1	Yes	
	AGD_ADM.1	Yes	
FPT_RCV.1	ADV_SPM.1	Yes	
	AGD_ADM.1	Yes	
FPT_RVM.1	None		
FPT_SEP.1	None		
FPT_STM.1	None		
FRU_FLT.1	FPT_FLS.1	Yes	
Assurance Requirements			
ACM_AUT.1	ACM_CAP.3	No	ACM_CAP.4
ACM_CAP.4	ACM_SCP.1	No	ACM_SCP.2
	ALC_DVS.1	Yes	
ACM_SCP.2	ACM_CAP.3	No	ACM_CAP.4
ADO_DEL.2	ACM_CAP.3	No	ACM_CAP.4
ADO_IGS.1	AGD_ADM.1	Yes	
ADV_FSP.2	ADV_RCR.1	Yes	
ADV_HLD.2	ADV_FSP.1	No	ADV_FSP.2
	ADV_RCR.1	Yes	
ADV_IMP.1	ADV_LLD.1	Yes	
	ADV_RCR.1	Yes	
	ALC_TAT.1	Yes	
ADV_LLD.1	ADV_HLD.2	Yes	

	ADV_RCR.1	Yes	
ADV_RCR.1	None		
ADV_SPM.1	ADV_FSP.1	No	ADV_FSP.2
AGD_ADM.1	ADV_FSP.1	No	ADV_FSP.2
AGD_USR.1	ADV_FSP.1	No	ADV_FSP.2
ALC_DVS.1	None		
ALC_LCD.1	None		
ALC_TAT.1	ADV_IMP.1	Yes	
ATE_COV.2	ADV_FSP.1	No	ADV_FSP.2
	ATE_FUN.1	Yes	
ATE_DPT.1	ADV_HLD.1	No	ADV_HLD.2
	ATE_FUN.1	Yes	
ATE_FUN.1	None		
ATE_IND.2	ADV_FSP.1	No	ADV_FSP.2
	AGD_ADM.1	Yes	
	AGD_USR.1	Yes	
	ATE_FUN.1	Yes	
AVA_MSU.2	ADO_IGS.1	Yes	
	ADV_FSP.1	No	ADV_FSP.2
	AGD_ADM.1	Yes	
	AGD_USR.1	Yes	
AVA_SOF.1	ADV_FSP.1	No	ADV_FSP.2
	ADV_HLD.1	No	ADV_HLD.2
AVA_VLA.2	ADV_FSP.1	No	ADV_FSP.2
	ADV_HLD.2	Yes	
	ADV_IMP.1	Yes	
	ADV_LLD.1	Yes	
	AGD_ADM.1	Yes	

	AGD_USR.1	Yes	

Table 13 Functional and Assurance Requirements Dependencies

8.4 Security Functional Requirements Grounding in Objectives

This section provides evidence supporting the internal consistency and completeness of the requirements in the ST. The section demonstrates that the set of security functional requirements identified in Section 5 are suitable to meet the security objectives identified in Section 4.

Requirements	Objectives
FAU_GEN.1	O.Audit, OE.Event_Log
FAU_GEN.2	O.Audit, OE.Event_Log
FAU_SAR.1	O.Audit, OE.Event_Log
FAU_SAR.2	O.Audit, OE.Event_Log
FAU_STG.2	O.Audit
FAU_STG.3	O.Audit
FDP_ACC.2,	OE.Access_Control
FDP_ACF.1	OE.Access_Control
FDP_IFC.2	O.Flow_Control
FDP_IFF.1	O.Flow_Control
FIA_UAU.2	OE.Access_Control
FIA_UID.2	OE.Access_Control
FMT_MSA.1	O.Config_Protection, OE.Access_Control
FMT_MSA.3	O.Config_Protection, OE.Access_Control
FMT_MTD.1	O.Config_Protection
FMT_SMF.1	O.Config_Protection, OE.Access_Control, OE.Event_Log
FMT_SMR.1	OE.Access_Control
FPT_AMT.1	O.Sec_Env
FPT_FLS.1	O.Flow_Control
FPT_RCV.1	O.Audit, O.Flow_Control, O.Sec_Env

FPT_RVM.1	O.Audit, O.Sec_Env, O.Flow_Control
FPT_SEP.1	O.Sec_Env
FPT_STM.1	O.Audit
FRU_FLT.1	O.Flow_Control

Table 14 Requirements to Objectives Mapping

8.5 TOE Summary Specification Rationale

This section shows how the TOE security functions satisfy the security function requirements.

TOE Security Functions	Requirement	Implementation description
SF.Audit	FAU_GEN.1	The XFER services are shut down if audit generation fails (for example if audit generation is shut down). Audit generation is performed at start-up and shut-down of the XFER services. File transfer is audited in Content Archive and Event log. Audit generation is performed using MS Windows audit functions.
	FAU_GEN.2	Audit of file transfer is identified by the SID of the file owner. Audit of start up and shut down of the XFER services is identified by user-ID of the user that performs the operation
	FAU_SAR.1	MS Windows access control is used to grant access to Event log, Schedlgu.txt and Content Archive to XFER Service Auditors and XFER Service Admins.
	FAU_SAR.2	MS Windows access control is used to prohibit all users read access to Event log, Schedlgu.txt and Content Archive except those users described in FAU_SAR.1
	FAU_STG.2	Event log configuration is set to “do not overwrite events”. Shut down of the XFER services is performed if the Event log or write to Content Archive fails.
	FAU_STG.3	Shut down of the XFER services is performed if the Event log or write to Content Archive fails.
SF.Flow_Control	FDP_IFC.2	Flow control policy is implemented as functionality in the XFER services. It is not possible to turn off the flow control policy using configuration.

TOE Security Functions	Requirement	Implementation description
	FDP_IFF.1	Flow control policy is implemented as functionality in the XFER services. Additional flow control policies are not allowed.
SF.Security_Management	FMT_MSA.1	Registry key is protected with MS Windows access control.
	FMT_MSA.3	MS Windows access control is used to set restrictive default values on the security attributes.
	FMT_MTD.1	MS Windows access control is used to restrict access to the security attributes only to XFER Service Enterprise Admins and XFER Service.
	FMT_SMF.1	The XFER Service will contain security management functions for starting script for creating and deleting user transfer areas, start of script for verifying the configuration of the TOE environment, modify the flow control policy, modify the configuration file for the configuration and the verification scripts, changing the password for the user accounts that the configuration and/or verification script uses to read the information from the high, low and XFER partitions domains and start and stop of the XFER Service.
SF.OS_Verification	FPT_AMT.1	Verification script will run a set of tests to demonstrate the correct operation of MS Windows.
SF.Shut_Down	FPT_RCV.1	The XFER Service will perform system shut down of the services when the specified errors occur.
	FPT_RVM.1	The XFER Service will perform system shut down of the services when the specified errors occur (FPT_RCV.1).
SF.Domain_Separation	FPT_SEP.1	MS Windows access control and installation of TOE in XFER domain.
SF.Time_Stamp	FPT_STM.1	Event log, Schedlgu.txt and Content Archive use server time stamp.
SF.Fault_Tolerance	FPT_FLS.1	The TSF shall preserve a secure state in the event of define failures.
	FRU_FLT.1	The TSF shall ensure the operation of XFER services and verification script in the event of

TOE Security Functions	Requirement	Implementation description
		defined failures.

Table 15 Security Functions to Requirements Mapping

9 References

Reference	Short title	Content
[1]	CCIMB-2004-01-001	Common Criteria for Information Technology Security Evaluation, January 2004, Version 2.2 Revision 256, Part 1
[2]	CCIMB-2004-01-002	Common Criteria for Information Technology Security Evaluation, January 2004, Version 2.2, Part 2
[3]	CCIMB-2004-01-003	Common Criteria for Information Technology Security Evaluation, January, Version 2.2 Revision 256, Part 3
[4]	LOV-1998-03-20 nr 10	Lov om forebyggende sikkerhetstjeneste (Sikkerhetsloven) (Norwegian Security Act)
[5]	FOR-2001-0701-744	Forskrift om informasjonssikkerhet (Directive on information security)
[6]	C-M(2002)49	Security policy within NATO
[7]	Usage Scenarios	Usage Scenarios according to MSF's template
[8]	Development Plan	Development Plan according to MSF's template
[9]	Test Plan	Test Plan according to MSF's template
[10]	Security Plan	Security Plan according to MSF's template
[11]	Functional Specification	Functional Specification according to MSF's template
[12]	High Level Design	High Level Design according to CC
[13]	Physical Design	Physical Design according to MSF's template
[14]	Informal correspondence demonstration	Informal correspondence demonstration
[15]	TSP model	Model of the TSP
[16]	Master Project Plan	Master Project Plan according to MSF's template
[17]		
[18]		
[19]	Subset of source code	Subset of source code according to MSF's template
[20]	User Guidance	User Guidance
[21]		
[22]		
[23]		
[24]	AC/35-D/2004	Primary Directive on Infosec
[25]	AC/35-D/2005	INFOSEC Management Directive for CIS
[26]	I-02	NSM Systems Integration Section: Windows Partitioned Mode of Operation, Implementation guidance no 2, DRAFT version 1.0
[27]	Administrator Guidance	Administration Guidance
[28]	Testing and Bug Report	Testing and Bug Report according to MSF's template
[29]	Test Specification and Test Cases	Test Specification and Test Cases according to MSF's template
[30]	Configuration List	List of configuration items for the TOE

Appendix A - Acronyms

ACL	Access Control List
CC	Common Criteria
CM	Configuration management
EAL	Evaluation Assurance Level
ID	Identification
IT	Information Technology
PP	Protection Profile
HP	High Partition
LP	Low Partition
MSF	Microsoft Solution Framework
NATO	North Atlantic Treaty Organisation
NDCISD	Norwegian Defence Communication and Information Services Division
NSM	Norwegian National Security Agency (Nasjonal sikkerhetsmyndighet)
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TA	Threat Agent
TE	Threats to the Environment
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TT	Threat to the TOE
XFER	Transfer