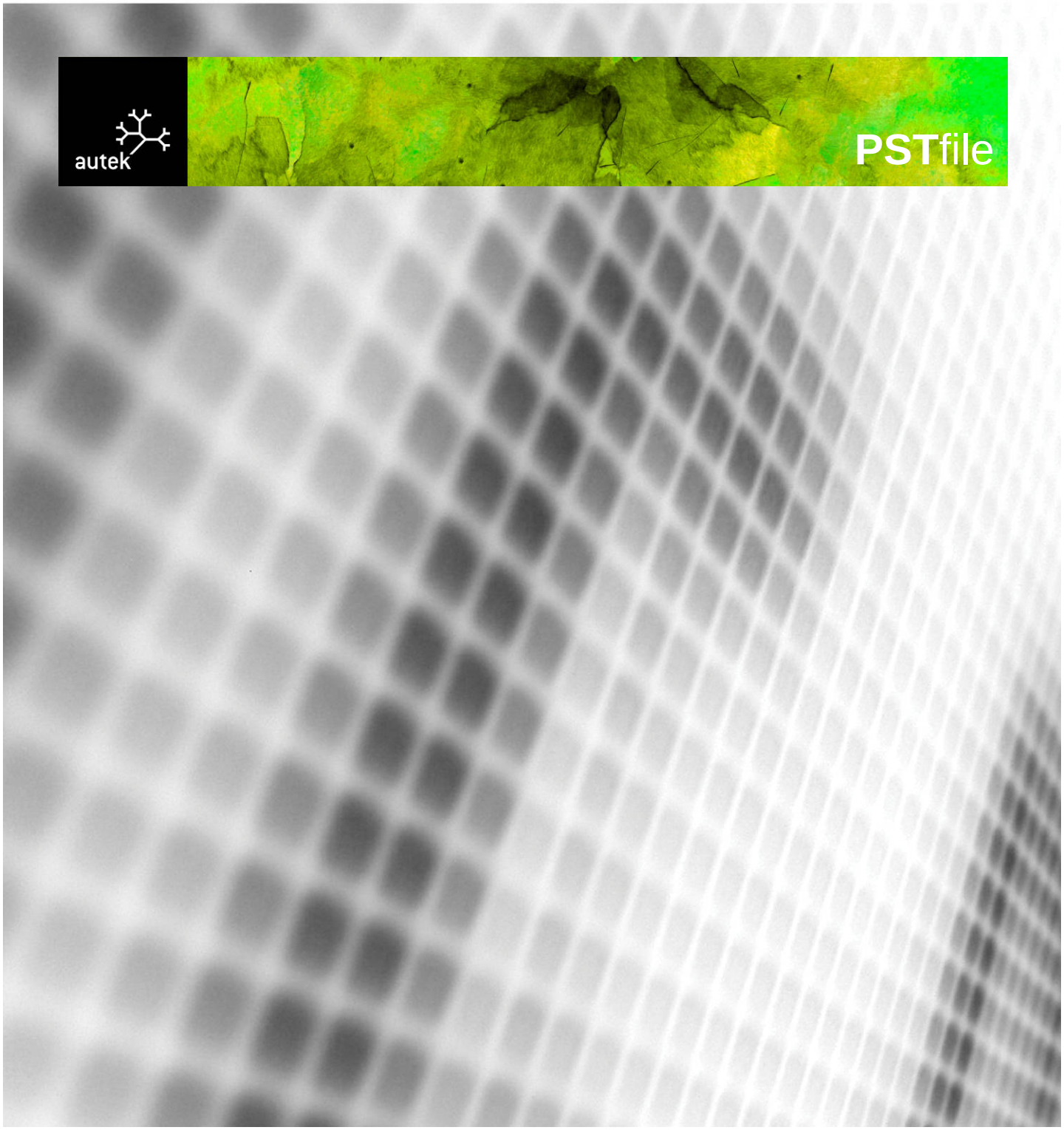

Security Target Lite

Revision 3.1

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1. Security Target Reference

1 **Title**: PSTfile Security Target

2 **Security Target version**: 3

3 **Author**: Autek Ingeniería, S.L.

4 **Security Target date**: October 7, 2013

5 **TOE name**: PSTfile

6 **TOE version**: 4.4.2

7 **Product name**: PSTfile Gateway

1.2. TOE Overview

1.2.1. TOE Usage

8 The TOE is part of a complete product called 'PSTfile Gateway'. The product is made up of two 'appliances' (including hardware, generic software (operating system) and specific software) and additional software installed on general purpose computers.

9 The TOE consists of specific software that is pre-installed on the appliances and provides the functionality of a secure application level file gateway. In addition, the TOE includes a software tool stored on an auto-start CD-ROM that allows updating of the software installed on the appliances and verifying their integrity.

10 The use of the TOE is to transfer files (FTP, FTPS and SMB file transfer protocols are supported) between two isolated networks whilst maintaining the networks in isolation and guaranteeing that the only information transferred between the networks is the one transferred by the gateway itself. To do this, the gateway discontinues the TCP/IP protocol stack at all levels.

11 The two networks are not equivalent: one is considered as having a higher security level or classification. The system is administered from the secure network which is also referred to as the internal network. Only digitally signed files will be transferred from the internal to the external network.

12 A high-availability version of the TOE exists that allows service to be maintained in the event of hardware failure. The normal configuration and the high-availability or redundant hardware configuration are described separately. Unless mentioned explicitly, documentation applies to both configurations. Sections that apply to the high-availability configuration only will state this explicitly.

13 PSTfile Gateway requires a secure use environment.

1.2.2. TOE Type

14 The TOE type is secure, application level, file gateway software.

1.3. Required Hardware and Software

15 The main part of the TOE runs on two specific servers delivered with the product. The supported version of the servers is S3 or higher. Internal units include a passive transfer device. The evaluated configuration uses a customized version of Windows Embedded Standard 2009.

16 Required hardware and software in the TOE environment:

- PSTadm administration application. A standard PC on which to install and run the administration application PSTadm is required. The minimum requirements for this PC are a processor and RAM amount sufficient to run the operating system which can be Windows XP SP3 or higher.
- PSTaud auditing service. A standard PC on which to install and run PSTaud is required. The minimum requirements for this PC are a processor and RAM amount sufficient to run the operating system which can be Windows XP SP3 or higher.
- Public Key Infrastructure (Internal network)
- Syslog server(s) (Internal network)
- ODBC accessible database server for transfers auditing (Internal network). Optionally auditing info can be stored in text files.
- File servers of supported file transfer protocols (FTP, FTPS or SMB) on both networks.

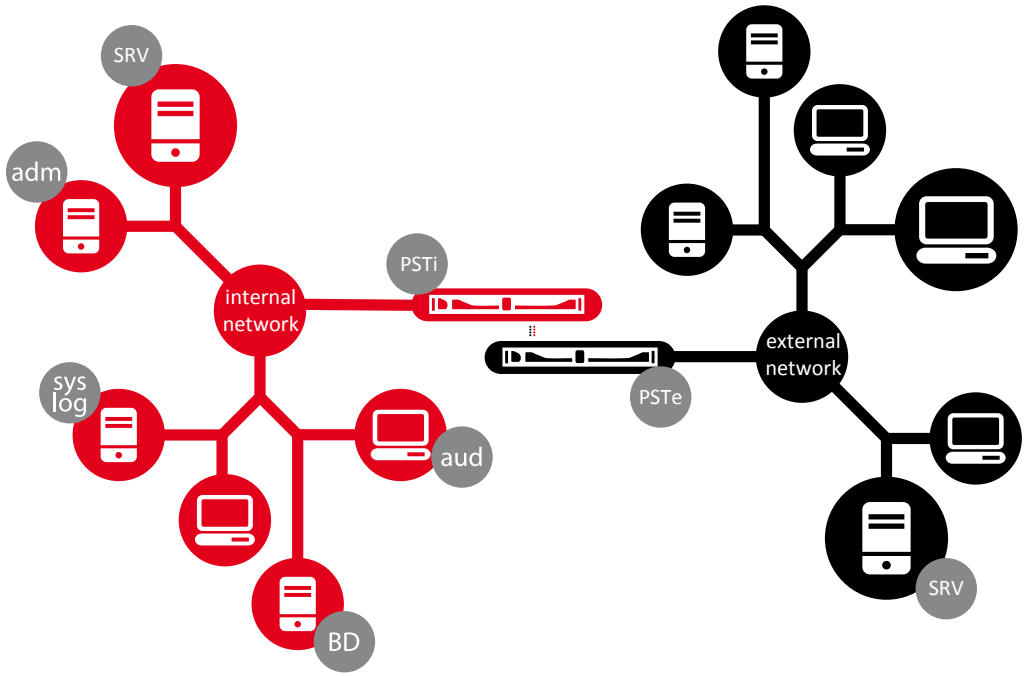

Figure 1. PSTfile environment

1.4. TOE Description

1.4.1. Physical Scope

17 The TOE is made up of specific binary software components developed by Autek Ingeniería, installed on PSTfile Gateway units together with a software tool, delivered on a bootable CD-ROM, that allows updating of the software installed on the units and integrity verification.

18 The following documents are also considered part of the TOE, and are distributed, in PDF format on the CD-ROM labelled as 'Software' included with the product:

19 [IG] PSTgateways - Installation and Deployment Guide. Revision 2.

20 [OG] PSTgateways - Operation Guide. Revision 2.

1.4.2. Logical Scope

21 TOE provides the following functionality:

- Administration (Administration functionality implemented on PSTfile Gateway units)
- Auditing (Auditing features offered by PSTfile Gateway units)
- High Availability (Optional operation mode)
- Cold boot integrity check and signature verification of updates

- Data flows
  - Automatic inbound file service (IF)
  - Automatic outbound file service (OF)

1.4.2.1. Administration

22 Local configuration is only performed with the system down. It is done on the internal unit to establish a few initial settings that seldom need to be modified.

23 Administration can take place from any station on the internal network, and it is done through the admAPI interface accessible by TLS. Access to each function is restricted to administrators with one of the four available roles.

24 There are 4 different remote administration roles, each with their respective permissions. You can assign any roles you want to an administrator.

25 The gateway also sends system events via the 'syslog' protocol to servers located on the internal network.

1.4.2.2. Auditing

26 Auditing is the recording of information about the transfers made by the system.

27 PSTi automatically connects to the configured server on the internal network. Using TLS and audPROT, sends transfer data to be inserted into an external database.

28 For each service, it is possible to configure whether or not auditing information will be sent.

1.4.2.3. High availability

29 A high-availability option exists which allows the two elements to work in a coordinated way: their configuration is synchronized using a direct link via a dedicated cable connecting the two internal units. If one element fails, the other assumes the entire load automatically. Once the failure has been resolved, the switch to the normal mode of operation is also made automatically.

1.4.2.4. Cold boot integrity check and signature verification of updates

30 A CD-ROM is delivered together with the product that allows the units to be booted from another operating system and checking the integrity of all installed software as well as installing updates from a USB device after the signature of the updates has been verified.

31 This is a local administrator function that is run according to the corresponding description in the 'Installation and Deployment Manual' [IG].

1.4.2.5. Data flows

1.4.2.5.1. Automatic inbound file service (IF)

32 The inbound file service is organized into channels that the system administrator can define and activate or deactivate as necessary. Active channels make transfers automatically.

Inbound File Channel

Inbound File Channel is the name given to the correspondence between a source folder on an external network file server and a destination folder on an internal network file server.

Channel Features

- Supported source and destination file protocols: FTP, FTPS and SMB.
- Gateway units *always* play the client role for supported protocols.
- It can be configured whether files are to be *moved* from the source to the target; i.e. once they have been transferred to the target location, they will be deleted from the source location or *copied*; i.e. they remain in the source folder (mirror mode).
- Recursive mode: in this mode all folders present in the source folder and their contents are also copied. The folder structure in the source is not deleted.
- File size and file extension restrictions can be configured.
- Optionally, files can be uploaded with a temporary name and renamed thereafter.
- In high availability versions the administrator can decide on which of the two elements each channel will run.

Service parameters

- Optional transfer log.

  The following information is recorded for transfers made by the system: time and date, source and destination servers, base directory and *relative directory*, name, size and SHA-256 hash of transferred files.

1.4.2.5.2. Automatic outbound file service (OF)

33 The outbound file service is organized into channels that the system administrator can define and activate or deactivate as necessary. Active channels make transfers automatically.

34 File transfers from the source folder must be authorized by a digital signature. The signature must be contained in a detached file in CMS format with the same name as the file to be authorized and a configurable extension (by default '.sign').

Outbound File Channel

This is the name given to the correspondence between a source folder on an internal network file server and a destination folder on an external network file server.

Channel Features

- Supported source and destination file protocols: FTP, FTPS and SMB.
- *Gateway units always* play the client role of supported protocols.
- It can be configured whether files are *moved* from the source to the target; i.e. once they have been transferred to the destination location, they will be deleted from the source location or *copied*; i.e. they remain in the source folder (mirror mode).
- Recursive mode: in this mode all folders, present in the source folder, and their contents are also copied. The folder structure in the source is not deleted.
- File size and file extension restrictions can be configured.
- Optionally files can be uploaded with a temporary name and renamed thereafter.
- In high availability versions, the administrator can decide on which of the two elements each channel will run.

Service parameters

- Configurable transfer log.

  The following information is recorded for transfers made by the system: time and date, source and target server, base directory and relative directory, name, size and SHA-256 hash of transferred files.

2. Conformance Claims

2.1. CC Conformance Claim

35 This Security Target is conformant with sections 2 and 3 of the CC v. 3.1, rel 4 of the ISO/IEC 15408:2009 standard and defines an evaluation assurance level EAL2 augmented with ALC_FLR.1.

2.2. PP Conformance Claim

36 This Security Target has been developed specifically for PSTfile's security problem and does not claim conformance with any protection profile.

3. Security Problem Definition

3.1. TOE Assets

37 The following assets are declared to be protected by the TOE:

3.1.1. Information flow

- **Inbound information flow;** The entry of information from the external network to the internal network should not be possible except for that which is transmitted by the gateway itself, in accordance with the source and destination configuration established.
- **Outbound information flow;** It should not be possible for information to exit the internal network except for that which is transmitted by the gateway itself, in accordance with the established source and destination and signature verification configuration.

3.1.2. TSF data

- **TOE security sensitive data;** Integrity of configuration data (both static and dynamic), events and transfer info not yet moved to PSTaud.

3.2. Threats

38 The following threats are considered:

3.2.1. Information flow

- **T.INTOUTLEAK;** An unauthorized user on the internal network causes data on the internal network to leak to the external network.
- **T.EXTOUTLEAK;** An attacker on the external network gains access to internal network data through the TOE.
- **T.EXTINFEED;** An attacker on the external network manages to introduce data to the internal network, other than the data available in configured sources.
- **T.INTINFEED;** An unauthorized user on the internal network (rogue user or malicious code) manages to introduce data to the internal network through the system, other than the data available in the configured sources.

3.2.2. TSF data

- **T.INTACCESS;** An unauthorized user on the internal network gains remote access to the TOE and alters or deletes security sensitive data on the TOE.

3.3. Assumptions

- **A.PHYSEC;** The TOE is deployed in a physically secure environment. Only authorized personnel has physical access to the TOE.

- **A.LOCNOEVIL;** Administrators with physical access to the TOE will not attempt to circumvent the TOE's security functionality.
- **A.SINGLECHAN;** There are no channels for information to flow between the networks apart from the TOE itself.
- **A.SECPLAT;** The platform (TOE environment) will be designed and securely configured so as to avoid attacks through the platform itself.
- **A.NETS;** The internal network is an isolated network, securely configured and trustworthy. The external network is a physically controlled network with security measures in place but it is connected by TCP/IP to other networks.

3.4. Organizational policies

3.4.1. Design Criteria

- **P.SEP;** Both networks must remain separate. There should be no possibility of establishing TCP / IP connections between the two networks.
- **P.CRYPT;**The TOE will use cryptography for the following purposes:
  - The information (regarding configuration and the one processed by the system) which is stored on disk drives in the units (PSTi and PSTe) must be encrypted.
  - Communications with PSTadm for remote administration and with PSTaud for logging of auditing data must be encrypted.
  - The user information sent in the outgoing data flow (from the internal to the external network) must be authorized using a digital signature.
- **P.ROLES;** The product must implement the following roles, with the indicated capabilities:
  1. **Root Administrator:**
     1. Establishes the CNs of certificates which are considered valid for the administration of the gateway, and their associated permissions.
  2. **Security Administrator:**
     1. Sets monitoring configuration: parameters which affect the system events and transfers logging.
     2. Can obtain a copy of security events files (which are stored locally on the internal unit of the gateway).
     3. Can send system commands (system time set and reboot).
  3. **Services Administrator:**

1. Establishes all the configuration of services (inbound and outbound file services).

2. Can start and stop inbound and outbound file services.

3. Can obtain a copy of operation events files (which are stored locally on the internal unit of the gateway).

4. **Monitoring Administrator:**

    1. Monitors the operating status of the gateway.

    2. Can reset statistical information of the services (inbound and outbound file services).

5. **Local Administrator:**

    1. Establishes the local configuration of internal units.

    2. Performs integrity checks of both units and deploys updates.

These roles and capabilities will be implemented through the authentication features that allow the policies and access control functions that regulate the authorized exercise of the capabilities indicated, to be established.

- **P.AUDIT;** The TOE will implement a mechanism to log its activity.
- **P.AVAIL;** A high availability configuration must be possible where a peer element can take over the services of a failing element. (This policy only applies to high availability configuration).

4. Security Objectives

4.1. Security Objectives for the TOE

- **O.FLOW;** The TOE implements the following information flow policy:

    1. It should not be possible for information to exit the internal network except for that which is transferred through the gateway itself (via outbound file service) once it has been duly authorized (by digital signature).

    2. The entry of information from the external network to the internal network should not be possible, except for that which is transferred by the gateway itself via inbound file service.

- **O.ROLES;** PSTfile must implement the following roles, with the indicated capabilities:

    1. **Root administrator:**

        1. Establishes the CNs of certificates which are considered valid for the administration of the gateway, and their associated permissions.

    2. **Security Administrator:**

        1. Sets monitoring configuration: parameters which affect the system events and transfers logging.

        2. Can obtain a copy of security events files (which are stored locally on the internal unit of the gateway).

        3. Can send system commands (system time set and reboot).

    3. **Services Administrator:**

        1. Establishes all the configuration of services (inbound and outbound file services).

        2. Can start and stop inbound and outbound file services.

        3. Can obtain a copy of operation events files (which are stored locally on the internal unit of the gateway).

    4. **Monitoring Administrator:**

        1. Monitors the operating status of the gateway.

        2. Can reset statistical information of the services (inbound and outbound file services).

    5. **Local Administrator:**

1. Establishes the local configuration of internal units.

2. Performs integrity checks of both units and deploys updates.

These roles and capabilities will be implemented through the authentication features that allow the policies and access control functions that regulate the authorized exercise of the capabilities indicated, to be established.

- **O.AUDIT;** The TOE will implement a mechanism to log its activity.

- **O.AVAIL;** This goal only applies to the high availability configuration. The TOE must optionally provide a failover solution where the services of a failing element are taken over by a redundant element.

4.2. Security Objectives for the Operational Environment

- **OE.PHYSEC;** No access will be granted to the hardware of either of the two units (except for the Local Administrator). It is assumed that the obvious ways to circumvent the system (for example, connect both units directly through a network cable) are ruled out by physical or organizational measures within the operational environment.

- **OE.SECPLAT;** The platform (TOE environment) will be designed and securely configured so as to avoid attacks through the platform itself.

- **OE.CRYPT;** The cryptographic operations use a third party trusted cryptographic module for the following:

  - Disk encryption on internal units (PSTi). Encryption is done on internal units with a key that is stored in an external device and is retrieved during each start-up for decryption.

  - Disk encryption on external units (PSTe). Encryption is done on external units with a session key. This grants that there will be no persistence between sessions.

  - TLS connection establishment for administration and sending of auditing data

  - Verification of the signature of outgoing files

- **OE.NETS;** The internal network is an isolated network, securely configured and trustworthy. The external Network is a physically controlled network with security measures in place but it is connected by TCP/IP to other networks.

- **OE.SEP;** Network separation. The hardware architecture must be designed in a way that a different host exists on each of the networks. Communication between the hosts must be made using a passive information exchange device.

4.3. Justification of Security Objectives

	O.FLOW	O.ROLES	O.AUDIT	O.AVAIL
P.ROLES		X		
P.AUDIT			X	
P.AVAIL				X
T.INTACCESS		X		
T.INTOUTLEAK	X			
T.EXTOUTLEAK	X			
T.EXTINFEED	X			
T.INTINFEED	X			

Table 1. Security Objectives for the TOE

39 The flow control objective (O.FLOW) mitigates following threats T.INTOUTLEAK, T.EXTOUTLEAK, T.EXTINFEED and T.INTINFEED.

40 The roles and capabilities objective (O.ROLES) enforces the P.ROLES policy compliance and mitigates the threat T.INTACCESS.

41 The audit objective (O.AUDIT) ensures P.AUDIT policy compliance.

42 The availability objective (O.AVAIL) ensures P.AVAIL policy compliance (only for high availability configuration).

	OE.PHYSEC	OE.SECPLAT	OE.CRYPT	OE.SEP	OE.NETS
P.CRYPT			X		
P.SEP				X	
A.PHYSEC	X				
A.LOCNOEVIL	X				
A.SINGLECHAN	X				
A.SECPLAT		X			
A.NETS					X

Table 2. Security objectives for the operational environment

43 The OE.PHYSEC objective for the environment ensures that the operational environment assumptions A.PHYSEC, A.LOCNOEVIL and A.SINGLECHAN are directly fulfilled.

44 The OE.SECPLAT objective for the environment ensures that the A.SECPLAT operational environment assumption is directly fulfilled.

45 The OE.CRYPT objective for the environment ensures P.CRYPT policy compliance.

46 The OE.SEP objective for the environment ensures P.SEP policy compliance.

47 The OE.NETS objective for the environment ensures that the A.NETS operational environment assumption is directly fulfilled.

5. TOE Security Requirements

5.1. Security Functional Requirements

5.1.1. Roles and Access Control

5.1.1.1. FMT_SMR.2 Restrictions on security roles

5.1.1.1.1. FMT_SMR.2.1

48 The TSF shall maintain the roles: [assignment: *Root Administrator, Security Administrator, Services Administrator, Monitoring Administrator, Local Administrator*].

5.1.1.1.2. FMT_SMR.2.2

49 The TSF shall be able to associate users with roles.

5.1.1.1.3. FMT_SMR.2.3

50 The TSF shall ensure that the conditions [assignment: *Up to five Root Administrators can be configured by means of the local interface of the internal unit. Root Administrators are the only administrators enabled to add new administrators and assign them roles. There are no restrictions on the roles that can be assigned to a particular administrator.*] are satisfied.

5.1.1.2. FMT_SMF.1 Specification of Management Functions

51 The TSF shall be capable of performing the following management functions: [assignment: *Root Administrator, Security Administrator, Services Administrator, Monitoring Administrator: shown in Table 3; Local Administrator: Local setting of static configuration on the internal PSTi unit (network configuration of both units, certificates of the trusted certification authorities, private key and certificate for the gateway, CN of Root Administrators - identification of Root Administrators), integrity checks and updates deployment*].

5.1.1.3. FIA_UID.1 Timing of identification

5.1.1.3.1. FIA_UID.1.1

52 The TSF shall allow [assignment: *Shutdown and reset of both units by the Local Administrator*] on behalf of the user to be performed before the user is identified.

5.1.1.3.2. FIA_UID.1.2

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

5.1.1.4. FIA_UAU.1 Timing of authentication

5.1.1.4.1. FIA_UAU.1.1

54 The TSF shall allow [assignment: *Shutdown and reset of both units by the local administrator*] on behalf of the user to be performed before the user is authenticated.

5.1.1.4.2. FIA_UAU.1.2

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

56 **Note**: A Local Administrator is only authenticated by means of a password which is entered the first time the administrator accesses the local configuration interface. Environment organizational measures must deny physical access to users not having Local Administrator permission.

5.1.1.5. FMT_MSA.1/ IFF Management of security attributes

5.1.1.5.1. FMT_MSA.1.1

57 The TSF shall enforce the [assignment: *"Inbound file policy", "outbound file policy"*] to restrict the ability to [selection: *change_default, query, modify, delete*] the security attributes [assignment: *of section 5.1.2.1 for inbound file service and of section 5.1.2.2 for outbound file service*] to [assignment: *Services Administrator*]

5.1.1.6. FMT_MSA.1 / ACC Management of security attributes

5.1.1.6.1. FMT_MSA.1.1

58 The TSF shall enforce the [assignment: *"Access policy and roles"*] to restrict the ability to [selection: *change_default, query, modify, delete*] the security attributes [assignment: *user roles*] to [assignment: *Root Administrator (CU6 of Table 3)*].

5.1.1.7. FMT_MSA.3 / IFF Static attribute initialisation

5.1.1.7.1. FMT_MSA.3.1

59 The TSF shall enforce the [assignment: *"inbound file policy", "outbound file policy"*] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the SFP.

5.1.1.7.2. FMT_MSA.3.2

60 The TSF shall allow the [assignment: *Services Administrator*] to specify alternative initial values to override the default values when an object or information is created.

5.1.1.8. FMT_MSA.3 / ACC Static attribute initialisation

5.1.1.8.1. FMT_MSA.3.1

61 The TSF shall enforce the [assignment: *"Access policy and roles"*] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the SFP.

5.1.1.8.2. FMT_MSA.3.2

62 The TSF shall allow the [assignment: *Root Administrator*] to specify alternative initial values to override the default values when an object or information is created.

5.1.1.9. FDP_ACF.1 Security attribute based access control

5.1.1.9.1. FDP_ACF.1.1

63 The TSF shall enforce the [assignment: *"Access policy and roles"*] to objects based on the following: [assignment:

- *Subjects: TOE users, attribute: their role*
- *Objects: TOE functionality shown in Table 3, attribute: functionality Id].*

5.1.1.9.2. FDP_ACF.1.2

64 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *access control will enforce the execution of the TOE capabilities in accordance to the roles assigned to the user as indicated in the roles definition.*].

5.1.1.9.3. FDP_ACF.1.3

65 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *None.*].

		Root Administrator	**Services Administrator**	**Security Administrator**	**Monitoring Administrator**
CU1	Static configuration query			X	
CU2	Operation monitoring				X
CU3	Services starting and stopping		X		
CU4	Service configuration editing		X		
CU5	Monitoring configuration editing			X	
CU6	Administration permissions editing	X			
CU7	Operation events files access		X		
CU8	Security events files access			X	

		Root Administrator	Services Administrator	Security Administrator	Monitoring Administrator
CU9	Reset of statistical information				X
CU10	System commands			X	

Table 3. Functionality available to administration roles

5.1.1.9.4. FDP_ACF.1.4

66 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *None.*].

5.1.1.10. FDP_ACC.2 Complete access control

5.1.1.10.1. FDP_ACC.2.1

67 The TSF shall enforce the [assignment: *"access policy and roles"*] on [assignment: *TOE users and TOE functionality listed in Table 3, "Functionality available to administration roles"*] and all operations among subjects and objects covered by the SFP.

5.1.1.10.2. FDP_ACC.2.2

68 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

5.1.2. Information flow

5.1.2.1. Inbound file flow

69 Flow control of inbound files is made using the 'inbound channel' definition. A channel must be defined and a source folder set in the channel configuration in order for the gateway to process the files located in a folder on the external network file server. The gateway supports up to 250 inbound channels. 'Services Administrator' permission is required to define the inbound channel configuration. Services administrators have absolute control over inbound file flow.

70 The channel definition determines how PSTfile inbound file service (IF) handles files located in the source directory.

5.1.2.1.1. Channel flow

71 The channel definition comprises the following:

- External source file server and all of the configuration elements needed to access the external network server (access protocol (FTP, FTPS, SMB), access ID, base folder, etc.).

- Internal destination file server and all of the configuration elements needed to access the internal network server(access protocol (FTP, FTPS, SMB), access ID, base folder, etc.).
- Option to move or copy files.
- Recursion option (take into account all folders within the base folder up to a maximum of 10 levels).
- Option to upload files using a temporary name and to rename the files with the definitive name once uploaded.
- Option to set for transferred files, the date and time values of the source file.
- Option to define limitations in the size and names of files to be transferred.

5.1.2.2. Outbound file flow

72 Flow control of outbound files is made using the 'outbound channel' definition. A channel must be defined and a source folder set in the channel configuration in order for the gateway to process the files located in that folder on the internal network file server. The gateway supports up to 250 outbound channels. 'Services Administrator' permission is required to define the outbound channel configuration.

73 The channel definition, determines how the PSTfile outbound file service (OF) handles files present in the internal directory.

5.1.2.2.1. Channel flow

74 The channel definition comprises the following:

- Internal source file server and all of the configuration elements required to access the internal network server (access protocol (FTP, FTPS, SMB), access ID, base folder, etc.).
- External destination file server and all of the configuration elements required to access the external network server (access protocol (FTP, FTPS, SMB), access ID, base folder, etc.).
- Option to move or copy files.
- Recursion option (take into account all folders within the base folder up to a maximum of 10 levels).
- Option to upload files using a temporary name and to rename the files with the definitive name once uploaded.
- Option to set for transferred files, the date and time values of the source file.
- Option to define limitations in the size and names of files to be transferred.

75 In addition, for the file to be transferred, a file containing a valid digital signature of the file, with the same name and a configurable extension, must be located in the source folder.

76 The CN of the certificate entitled to sign files is defined as a configuration parameter of the channel. The trusted root CAs are also defined as configuration parameters of the outbound file service.

5.1.2.3. FDP_IFC.2 / IN Complete information flow control

5.1.2.3.1. FDP_IFC.2.1

77 The TSF shall enforce the [assignment: *"inbound file policy"*] on [assignment:

- *Information: files (as shown in Section 5.1.2.1, "Inbound file flow").*
- *Subjects: external network information source and internal network information destination, entities.*]

and all operations that cause that information to flow to and from subjects covered by the SFP.

5.1.2.3.2. FDP_IFC.2.2

78 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

5.1.2.4. FDP_IFF.1 / IN Simple security attributes

5.1.2.4.1. FDP_IFF.1.1

79 The TSF shall enforce the [assignment: *"inbound file policy"*] based on the following types of subject and information security attributes: [assignment:

- *Information: files, attributes required by policies of Section 5.1.2.1, "Inbound file flow".*
- *Subjects: external network information source and internal network information destination, entities.*]

5.1.2.4.2. FDP_IFF.1.2

80 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for inbound file policy of Section 5.1.2.1, "Inbound file flow"*].

5.1.2.4.3. FDP_IFF.1.3

81 The TSF shall enforce the [assignment: *None.*].

5.1.2.4.4. FDP_IFF.1.4

82 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *None*].

5.1.2.4.5. FDP_IFF.1.5

83 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *None*].

5.1.2.5. FDP_IFC.2 / OUT Complete information flow control

5.1.2.5.1. FDP_IFC.2.1

84 The TSF shall enforce the [assignment: *"outbound file policy"*] on [assignment:

- *Information: files, (as described in Section 5.1.2.2, "Outbound file flow").*
- *Subjects: internal network information source and external network information destination, entities.*]

and all operations that cause that information to flow to and from subjects covered by the SFP.

5.1.2.5.2. FDP_IFC.2.2

85 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

5.1.2.6. FDP_IFF.1 / OUT Simple security attributes

5.1.2.6.1. FDP_IFF.1.1

86 The TSF shall enforce the [assignment: *"outbound file policy"*] based on the following types of subject and information security attributes: [assignment:

- *Information: files, attributes required by policies of Section 5.1.2.2, "Outbound file flow".*]
- *Subjects: internal source information network and external target information network entities.*]

5.1.2.6.2. FDP_IFF.1.2

87 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for outbound file policy of Section 5.1.2.2, "Outbound file flow"*].

5.1.2.6.3. FDP_IFF.1.3

88 The TSF shall enforce the [assignment: *None.*].

5.1.2.6.4. FDP_IFF.1.4

89 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *None*].

5.1.2.6.5. FDP_IFF.1.5

90 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *None*].

5.1.3. Audit

5.1.3.1. FAU_GEN.1 Audit data generation

5.1.3.1.1. FAU_GEN.1.1

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

- Start-up and shutdown of the audit functions;
- All auditable events for the [selection: *not specified*] level of audit; and
- [assignment: *The following events:*]

Operation Events

AuditDebug

AuditServerConnect

AuditServerConnectFail

AuditServerDisconnect

AuditServerCommandFailed

AuditServerUnavailable

ChannelWarning

ChannelError

ChannelOk

ChannelDebug

ChannelIssue

GlobalFailure

GlobalSystemStartup

GlobalSystemShutdown

GlobalLinkUp

GlobalLinkDown

GlobalLinkFailure

GlobalAuditFailure

GlobalPrimaryClusterFailed

GlobalPrimaryConnected

GlobalPrimaryDisconnected

GlobalSecondaryConnected

GlobalSecondaryClusterFailed

GlobalSecondaryDisconnected

GlobalPrimaryEnabled

GlobalPrimaryDisabled

GlobalSecondaryEnabled

GlobalSecondaryDisabled

GlobalVersionFailure

GlobalDebug

ServiceStart

ServiceStop

ServiceFailure

Security Events

AdminConnect

AdminDisconnect

AdminConnectRejection

AdminWriteCommand

AuditServerConnectinSecFail

ChannelRequestSecRejection

File transfer events

Inbound file transfer 'if_transfer'

Outbound file transfer 'of_transfer'

5.1.3.1.2. FAU_GEN.1.2

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment:]

Operation and security events

Severity	Informational (6), Notice (5), Warning (4), Error (3) and Critical (2)
Specific event info	Event specific
Hostname	IP address of internal unit of gateway sending the event
Tag	Gateway Id

5.1.3.2. FAU_SAR.1 Audit review

5.1.3.2.1. FAU_SAR.1.1

93 The TSF shall provide [assignment: *Security / Services Administrator*] with the capability to read [assignment: *security / operation system events*] from the audit records.

5.1.3.2.2. FAU_SAR.1.2

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

5.1.3.3. FAU_SAR.2 Restricted audit review

5.1.3.3.1. FAU_SAR.2.1 Restricted audit review

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

5.1.4. Availability

5.1.4.1. FRU_FLT.1 Degraded fault tolerance

5.1.4.1.1. FRU_FLT.1.1

96 The TSF shall ensure the operation of [assignment:

"All security functions", "All security functions apart from persistent admAPI commands belonging to use cases CU3, CU4, CU5 y CU6 as well as SetSystemTime."

] when the following failures occur: [assignment:

"Failure of secondary element caused by internal or external unit.", "Failure of primary element caused by internal o external unit."

].

97 **Application Note:** In the event of failure of the primary element, the following commands corresponding to the security functionality are excluded:

- RemoveChCfg
- SetAdmCfg
- SetMonitorCfg
- SetSrvCfg
- ShutdownSrv
- StartSrv
- StopSrv
- UpdateChCfg
- SetSystemTime

5.1.4.2. FPT_FLS.1 Failure with preservation of secure state

5.1.4.2.1. FPT_FLS.1.1

98 The TSF shall preserve a secure state when the following types of failures occur: [assignment:

"Primary element failure that prevents service operation.", "Secondary element failure that prevents service operation."

].

5.1.4.3. FPT_TRC.1 Internal TSF consistency

5.1.4.3.1. FPT_TRC.1.1

99 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

5.1.4.3.2. FPT_TRC.1.2

100 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [assignment: *inbound file service; outbound file service*].

5.1.4.4. FPT_ITT.1 Basic internal TSF data transfer protection

5.1.4.4.1. FPT_ITT.1.1

101 The TSF shall protect TSF data from [selection: *disclosure, modification*] when it is transmitted between separate parts of the TOE.

5.2. Security Assurance Requirements

102 TOE development and evaluation will be done in conformity with following assurance level:

- EAL2
- ALC_FLR.1

5.2.1. ADV_ARC.1 Security architecture description

Developer action elements:

5.2.1.1. ADV_ARC.1.1D

103 **The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.**

5.2.1.2. ADV_ARC.1.2D

104 **The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.**

5.2.1.3. ADV_ARC.1.3D

105 **The developer shall provide a security architecture description of the TSF.**

Content and presentation of evidence elements:

5.2.1.4. ADV_ARC.1.1C

106 **The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.**

5.2.1.5. ADV_ARC.1.2C

107 **The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.**

5.2.1.6. ADV_ARC.1.3C

108 **The security architecture description shall describe how the TSF initialisation process is secure.**

5.2.1.7. ADV_ARC.1.4C

109 **The security architecture description shall demonstrate that the TSF protects itself from tampering.**

5.2.1.8. ADV_ARC.1.5C

110 **The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.**

5.2.2. ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

5.2.2.1. ADV_FSP.2.1D

111 **The developer shall provide a functional specification.**

5.2.2.2. ADV_FSP.2.2D

112 **The developer shall provide a tracing from the functional specification to the SFRs.**

Content and presentation elements:

5.2.2.3. ADV_FSP.2.1C

113 **The functional specification shall completely represent the TSF.**

5.2.2.4. ADV_FSP.2.2C

114 **The functional specification shall describe the purpose and method of use for all TSFI.**

5.2.2.5. ADV_FSP.2.3C

115 **The functional specification shall identify and describe all parameters associated with each TSFI.**

5.2.2.6. ADV_FSP.2.4C

116 **For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.**

5.2.2.7. ADV_FSP.2.5C

117 **For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.**

5.2.2.8. ADV_FSP.2.6C

118 **The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.**

5.2.3. ADV_TDS.1 Basic design

Developer action elements:

5.2.3.1. ADV_TDS.1.1D

119 **The developer shall provide the design of the TOE.**

5.2.3.2. ADV_TDS.1.2D

120 **The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.**

Content and presentation elements:

5.2.3.3. ADV_TDS.1.1C

121 **The design shall describe the structure of the TOE in terms of subsystems.**

5.2.3.4. ADV_TDS.1.2C

122 **The design shall identify all subsystems of the TSF.**

5.2.3.5. ADV_TDS.1.3C

123 **The design shall describe the behaviour of each SFR-supporting or SFRnon-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.**

5.2.3.6. ADV_TDS.1.4C

124 **The design shall summarise the SFR-enforcing behaviour of the SFRenforcing subsystems.**

5.2.3.7. ADV_TDS.1.5C

125 **The design shall provide a description of the interactions among SFRenforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.**

5.2.3.8. ADV_TDS.1.6C

126 **The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.**

5.2.4. AGD_OPE.1 Operational user guidance

Developer action elements:

5.2.4.1. AGD_OPE.1.1D

127 **The developer shall provide operational user guidance.**

Content and presentation of evidence elements:

5.2.4.2. AGD_OPE.1.1C

128 **The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.**

5.2.4.3. AGD_OPE.1.2C

129 **The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.**

5.2.4.4. AGD_OPE.1.3C

130 **The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.**

5.2.4.5. AGD_OPE.1.4C

131 **The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.**

5.2.4.6. AGD_OPE.1.5C

132 **The operational user guidance 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.**

5.2.4.7. AGD_OPE.1.6C

133 **The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.**

5.2.4.8. AGD_OPE.1.7C

134 **The operational user guidance shall be clear and reasonable.**

5.2.5. AGD_PRE.1 Preparative procedures

Developer action elements:

5.2.5.1. AGD_PRE.1.1D

135 **The developer shall provide the TOE including its preparative procedures.**

Content and presentation of evidence elements:

5.2.5.2. AGD_PRE.1.1C

136 **The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.**

5.2.5.3. AGD_PRE.1.2C

137 **The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.**

5.2.6. ALC_CMC.2 Use of a CM system

Developer action elements:

5.2.6.1. ALC_CMC.2.1D

138 **The developer shall provide the TOE and a reference for the TOE.**

5.2.6.2. ALC_CMC.2.2D

139 **The developer shall provide the CM documentation.**

5.2.6.3. ALC_CMC.2.3D

140 **The developer shall use a CM system.**

Content and presentation elements:

5.2.6.4. ALC_CMC.2.1C

141 **The TOE shall be labelled with its unique reference.**

5.2.6.5. ALC_CMC.2.2C

142 **The CM documentation shall describe the method used to uniquely identify the configuration items.**

5.2.6.6. ALC_CMC.2.3C

143 **The CM system shall uniquely identify all configuration items.**

5.2.7. ALC_CMS.2 Parts of the TOE CM coverage

Developer action elements:

5.2.7.1. ALC_CMS.2.1D

144 **The developer shall provide a configuration list for the TOE.**

Content and presentation elements:

5.2.7.2. ALC_CMS.2.1C

145 **The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.**

5.2.7.3. ALC_CMS.2.2C

146 **The configuration list shall uniquely identify the configuration items.**

5.2.7.4. ALC_CMS.2.3C

147 **For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.**

5.2.8. ALC_DEL.1 Delivery procedures

Developer action elements:

5.2.8.1. ALC_DEL.1.1D

148 **The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.**

5.2.8.2. ALC_DEL.1.2D

149 **The developer shall use the delivery procedures.**

Content and presentation of evidence elements:

5.2.8.3. ALC_DEL.1.1C

150 **The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.**

5.2.9. ALC_FLR.1 Basic flaw remediation

Developer action elements:

5.2.9.1. ALC_FLR.1.1D

151 **The developer shall document and provide flaw remediation procedures addressed to TOE developers.**

Content and presentation of evidence elements:

5.2.9.2. ALC_FLR.1.1C

152 **The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.**

5.2.9.3. ALC_FLR.1.2C

153 **The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.**

5.2.9.4. ALC_FLR.1.3C

154 **The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.**

5.2.9.5. ALC_FLR.1.4C

155 **The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.**

5.2.10. ASE_CCL.1 Conformance claims

Developer action elements:

5.2.10.1. ASE_CCL.1.1D

156 **The developer shall provide a conformance claim.**

5.2.10.2. ASE_CCL.1.2D

157 **The developer shall provide a conformance claim rationale.**

Content and presentation of evidence elements:

5.2.10.3. ASE_CCL.1.1C

158 **The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.**

5.2.10.4. ASE_CCL.1.2C

159 **The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.**

5.2.10.5. ASE_CCL.1.3C

160 **The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.**

5.2.10.6. ASE_CCL.1.4C

161 **The CC conformance claim shall be consistent with the extended components definition.**

5.2.10.7. ASE_CCL.1.5C

162 **The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.**

5.2.10.8. ASE_CCL.1.6C

163 **The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.**

5.2.10.9. ASE_CCL.1.7C

164 **The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.**

5.2.10.10. ASE_CCL.1.8C

165 **The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.**

5.2.10.11. ASE_CCL.1.9C

166 **The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.**

5.2.10.12. ASE_CCL.1.10C

167 **The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.**

5.2.11. ASE_ECD.1 Extended components definition

Developer action elements:

5.2.11.1. ASE_ECD.1.1D

168 **The developer shall provide a statement of security requirements.**

5.2.11.2. ASE_ECD.1.2D

169 **The developer shall provide an extended components definition.**

Content and presentation of evidence elements:

5.2.11.3. ASE_ECD.1.1C

170 **The statement of security requirements shall identify all extended security requirements.**

5.2.11.4. ASE_ECD.1.2C

171 **The extended components definition shall define an extended component for each extended security requirement.**

5.2.11.5. ASE_ECD.1.3C

172 **The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.**

5.2.11.6. ASE_ECD.1.4C

173 **The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.**

5.2.11.7. ASE_ECD.1.5C

174 **The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.**

5.2.12. ASE_INT.1 ST introduction

Developer action elements:

5.2.12.1. ASE_INT.1.1D

175 **The developer shall provide an ST introduction.**

Content and presentation of evidence elements:

5.2.12.2. ASE_INT.1.1C

176 **The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.**

5.2.12.3. ASE_INT.1.2C

177 **The ST reference shall uniquely identify the ST.**

5.2.12.4. ASE_INT.1.3C

178 **The TOE reference shall identify the TOE.**

5.2.12.5. ASE_INT.1.4C

179 **The TOE overview shall summarise the usage and major security features of the TOE.**

5.2.12.6. ASE_INT.1.5C

180 **The TOE overview shall identify the TOE type.**

5.2.12.7. ASE_INT.1.6C

181 **The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.**

5.2.12.8. ASE_INT.1.7C

182 **The TOE description shall describe the physical scope of the TOE.**

5.2.12.9. ASE_INT.1.8C

183 **The TOE description shall describe the logical scope of the TOE.**

5.2.13. ASE_OBJ.2 Security objectives

Developer action elements:

5.2.13.1. ASE_OBJ.2.1D

184 **The developer shall provide a statement of security objectives.**

5.2.13.2. ASE_OBJ.2.2D

185 **The developer shall provide a security objectives rationale.**

Content and presentation of evidence elements:

5.2.13.3. ASE_OBJ.2.1C

186 **The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.**

5.2.13.4. ASE_OBJ.2.2C

187 **The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.**

5.2.13.5. ASE_OBJ.2.3C

188 **The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.**

5.2.13.6. ASE_OBJ.2.4C

189 **The security objectives rationale shall demonstrate that the security objectives counter all threats.**

5.2.13.7. ASE_OBJ.2.5C

190 **The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.**

5.2.13.8. ASE_OBJ.2.6C

191 **The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.**

5.2.14. ASE_REQ.2 Derived security requirements

Developer action elements:

5.2.14.1. ASE_REQ.2.1D

192 **The developer shall provide a statement of security requirements.**

5.2.14.2. ASE_REQ.2.2D

193 **The developer shall provide a security requirements rationale.**

Content and presentation of evidence elements:

5.2.14.3. ASE_REQ.2.1C

194 **The statement of security requirements shall describe the SFRs and the SARs.**

5.2.14.4. ASE_REQ.2.2C

195 **All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.**

5.2.14.5. ASE_REQ.2.3C

196 **The statement of security requirements shall identify all operations on the security requirements.**

5.2.14.6. ASE_REQ.2.4C

197 **All operations shall be performed correctly.**

5.2.14.7. ASE_REQ.2.5C

198 **Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.**

5.2.14.8. ASE_REQ.2.6C

199 **The security requirements rationale shall trace each SFR back to the security objectives for the TOE.**

5.2.14.9. ASE_REQ.2.7C

200 **The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.**

5.2.14.10. ASE_REQ.2.8C

201 **The security requirements rationale shall explain why the SARs were chosen.**

5.2.14.11. ASE_REQ.2.9C

202 **The statement of security requirements shall be internally consistent.**

5.2.15. ASE_SPD.1 Security problem definition

Developer action elements:

5.2.15.1. ASE_APD.1.1D

203 **The developer shall provide a security problem definition.**

Content and presentation of evidence elements:

5.2.15.2. ASE_SPD.1.1C

204 **The security problem definition shall describe the threats.**

5.2.15.3. ASE_SPD.1.2C

205 **All threats shall be described in terms of a threat agent, an asset, and an adverse action.**

5.2.15.4. ASE_SPD.1.3C

206 **The security problem definition shall describe the OSPs.**

5.2.15.5. ASE_SPD.1.4C

207 **The security problem definition shall describe the assumptions about the operational environment of the TOE.**

5.2.16. ASE_TSS.1 TOE summary specification

Developer action elements:

5.2.16.1. ASE_TSS.1.1D

208 **The developer shall provide a TOE summary specification.**

Content and presentation of evidence elements:

5.2.16.2. ASE_TSS.1.1C

209 **The TOE summary specification shall describe how the TOE meets each SFR.**

5.2.17. ATE_COV.1 Analysis of coverage

Developer action elements:

5.2.17.1. ATE_COV.1.1D

210 **The developer shall provide evidence of the test coverage.**

Content and presentation elements:

5.2.17.2. ATE_COV.1.1C

211 **The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.**

5.2.18. ATE_FUN.1 Functional testing

Developer action elements:

5.2.18.1. ATE_FUN.1.1D

212 **The developer shall test the TSF and document the results.**

5.2.18.2. ATE_FUN.1.2D

213 **The developer shall provide test documentation.**

Content and presentation of evidence elements:

5.2.18.3. ATE_FUN.1.1C

214 **The test documentation shall consist of test plans, expected test results and actual test results.**

5.2.18.4. ATE_FUN.1.2C

215 **The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.**

5.2.18.5. ATE_FUN.1.3C

216 **The expected test results shall show the anticipated outputs from a successful execution of the tests.**

5.2.18.6. ATE_FUN.1.4C

217 **The actual test results shall be consistent with the expected test results.**

5.2.19. ATE_IND.2 Independent testing - sample

Developer action elements:

5.2.19.1. ATE_IND.2.1D

218 **The developer shall provide the TOE for testing.**

Content and presentation of evidence elements:

5.2.19.2. ATE_IND.2.1C

219 **The TOE shall be suitable for testing.**

5.2.19.3. ATE_IND.2.2C

220 **The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.**

5.2.20. AVA_VAN.2 Vulnerability analysis

Developer action elements:

5.2.20.1. AVA_VAN.2.1D

221 **The developer shall provide the TOE for testing.**

Content and presentation elements:

5.2.20.2. AVA_VAN.2.1C

222 **The TOE shall be suitable for testing.**

5.3. Security Requirements Rationale

	O.FLOW	O.ROLES	O.AUDIT	O.AVAIL
FMT_SMF.1				

	O.FLOW	O.ROLES	O.AUDIT	O.AVAIL
FDP_IFC.2 / IN FDP_IFF.1 / IN FDP_IFC.2 / OUT FDP_IFF.1 / OUT FMT_MSA.1 / IFF FMT_MSA.3 / IFF	X			
FMT_SMR.2 FMT_SMF.1 FDP_ACF.1 FDP_ACC.2 FMT_MSA.1 / ACC FMR_MSA.3 / ACC FIA_UID.1 FIA_UAU.1		X		
FAU_GEN.1 FAU_SAR.1 FAU_SAR.2 FMT_SMF.1			X	
FRU_FLT.1 FPT_FLS.1 FPT_TRC.1 FPT_ITT.1				X

Table 4. Security requirements rationale

5.3.1. Non satisfied dependencies justification

223 FPT_STM.1 is not satisfied because the TOE uses the system clock as time reference.

5.3.2. Functional security requirements rationale

224 The flow objective O.FLOW is satisfied due to the existence of a complete flow control policy (FDP_IFC.2 / IN for inbound files and FDP_IFC.2 / OUT for outbound files) with the security attributes expressed in FDP_IFF.1 / IN for inbound and FDP_IFF.1 / OUT for outbound and those security attributes are managed in accordance with FMT_MSA.1 / IFF and FMT_MSA.3 / IFF. Management of the corresponding attributes is done with FMT_SMF.1.

225 The objective O.ROLES is satisfied by the roles specified in FMT_SMR.2. The functions of each of the roles are specified in FMT_SMF.1. Identification and authentication of users before any action are covered by FIA_UID.1 and FIA_UAU.1. Security

attributes are managed in accordance with FMT_MSA.1 / ACC and FMT_MSA.3 / ACC. Security attributes based access control and complete control are enforced by FDP_ACF.1 y FDP_ACC.2.

226 The objective O.AUDIT is satisfied through the functions FAU_GEN.1, FAU_SAR.1 y FAU_SAR.2. Auditing is configurable as stated in FMT_SMF.1

227 The objective O.AVAIL is satisfied because all security functions (with the corresponding exceptions) described in FRU_FLT.1 are maintained in the event of failure of one of the elements (primary or secondary) according to FTP_FLS.1. When operation of both elements is recovered after the failure, the coherence of the configuration of both elements is guaranteed according to FPT_TRC.1. The data exchanged between the primary units of both elements is protected according to FPT_ITT.1 and the security mechanisms are managed according to FMT_SMF.1

5.3.3. Security assurance requirements rationale

228 The desired security assurance for the TOE is the one provided by EAL2 + ALC_FLR.1 assurance level.

229 EAL2 has been chosen for market reasons.

6. TOE summary specification

6.1. FMT_SMR.2 Restrictions on security roles

6.1.1. Administration roles

230 There are 5 distinct administrator roles:

- Root Administrator
- Security Administrator
- Services Administrator
- Monitoring Administrator
- Local Administrator

231 The association of the Local Administrator role to users is accomplished by limiting physical access to PSTfile units through organizational measures. A password is supplied during the first access to local interface at internal units, which is required in successive accesses.

232 Association of roles to users is done by means of the CN (Common Name) of a user certificate issued by a CA (Certification Authority) preconfigured (statical initialization) in PSTfile.

233 The association of the 'Root Administrator' role to users can only be locally done (statical initialization) and is limited to 5 users.

234 The association of the roles 'Security Administrator', 'Services Administrator' and 'Monitoring Administrator' is remotely done (from within the internal network) by a 'Root Administrator'. There is no restriction to the roles that a user can be assigned to.

6.2. FMT_SMF.1 Specification of Management Functions

235 Table 3 shows the functions accessible to each administration role: 'Root Administrator', 'Security Administrator', 'Services Administrator' and 'Monitoring Administrator'.

236 'Local Administrator' establishes the static configuration on the internal unit PSTi. The static configuration has the following attributes:

- Network parameters of both units
- Certificates of trusted root certification authorities
- Gateway's private key and certificate

- Root Administrator CNs

In addition, the 'Local Administrator' deploys updates and verifies the integrity of the software installed on both units.

6.3. FIA_UID.1 Timing of identification

237 All administrators apart from local administrators have access to security functionality through admAPI functions. In order to access any of the admAPI functions, a TLS connection with PSTi must be made. The CN of the certificate sent to establish the TLS connection is used to identify the administrator.

238 'Local Administrator' identification is made by means of a password. 'Local Administrator' authentication is exclusively done by means of a password supplied by the local administrator on entering the local configuration interface for the first time. Identification is implicit when accessing this interface.

6.4. FIA_UAU.1 Timing of authentication

239 All administrators apart from local administrators have access to security functionality through the admAPI functions. In order to access any of the admAPI functions, a TLS connection with PSTi must be made. The CN of the certificate sent to establish the TLS connection is used to identify the administrator.

240 The certificate must be signed by a CA, configured in PSTi's static configuration.

241 Local administrators are authenticated by means of a password.

6.5. FMT_MSA.1 / IFF Management of security attributes

242 Inbound policy and outbound policy are set through admAPI commands. In order to access any of admAPI commands, a TLS connection with PSTi must be made. The CN of the certificate sent to establish the TLS connection is used to authenticate the administrator.

243 A 'Services Administrator' role is required to access these commands.

244 The managed attributes for the inbound file service are described in Section 5.1.2.1, “Inbound file flow”.

245 The managed attributes for the outbound file service are described in Section 5.1.2.2, “Outbound file flow”.

6.6. FMT_MSA.1 / ACC Management of security attributes

246 The 'Local Administrator' establishes the CN of Root administrators in the static configuration using the local configuration interface. Physical access to the local configuration interface is restricted through organizational environment policies.

247 Access policy and roles are established through admAPI commands. In order to access any of admAPI commands, a TLS connection with PSTi must be made. The CN of the certificate sent to establish the TLS connection is used to identify the administrator.

248 'Root Administrator' role is required for accessing this command.

249 The command permits to define a list of authorized administrators and a list of IP addresses from which system administration is allowed. Each administrator is identified by the CN and the possible permissions are: ‘Monitoring Administrator’, ‘Services Administrator’ and 'Security Administrator’. ‘Root Administrator’ permission can only be locally modified.

250

6.7. FMT_MSA.3 / IFF Static attribute initialization

6.7.1. Inbound file policy and outbound file policy

251 Initialization provides a configuration without channels nor any other configuration element. This precludes any flow nor inbound nor outbound, unless explicitly set by a Services Administrator (see FMT_MSA.1.IFF).

6.8. FMT_MSA.3 / ACC Static attribute initialization

6.8.1. Access policy and roles

252 Initialization provides a configuration without any administration role assigned, except Root Administrators which can only be locally set through statical initialization. This guarantees that no administrator with the role 'Security Administrator', 'Services Administrator' nor 'Monitoring Administrator' will initially exist. All administrators of these types must be added through admAPI (see FMT_MSA.1.ACC).

6.9. FDP_ACF.1 Security attribute based access control

253 Administrators access security functionality through admAPI functions. In order to access any of admAPI functions, a TLS connection with PSTi must be made. The CN of the certificate sent to establish the TLS connection is used to authenticate the administrator. Every time a function is called, the system verifies that the administrator who established the connection has the permission required to execute the command. Every command has a unique required permission (see command table in FDP_ACF.1.3). If the administrator has the required permission the command is executed, otherwise the TLS connection is interrupted.

6.10. FDP_ACC.2 Complete access control

254 See Section 6.9, “FDP_ACF.1 Security attribute based access control”.

6.11. FDP_IFC.2 / IN Complete information flow control

255 The PSTfile inbound file service transfers a file from the external network to the internal network only if the following conditions are met:

- The file is located in a folder on an external network server for which a corresponding inbound channel has been defined in the inbound channels configuration.
- The channel to which the file belongs is in the ON state.

256 The inbound file channel configuration includes the definition of the elements mentioned above: directories on external network servers that will be checked and channel state (ON / OFF). This is described in more detail in Section 5.1.2.1, “Inbound file flow”.

257 Channel configuration is set through admAPI commands. 'Services Administrator' permission is required for accessing these commands.

6.12. FDP_IFF.1 / IN Simple security attributes

258 See Section 6.11, “FDP_IFC.2 / IN Complete information flow control”.

6.13. FDP_IFC.2 / OUT Complete information flow control

259 The PSTfile outbound file service transfers a file from the internal network to the external network only if the following conditions are met:

- The channel that will be used to transfer the file is in the ON state.
- The file is properly signed.
- The file has been signed with a certificate issued by a trusted CA.
- The supervisor signing the file, identified by the CN of the certificate, is in the list of the entitled signers for the channel.

260 The outbound file channel configuration includes the CNs entitled to authorize outbound files through this channel and the ON / OFF channel state. This configuration is described in more detail in Section 5.1.2.2, “Outbound file flow”.

261 This configuration is set by means of admAPI commands. 'Services Administrator' permission is required for accessing this commands.

6.14. FDP_IFF.1 / OUT Simple security attributes

262 See Section 6.13, “FDP_IFC.2 / OUT Complete information flow control”.

6.15. FAU_GEN.1 Audit data generation

263 PSTfile generates two distinct audit data types:

- System events
- Transfer logs

6.15.1. System events

264 System events are sent through 'syslog' and also stored in files which rotate with configurable file size and file number. System events belong to one of two categories: security or operation. Configuration parameters (destination server, minimal severity and file rotation parameters) for both categories are independent. Security Administrator permission is needed for setting them.

265 System event files cannot be deleted. A copy can be remotely requested through admAPI commands. 'Security Administrator' role is required for accessing security event files and 'Services Administrator' role for operation event files.

266 All system events log the following information: event date and time, event type, subject identity (where this applies) and other relevant information like severity level.

267 'GlobalSystemStartUp' and 'GlobalSystemShutdown' events signal the start and end of auditing functions.

6.15.2. Transfer logs

268 Inbound and outbound file transfer data are logged to an external database through PSTaud. 'Security Administrator' permission is required for setting the configuration data needed for accessing PSTaud.

269 Transfers logging on / off is a parameter of the general configuration of a service. 'Services Administrator' role is required to set this parameter.

270 All transfer events log the following information: time and date of the transfer, channel ID, source and destination server, folder and protocol; file name, size, date and hash.

6.16. FAU_SAR.1 Audit review

271 The TOE implements this requirement only for system events.

272 'Security Administrator' role is required for accessing security system event files.

273 'Services Administrator' role is required for accessing operation system event files.

274 Event files are plain text files. Each system event is stored in a single line using ‘syslog’ format.

6.17. FAU_SAR.2 Restricted audit review

275 The TOE implements this requirement only for system events.

276 admAPI commands are used for accessing event files. In order to access any of admAPI commands, a TLS connection with PSTi must be made. The CN of the certificate sent to establish the TLS connection is used to identify the administrator.

6.18. FRU_FLT.1 Degraded fault tolerance

277 This requirement applies to high-availability or redundant mode in which 2 elements are operating simultaneously.

278 If an error leads to failure of a secondary element, the primary maintains all TOE functionality, without exceptions.

279 If an error leads to failure of the primary element, the secondary element maintains all security functions except persistent effect commands that are not accepted by the secondary element.

280 This functionality is recovered automatically once the other element is operating correctly. Alternatively, the element can be stopped and reset as an individual element whilst maintaining the rest of the configuration.

6.19. FPT_FLS.1 Failure with preservation of secure state

281 The two elements are connected using a crossover network cable between the two internal units which allows synchronization of the configuration at all times and permits detection of an operating failure in one of the elements.

282 In the event of this happening, the functioning element maintains the configuration and, subsequently, the security features.

6.20. FPT_TRC.1 Internal TSF consistency

283 After failure of one of the elements, the first action taken during recovery, before service operation, is to synchronize the configuration of the internal units of the two elements (primary and secondary).

6.21. FPT_ITT.1 Basic internal TSF data transfer protection

284 In a cluster configuration, the internal units of the primary and secondary elements are connected by a dedicated cable, without switches or other intermediate network elements. The TLS protocol is used to establish an encrypted connection and digital certificates are used for authentication with the other party. The configuration of the authentication requirements forms part of the local configuration.