Security Target Lite

Revision 1.2

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1. Security Target Reference

1 **Title**: PSTmail Security Target

2 **Security Target version**: 1.2

3 **Author**: Autek Ingeniería, S.L.

4 **Security Target date**: July 12, 2011

5 **Product name**: PSTmail

6 **Product version**: 3.0.5

1.2. TOE Overview

1.2.1. TOE Usage

7 PSTmail is a system which allows the exchange of e-mail between two TCP/IP networks with various degrees of classification or security policies which would impede their connection through any other means. The two networks are not equivalent: one is considered to have a higher classification degree or security level. PSTmail guarantees the impossibility of any type of traffic between the two networks except the mail transferred by the system itself.

8 The system is exclusively administered from the securest network.

9 The supported email protocols are those which are standard in Internet: POP3 and IMAP4 for receiving and SMTP for sending. The gateway does not substitute the mail servers of the two networks but rather uses them as intermediary elements for sending and receiving the messages.

10 The mail enters a secure network in a transparent way for the users, even though filtering policies, conditional forwarding can be applied and it can be sent to various internal accounts.

11 The outgoing mail requires authorization by way of an electronic signature of each of the messages in order to leave the secure network.

1.2.2. TOE Type

12 PSTmail is a software email gateway wich allows the email interchange betwen two separated networks. Messaging traffic flow is controlled by configurable policies.

13 A PSTmail element is made up of two computers called 'units'. Each unit is connected to one of the networks. The unit connected to the internal network will be called PSTi and the one connected to the external network PSTe. Both units' computers are

dedicated, i.e. they run no software applications appart from the ones that constitute PSTmail.

14 The TOE includes the specific software components that run on the units and the auditing service 'PSTaud'.

15 PSTmail requires a secure physical use environment.

1.2.2.1. Required Hardware and Software

16 The main part of the TOE runs on two specific servers supplied by the developer, running Windows Embedded Standard. The supported version of the servers is S2. Internal units include a pasive transfer device.

17 A standard PC on which to install and run the auditing service is required. The minimum requirements for this PC are a 1GHz or higher processor, at least 1GB of RAM and running Microsoft Windows XP SP3 or higher.

18 Required hardware and software in the TOE environment:

- A standard PC on which to install and run the administration application PSTadm is required. The minimum requirements for this PC are a 1GHz or higher processor, at least 1GB of RAM and running Microsoft Windows XP SP3 or higher.
- Public Key Infrastructure
- Syslog server(s)(Internal network)
- ODBC accesible database server for transfers auditing (Internal network)
- Email servers
- Email clients supporting S/MIME (Internal network)

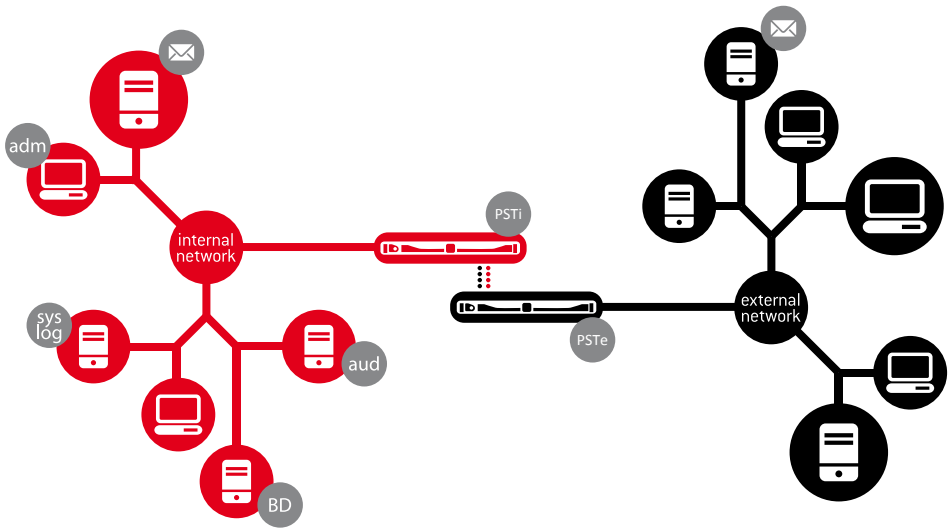

Figure 1. PSTmail environment

1.3. TOE Description

1.3.1. Physical Scope

19 The TOE includes the specific software components that run on the units and the auditing service 'PSTaud'.

20 The following documents are also considered part of the TOE:

21 [IG] Installation and Deployment Guide. Ref 0521-14

22 [OG] Operation Guide. Ref. 0521-15

1.3.2. Logical Scope

23 TOE provides the following functionality:

- Incoming Mail
- Outgoing Mail
- Administration (Administration features offered by PSTmail units)
- Auditing

1.3.3. System Description

24 The fundamental component of PSTmail consists of two computers called ‘units’. Each unit is connected to one of the networks. The one connected to the internal network is called PSTi and the one connected to the external network is called PSTe. These are dedicated computers; i.e. no software application is executed on them apart from those of PSTmail. They are supplied with all the required software installed.

- **PSTmail element**

  Each pair of PSTi and PSTe units forms an element. The element also includes the hardware device used for communication between the units.

  There are two possible configurations: standard –formed by an element– and high availability –formed by two elements in an active-passive redundancy scheme–.

25 The system is also formed by the following software components, which will run on general purpose stations or servers located on the internal network:

- **PSTadm**- Administration application

  The administration of the complete system is carried out from a station on the internal network. The unit located on the external network (PSTe) requires no administration.

- **PSTaud**- Audit records reception service

  Activity data (data of the messages transferred through the gateway) is recorded on a database separate from PSTmail. The job of PSTaud is to enter the data it receives from the internal unit into the database.

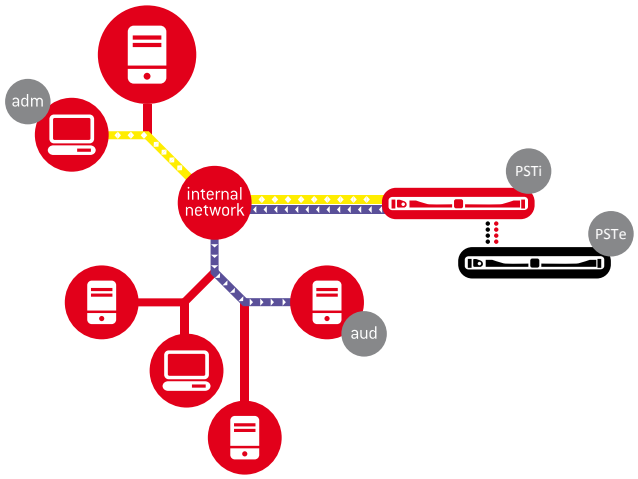

Figure 2. PSTmail components

1.3.4. Incoming Mail

26 The gateway manages incoming mail transparently: it periodically checks the external network mailboxes which are configured, enters the messages it finds into the internal network and sends them to the destination accounts on the internal network which are established by configuration.

- Incoming mail channel

  This is the name given to the correspondence between an external network mailbox and one or more internal network mailboxes. The simplest case is for each user to have an account on each of the networks and hence for correspondence to be 1 to 1.

  There are also a number of parameters that can be individually specified for each channel, such as, a rejection filter and conditional forwarding.

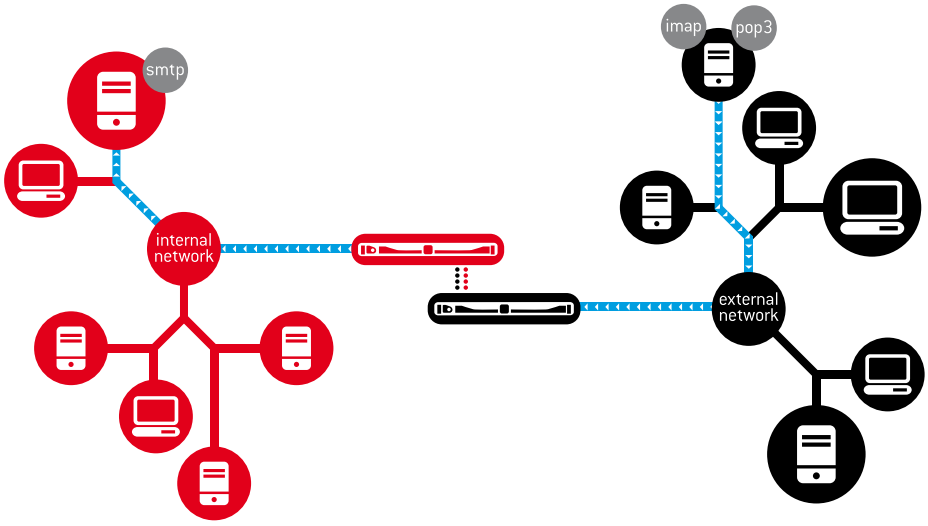

Figure 3. Incoming Mail

1.3.5. Outgoing Mail

27 All outgoing messages need to be authorized by digital signature. PSTi works as a mail server on the internal network and checks the digital signature of each message before sending it to its recipients on the external network.

28 It also deletes any internal network information contained in the message headers and permits basic filtering of the messages by format.

- Supervisor

  Users of the internal network entitled to authorize the sending of messages are called supervisors.

- Outgoing mail channel

  A channel is characterized by the sender's address on the external network. Each channel is assigned a supervisor (or more than one) by configuration.

  The filtering features, and other parameters such as the notification of messages sent, can be configured individually for each channel.

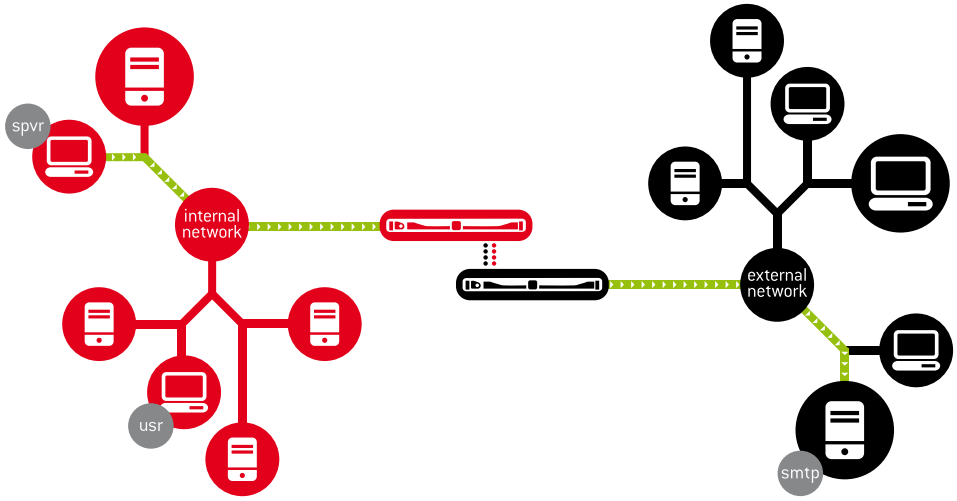

Figure 4. Outgoing Mail

1.3.6. Administration

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

30 Administration takes place from a station on the internal network, through the PSTadm application, which is out of the TOE. PSTadm connects via SSL to the internal unit, PSTi. The gateway also sends system events via the 'syslog' protocol to servers located on the internal network.

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

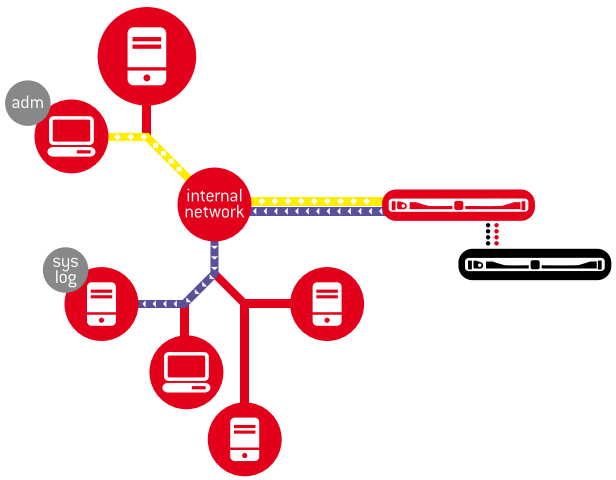

Figure 5. Administración

1.3.7. Auditing

32 Auditing is the recording of information about the transfers made by the system (e.g. messages sent to their recipients on the internal network).

33 The PSTaud software component, installed in a computer on the internal network, is responsible for entering these records into a database outside the system.

34 PSTi automatically connects to PSTaud via SSL.

35 For each service (incoming and outgoing mail), it is possible to configure whether or not auditing information will be sent and the level of detail of the same.

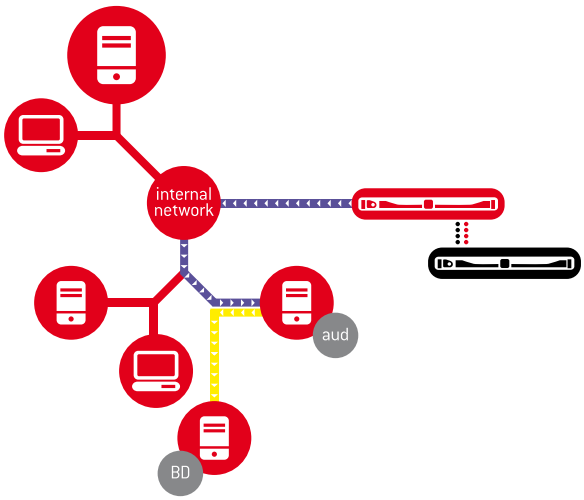

Figure 6. Auditing

1.3.8. Secure Configuration of the TOE

1.3.8.1. Rejection Filter

36 The following configurable filtering conditions, exclusively refer to the names of the attached files declared in the standard form specified in the MIME RFCs:

- Allow files with more than one extension
- Allow files without extension
- Restrict extensions

37 **Rejection filtering does not make any checking of file's content when applying this conditions. Therefore, innumerable possibilities exist for falsifying file names. This must be taken into account and if you want to prevent certain file types to be transmitted some content control product must be used.**

38 Similarly, if a message does not include an attachment's name, it will not be possible to apply rejection filter conditions based on file extensions.

1.3.8.2. Selection Filter

39 For the incoming mail selection mechanism to work properly, the rejection filter must reject messages without standard MIME format.

40 In addition, it should be taken into account that the internal SMTP server used for selection deliveries is a configuration element of the channel. This may not be evident if for example the same selection filter is applied to channels that use different internal SMTP servers.

Destinations Consistency

41 The gateway does not make any checking on destination addresses of channels nor destination of selection filters. It is the administrator's responsibility to check that destination addresses of selection filters are correct.

1.3.8.3. Incoming Mail Filtering Order

42 Filters are run once: the rejection filter is run first and then the selection filter. The rejection filter is defined and applied to a channel, i.e. for messages received at an external address.

1.3.8.4. Outgoing Mail Responsibility

43 An outgoing mail channel is associated with only one external network email address. The supervisors assigned to the channel are the only persons responsible for what is sent through the channel. Both internal network users and supervisors are invisible to the external network. A supervisor’s powers enable them to send anything they consider appropriate through their assigned channels. This includes the possibility of modifying user messages received for authorization purposes.

2. Conformance Claims

2.1. Common Criteria Conformance Claim

44 This Security Target is compliant with the requirements of CC v. 3.1, rel 3, ISO/IEC 15408:2009. This Security Target is functional requirements (Part 2 of CC) conformant and assurance requirements (Part 3 of CC) conformant for EAL4, augmented with ALC_FLR.1.

45 Reference documentation:
FS PSTmail: Functional Specification

2.2. Protection Profiles Conformance Claim

46 This Security Target has been specifically developed for PSTmail's security problem and does not claim conformance to any protection profile.

3. Security Problem Definition

3.1. TOE Assets

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

3.1.1. Information flow

- **A1.IFF-ENT;** Incoming 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 via email, in accordance with the relevant policy and rejection filtering rules of incoming mail. The final destination of the messages introduced in the internal network should be the destination email accounts specified in the corresponding definition of channels and forwarding rules.

- **A2.IFF-SAL;** Outgoing 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 relevant policy and rejection filtering rules of outgoing mail. The final destination of authorised messages on the external network should be the delivery through the servers that were configured to the recipients specified in the original message.

3.2. Threats

3.2.1. Information flow

- **T1.IFF-ENT;** An attacker on the internal network receives in his mailbox messages that should be delivered to other mailboxes, in an unauthorizad manner.

- **T2.IFF-SAL;** An attacker on the internal network sends an unauthorized outgoing message through the gateway.

- **T3.IFF-EXT1;** An attacker on the external network manages to introduce information on the internal network through the gateway hardware but using a different flow than that of incoming email.

- **T4.IFF-EXT2;** An attacker on the external network manages to obtain information of the internal network by any other means than authorized outgoing email.

3.3. Assumptions

3.3.1. Operational environment

- **AS1;** No one has access to the hardware of either of the two units (except local administrators). 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 from the operational environment.

- **AS2;** The Internal Network is an isolated network, securely configured and trustworthy. The external Network is a physically controlled network (no new machines can be connected to the network) and with security measures in place (firewalls on their connections to other networks, securely configured machines and with the latest updates and security patches, etc.) but that it is connected by TCP / IP to other networks.

- **AS3;** The platform (TOE environment) will be designed and securely configured so as to avoid attacks through the platform itself.

3.4. Organizational policies

3.4.1. Design Criteria

- **P1.SEP;** Both networks must remain separate. There should be no possibility of establishing TCP / IP connections between the two networks.

- **P2.SAL;** The outgoing email messages (i.e. those directed from the Internal Network to the External Network) should be authorized by electronic signature.

- **P3.CRYPT;** The information (regarding configuration and that processed by the system) which is stored on disk drives in the units (PSTi and PSTe) must be encrypted *as should communications for remote administration and logging of auditing data*.

- **P4.ROLES;** PSTmail must implement the following roles, with the indicated capabilities:

    1. **Root administrator:**

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

    2. **Security Administrator:**

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

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

    3. **Services Administrator:**

        1. Establishes all the configuration of services (incoming and outgoing mail).

        2. Can start and stop incoming and outgoing mail 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 (incoming and outgoing mail).

5. **Local Administrator:**

    1. Establishes the local configuration of internal units.

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.

- **P5.AUDITORIA;** PSTmail will implement a mechanism to log its activity.

4. Security Objectives

4.1. Security Objectives for the TOE

- **O1.FLUJO;** PSTmail 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 email 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 email, according to the definition of channels and forwarding rules.

- **O2.ROLES;** PSTmail must implement the following roles, with the indicated capabilities:

    1. **Root administrator:**

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

    2. **Security Administrator:**

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

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

    3. **Services Administrator:**

        1. Establishes all the configuration of services (incoming and outgoing mail).

        2. Can start and stop incoming and outgoing mail 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 (incoming and outgoing mail).

    5. **Local Administrator:**

        1. Establishes the local configuration of internal units.

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.

- **O3.AUDITORIA;** PSTmail will implement a mechanism to log its activity.

4.2. Security Objectives for the Operational Environment

- **O.ENV.AS1;** 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.

- **O.ENV.AS2;** The Internal Network is an isolated network, securely configured and trustworthy. The external Network is a physically controlled network (no new machines can be connected to the network) and with security measures in place (firewalls on their connections to other networks, securely configured machines and with the latest updates and security patches, etc.) but that it is connected by TCP / IP to other insecure networks.

- **O.ENV.AS3;** The platform (TOE environment) will be designed and securely configured so as to avoid attacks through the platform itself.

- **O.ENV.AS4;** The cryptographic operations use Windows cryptography 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.

    - Verification of the signature of outgoing messages

    - TLS connection establishment for administration and sending of auditing data

- **O.ENV.AS5;** Network separation. The hardware architecture must ensure that there is a different host on each of the networks. The communication between both hosts should be done by means of a passive device for information exchange.

4.3. Justification of Security Objectives

	O1.FLUJO	O2.ROLES	O3.AUDITORIA
P2.SAL	X		
P4.ROLES		X	
P5.AUDITORIA			X
T1.IFF-ENT	X		
T2.IFF-SAL	X		
T3.IFF-EXT1	X		
T4.IFF-EXT2	X		

Table 1. Security Objectives for the TOE

48 The flow control objective (O1.FLUJO) mitigates following threats T1.IFFENT, T1.IFF-SAL, T1.IFF-EXT1, EXT2 T1.IFF-and complies with the P2.SAL policy.

49 The roles and capabilities objective (O2.ROLES) enforces the P4.ROLES policy compliance, except in the case of the Local Administrator (see below).

50 The (O3.AUDITORIA) objective ensures P5.AUDITORIA policy compliance.

	O.ENV.AS1	O.ENV.AS2	O.ENV.AS3	O.ENV.AS4	O.ENV.AS5
P1.SEP					X
P2.SAL				X	
P3.CRYPT				X	
AS1	X				
AS2		X			
AS3			X		

Table 2. Security Objectives for the Operational Environment

51 The O.ENV.AS1 objective for the environment ensures that the AS1 assumption of the environment is directly fulfilled.

52 The O.ENV.AS2 objective for the environment ensures that the AS2 assumption of the environment is directly fulfilled.

53 The O.ENV.AS3 objective for the environment ensures that the AS3 assumption of the environment is directly fulfilled.

54 The O.ENV.AS4 objective of the environment ensures the fulfillment of the following policies:

- P2.SAL for signature verification

- P3.CRYPT in the encryption of the data being written to the disk on both units

55 The O.ENV.AS5 objective of the environment enforces the P1.SEP network separation policy.

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

56 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

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

5.1.1.1.3. FMT_SMR.2.3

58 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 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

59 The TSF shall be capable of performing the following management functions: [assignment: *Root Administrator, Security Administrator, Services Administrator, Monitoring Administrator: the ones showned in Table 3; Local Administrator: Local setting of statical configuration on the internal unit PSTi (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)*].

5.1.1.3. FIA_UID.2 User identification before any action

5.1.1.3.1. FIA_UID.2.1

60 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.2 User authentication before any action

5.1.1.4.1. FIA_UAU.2.1

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

62 **Note**: Local Administrator is only authenticated by means of a password which he provides the first time he accesses the local configuration interface. Environment organizational measures must deny physical access to people 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

63 The TSF shall enforce the [assignment: *"Incoming and outgoing message filters and policy"*] to restrict the ability to [selection: change_default, query, modify, delete] the security attributes [assignment: *of section 5.1.2.1 for incoming mail and of section 5.1.2.2 for outgoing mail*] 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

64 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

65 The TSF shall enforce the [assignment: *"incoming message filters and policy", "outgoing message filters and 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

66 The TSF shall allow the [assignment: *Services Administrtor*] 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

67 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

68 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

69 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 functionalities shown in Table 3, attribute functionality Id].*

5.1.1.9.2. FDP_ACF.1.2

70 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

71 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**
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	
CU9	Reset of statistical information				X

Table 3. Functionality available to administration roles

5.1.1.9.4. FDP_ACF.1.4

72 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

73 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

74 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. Incoming mail flow

75 Incoming mail message flow control is implemented through the definintion of 'input channels'. For the gateway to process messages received at a mail account on the external network, a channel associated with this account must be defined. Up to 5,000 channels can be defined. To establish or edit 'Channels configuration' which completely controls incoming mail message flow, 'Services Administrator' permission is required.

76 The channel definition, determines how PSTmail handles messages received at the associated external mail account. For the sake of clarity a 'basic channel flow', which constitutes the essence of a channel, is introduced. The optional elements 'Rejection Filter' and 'Selection' may or may not be present.

- Basic channel flow
- Rejection Filter (optional)
- Selection (optional)

5.1.2.1.1. Basic channel flow

77 The basic channel flow definition comprises the following:

- External mail account
- External mail server and all configuration elements needed to access the POP or IMAP mail account on the external network.
- Internal network destination addresses

  1 to 20 mail addresses hosted on an internal network server, where messages found on the external account will be moved.

5.1.2.1.2. Rejection Filter

78 A rejection filter can be applied to a channel. The filter enforces some conditions on message format and content. Messages that don't comply with any condition will be rejected.

79 Possible actions on uncompliant messages (rejected):

- Delete
- Send to configurable external network account

80 Filtering conditions:

- Allow or deny (one of both) attached files with listed extensions
- Allow attached files without extension
- Allow attachments with more than one extension
- Maximum attachment size
- Maximum message size
- Maximum number of recipients
- Maximum number of attachments
- Maximum allowed nesting level
- Standard format required

5.1.2.1.3. Selection

81 None, one or many selection conditions can be applied to a channel. They are evaluated after the rejection filter (if any). A selection condition includes a destination internal network address and a boolean condition on some message properties. The first selection condition which is met determines the internal network destination address of the message.

82 Message properties that can be used in the boolean expresion

- MIME type/subtype of the message
- MIME type/subtype of attached files
- Attached file name
- Attached file extension
- Message subject
- Sender
- Sender's domain

5.1.2.2. Outgoing mail flow

83 Outgoing mail message flow control is implemented through the definintion of 'output channels'. For the gateway to allow sending messages with a certain sender address on the external network, a channel associated with this account must be defined. Up to 5,000 channels can be defined. To establish or edit 'Channels configuration' which completely controls outgoing mail message flow, 'Services Administration' permission is required.

84 The gateway performs following operations on a message intended to be sent over a certain channel:

- Authorization verification
- Internal network information sanitization
- Rejection Filter (optional)

5.1.2.2.1. Authorization

85 Every outgoing message must be digitally signed by a supervisor.

86 The gateway checks following conditions before sending a message to external network destination addresses:

- Message must be correctly signed
- The certificate of the signing key must be attached to the message an have been issued by a CA configured in the gateway.
- The CN of the signing certificate must have been assigned to the channel

5.1.2.2.2. Internal network information sanitization

87 All message headers not listed below are removed from the message. In addition, email addresses belonging to internal domains are removed from remaining message headers if present. Internal domains are specified in service configuration.

- Bcc:
- Cc:
- Comments:
- Content-Description:
- Content-Transfer-Encoding:
- Content-Type:
- Date:
- Disposition-Notification-To:
- From:
- In-Reply-To:
- Keywords:
- MIME-Version:
- Organization:

- Priority:
- References:
- Reply-To:
- Subject:
- To:

5.1.2.2.3. Rejection Filter

88 A rejection filter can be applied to a channel. Messages that don't comply with any condition will be rejected.

89 Filtering conditions

- Allow or deny (one of both) attached files with listed extensions
- Allow attached files without extension
- Allow attachments with more than one extension
- Maximum attachment size
- Maximum message size
- Maximum number of recipients
- Maximum number of attachments
- Maximum allowed nesting level

5.1.2.3. FDP_IFC.2 / ENT Complete information flow control

5.1.2.3.1. FDP_IFC.2.1

90 The TSF shall enforce the [assignment: *“incoming mail policy and filtering rules”*] on [assignment:

- *Information: mail messages (as shown in Section 5.1.2.1, “Incoming mail 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

91 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 / ENT Simple security attributes

5.1.2.4.1. FDP_IFF.1.1

92 The TSF shall enforce the [assignment: *"incoming mail policy and filtering rules"*] based on the following types of subject and information security attributes: [assignment:

- *Information: mail messages, attributes required by filtering rules and policies of Section 5.1.2.1, "Incoming mail flow"* .
- *Subjects: external network information source and internal network information destination, entities*]

5.1.2.4.2. FDP_IFF.1.2

93 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 incoming mail messages, mail policy and filtering rules of paragraph 5.1.2.1.*].

5.1.2.4.3. FDP_IFF.1.3

94 The TSF shall enforce the [assignment: *the rules of paragraph 5.1.2.1 that do not apply to the role or identity of the recipient but to message content.*].

5.1.2.4.4. FDP_IFF.1.4

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

5.1.2.4.5. FDP_IFF.1.5

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

5.1.2.5. FDP_IFC.2 / SAL Complete information flow control

5.1.2.5.1. FDP_IFC.2.1

97 The TSF shall enforce the [assignment: *"outgoing mail policy and filtering rules"*] on [assignment:

- *Information: mail messages, (as described in Section 5.1.2.2, "Outgoing mail 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

98 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 / SAL Simple security attributes

5.1.2.6.1. FDP_IFF.1.1

99 The TSF shall enforce the [assignment: *"outgoing mail policy and filtering rules"*] based on the following types of subject and information security attributes: [assignment:

- *Information: mail messages, attributes required by filtering rules and policies of Section 5.1.2.1, "Incoming mail flow".*]
- Sujetos: internal network information source and external network information destination, entities.]

5.1.2.6.2. FDP_IFF.1.2

100 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 outgoing mail messages, mail policy and filtering rules of paragraph 5.1.2.2.*].

5.1.2.6.3. FDP_IFF.1.3

101 The TSF shall enforce the [assignment: *the rules of paragraph 5.1.2.2 that do not apply to the role or identity of the sender but to message content*].

5.1.2.6.4. FDP_IFF.1.4

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

5.1.2.6.5. FDP_IFF.1.5

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

5.1.3. Auditoría

5.1.3.1. FAU_GEN.1 Audit data generation

5.1.3.1.1. FAU_GEN.1.1

104 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

- [asignment: *The following events:*]

Operation Events

AuditServerConnect

AuditServerConnectFail

AuditServerDisconnect

AuditServerCommandFailed

AuditServerUnavailable

ChannelWarning

ChannelError

ChannelOk

ChannelRequestAcceptance

ChannelRequestRejection

ChannelDebug

GlobalFailure

GlobalSystemStartup

GlobalSystemShutdown

GlobalLinkUp

GlobalLinkDown

GlobalLinkFailure

GlobalAuditFailure

GlobalPrimaryConnect

GlobalPrimaryConnectFail

GlobalPrimaryDisconnect

GlobalSecondaryConnect

GlobalSecondaryDisconnect

GlobalPrimaryEnabled

GlobalPrimaryDisabled

GlobalSecondaryEnabled

GlobalSecondaryStandBy

GlobalDebug

ServiceStart

ServiceStop

ServiceFailure

Security Events

AdminConnect

AdminDisconnect

AdminConnectRejection

AdminWriteCommand

AuditServerConnectinSecFail

ChannelRequestSecRejection

ServiceRequestRejection

Incoming mail transfers

SendingTransfer	Message sent to destination accounts on internal network.
RejectionTransfer	Rejected Message.
SelectionTransfer	Message sent to selection destination accounts.
DeletionTransfer	Message deleted from external network mail account.

Outgoing mail trasnfers

OmTransfer	Successful outgoing mail message transfer.
OmFailedTransfer	Outgoing mail message delivery failure.

5.1.3.1.2. FAU_GEN.1.2

105 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, [asignment:]

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

Incoming mail transfers

ChannelId	Channel Id
TransferId	Transfer Id
CycleStartTime	Date and time of mail cycle begin

Optionally, if extended message info loging is enabled:

From	Message sender
To	'To:' recipient of message
Cc	Carbon copy ('Cc:') recipient of message
MimeType	MIME type
Attachment info	For each attachment: Filename and extension, size, MIME type an subtype, number of extensions
IsStandard	Standard format
Nesting	Nesting level
Subject	Subject
SizeKB	Size in KB
ToNumber	Number of 'TO' recipients
CcNumber	Number of 'CC' recipients
AttachmentNumber	Number of attachments

Outgoing mail transfers

ChannelId	Channel Id

TransferId	Transfer Id
AcceptanceTime	Date and time of acceptance of message by the system
SigningAuthority	Internal address of supervisor signing outgoing message
OriginatingUser	Internal address of outgoing message originator
ExternalRcptTo	Message recipient on external network
FailReason (only if delivery failure)	Delivery failure reason
AdditionalInfo (only if delivery failure)	Additional info

Optionally, if extended message info logging is enabled:

From	Message sender
To	'To:' recipient of message
Cc	Carbon copy ('Cc:') recipient of message
MimeType	MIME type
Attachment info	For each attachment: Filename and extension, size, MIME type an subtype, number of extensions
IsStandard	Standard format
Nesting	Nesting level
Subject	Subject
SizeKB	Size in KB
ToNumber	Number of 'TO' recipients
CcNumber	Number of 'CC' recipients
AttachmentNumber	Number of attachments

5.1.3.2. FAU_SAR.1 Audit review

5.1.3.2.1. FAU_SAR.1.1

106 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

107 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.1.2 Restricted audit review

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

5.2. Security Assurance Requirements

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

- EAL4
- ALC_FLR.1

5.2.1. ADV_ARC.1 Security architecture description

Developer action elements:

5.2.1.1. ADV_ARC.1.1D

110 **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

111 **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

112 **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

113 **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

114 **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

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

5.2.1.7. ADV_ARC.1.4C

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

5.2.1.8. ADV_ARC.1.5C

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

5.2.2. ADV_FSP.4 Complete functional specification

Developer action elements:

5.2.2.1. ADV_FSP.4.1D

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

5.2.2.2. ADV_FSP.4.2D

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

5.2.2.3. ADV_FSP.4.1C

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

5.2.2.4. ADV_FSP.4.2C

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

5.2.2.5. ADV_FSP.4.3C

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

5.2.2.6. ADV_FSP.4.4C

123 **The functional specification shall describe all actions associated with each TSFI.**

5.2.2.7. ADV_FSP.4.5C

124 **The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.**

5.2.2.8. ADV_FSP.4.6C

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

5.2.3. ADV_IMP.1 Implementation representation of the TSF

Developer action elements:

5.2.3.1. ADV_IMP.1.1D

126 **The developer shall make available the implementation representation for the entire TSF.**

5.2.3.2. ADV_IMP.1.2D

127 **The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.**

Content and presentation of evidence elements:

5.2.3.3. ADV_IMP.1.1C

128 **The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.**

5.2.3.4. ADV_IMP.1.2C

129 **The implementation representation shall be in the form used by the development personnel.**

5.2.3.5. ADV_IMP.1.3C

130 **The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.**

5.2.4. ADV_TDS.3 Basic modular design

Developer action elements:

5.2.4.1. ADV_TDS.3.1D

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

5.2.4.2. ADV_TDS.3.2D

132 **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 of evidence elements:

5.2.4.3. ADV_TDS.3.1C

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

5.2.4.4. ADV_TDS.3.2C

134 **The design shall describe the TSF in terms of modules.**

5.2.4.5. ADV_TDS.3.3C

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

5.2.4.6. ADV_TDS.3.4C

136 **The design shall provide a description of each subsystem of the TSF.**

5.2.4.7. ADV_TDS.3.5C

137 **The design shall provide a description of the interactions among all subsystems of the TSF.**

5.2.4.8. ADV_TDS.3.6C

138 **The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.**

5.2.4.9. ADV_TDS.3.7C

139 **The design shall describe each SFR-enforcing module in terms of its purpose and relationship with other modules.**

5.2.4.10. ADV_TDS.3.8C

140 **The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFRenforcing modules.**

5.2.4.11. ADV_TDS.3.9C

141 **The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.**

5.2.4.12. ADV_TDS.3.10C

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

5.2.5. AGD_OPE.1 Operational user guidance

Developer action elements:

5.2.5.1. AGD_OPE.1.1D

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

Content and presentation of evidence elements:

5.2.5.2. AGD_OPE.1.1C

144 **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.**

5.2.5.3. AGD_OPE.1.2C

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

5.2.5.4. AGD_OPE.1.3C

146 **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.**

5.2.5.5. AGD_OPE.1.4C

147 **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.**

5.2.5.6. AGD_OPE.1.5C

148 **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.**

5.2.5.7. AGD_OPE.1.6C

149 **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.**

5.2.5.8. AGD_OPE.1.7C

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

5.2.6. AGD_PRE.1 Preparative procedures

Developer action elements:

5.2.6.1. AGD_PRE.1.1D

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

Content and presentation of evidence elements:

5.2.6.2. AGD_PRE.1.1C

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

5.2.6.3. AGD_PRE.1.2C

153 **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.**

5.2.7. ALC_CMC.4 Production support, acceptance procedures and automation

Developer action elements:

5.2.7.1. ALC_CMC.4.1D

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

5.2.7.2. ALC_CMC.4.2D

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

5.2.7.3. ALC_CMC.4.3D

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

Content and presentation of evidence elements:

5.2.7.4. ALC_CMC.4.1C

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

5.2.7.5. ALC_CMC.4.2C

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

5.2.7.6. ALC_CMC.4.3C

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

5.2.7.7. ALC_CMC.4.4C

160 **The CM system shall provide automated measures such that only authorised changes are made to the configuration items.**

5.2.7.8. ALC_CMC.4.5C

161 **The CM system shall support the production of the TOE by automated means.**

5.2.7.9. ALC_CMC.4.6C

162 **The CM documentation shall include a CM plan.**

5.2.7.10. ALC_CMC.4.7C

163 **The CM plan shall describe how the CM system is used for the development of the TOE.**

5.2.7.11. ALC_CMC.4.8C

164 **The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.**

5.2.7.12. ALC_CMC.4.9C

165 **The evidence shall demonstrate that all configuration items are being maintained under the CM system.**

5.2.7.13. ALC_CMC.4.10C

166 **The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.**

5.2.8. ALC_CMS.4 Problem tracking CM coverage

Developer action elements:

5.2.8.1. ALC_CMS.4.1D

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

Content and presentation of evidence elements:

5.2.8.2. ALC_CMS.4.1C

168 **The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.**

5.2.8.3. ALC_CMS.4.2C

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

5.2.8.4. ALC_CMS.4.3C

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

5.2.9. ALC_DEL.1 Delivery procedures

Developer action elements:

5.2.9.1. ALC_DEL.1.1D

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

5.2.9.2. ALC_DEL.1.2D

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

Content and presentation of evidence elements:

5.2.9.3. ALC_DEL.1.1C

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

5.2.10. ALC_DVS.1 Identification of security measures

Developer action elements:

5.2.10.1. ALC_DVS.1.1D

174 **The developer shall produce and provide development security documentation.**

Content and presentation of evidence elements:

5.2.10.2. ALC_DVS.1.1C

175 **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.**

5.2.11. ALC_FLR.1 Basic flaw remediation

Developer action elements:

5.2.11.1. ALC_FLR.1.1D

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

Content and presentation of evidence elements:

5.2.11.2. ALC_FLR.1.1C

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

5.2.11.3. ALC_FLR.1.2C

178 **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.**

5.2.11.4. ALC_FLR.1.3C

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

5.2.11.5. ALC_FLR.1.4C

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

5.2.12. ALC_LCD.1 Developer defined life-cycle model

Developer action elements:

5.2.12.1. ALC_LCD.1.1D

181 **The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.**

5.2.12.2. ALC_LCD.1.2D

182 **The developer shall provide life-cycle definition documentation.**

Content and presentation of evidence elements:

5.2.12.3. ALC_LCD.1.1C

183 **The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.**

5.2.12.4. ALC_LCD.1.2C

184 **The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.**

5.2.13. ALC_TAT.1 Well-defined development tools

Developer action elements:

5.2.13.1. ALC_TAT.1.1D

185 **The developer shall provide the documentation identifying each development tool being used for the TOE.**

5.2.13.2. ALC_TAT.1.2D

186 **The developer shall document and provide the selected implementationdependent options of each development tool.**

Content and presentation of evidence elements:

5.2.13.3. ALC_TAT.1.1C

187 **Each development tool used for implementation shall be well-defined.**

5.2.13.4. ALC_TAT.1.2C

188 **The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.**

5.2.13.5. ALC_TAT.1.3C

189 **The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.**

5.2.14. ASE_INT.1 ST introduction

Developer action elements:

5.2.14.1. ASE_INT.1.1D

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

Content and presentation of evidence elements:

5.2.14.2. ASE_INT.1.1C

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

5.2.14.3. ASE_INT.1.2C

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

5.2.14.4. ASE_INT.1.3C

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

5.2.14.5. ASE_INT.1.4C

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

5.2.14.6. ASE_INT.1.5C

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

5.2.14.7. ASE_INT.1.6C

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

5.2.14.8. ASE_INT.1.7C

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

5.2.14.9. ASE_INT.1.8C

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

5.2.15. ASE_CCL.1 Conformance claims

Developer action elements:

5.2.15.1. ASE_CCL.1.1D

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

5.2.15.2. ASE_CCL.1.2D

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

Content and presentation of evidence elements:

5.2.15.3. ASE_CCL.1.1C

201 **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.**

5.2.15.4. ASE_CCL.1.2C

202 **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.**

5.2.15.5. ASE_CCL.1.3C

203 **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.**

5.2.15.6. ASE_CCL.1.4C

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

5.2.15.7. ASE_CCL.1.5C

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

5.2.15.8. ASE_CCL.1.6C

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

5.2.15.9. ASE_CCL.1.7C

207 **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.**

5.2.15.10. ASE_CCL.1.8C

208 **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.**

5.2.15.11. ASE_CCL.1.9C

209 **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.**

5.2.15.12. ASE_CCL.1.10C

210 **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.**

5.2.16. ASE_SPD.1 Security problem definition

Developer action elements:

5.2.16.1. ASE_APD.1.1D

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

Content and presentation of evidence elements:

5.2.16.2. ASE_SPD.1.1C

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

5.2.16.3. ASE_SPD.1.2C

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

5.2.16.4. ASE_SPD.1.3C

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

5.2.16.5. ASE_SPD.1.4C

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

5.2.17. ASE_OBJ.2 Security objectives

Developer action elements:

5.2.17.1. ASE_OBJ.2.1D

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

5.2.17.2. ASE_OBJ.2.2D

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

Content and presentation of evidence elements:

5.2.17.3. ASE_OBJ.2.1C

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

5.2.17.4. ASE_OBJ.2.2C

219 **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.**

5.2.17.5. ASE_OBJ.2.3C

220 **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.

5.2.17.6. ASE_OBJ.2.4C

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

5.2.17.7. ASE_OBJ.2.5C

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

5.2.17.8. ASE_OBJ.2.6C

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

5.2.18. ASE_ECD.1 Extended components definition

Developer action elements:

5.2.18.1. ASE_ECD.1.1D

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

5.2.18.2. ASE_ECD.1.2D

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

Content and presentation of evidence elements:

5.2.18.3. ASE_ECD.1.1C

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

5.2.18.4. ASE_ECD.1.2C

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

5.2.18.5. ASE_ECD.1.3C

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

5.2.18.6. ASE_ECD.1.4C

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

5.2.18.7. ASE_ECD.1.5C

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

5.2.19. ASE_REQ.2 Derived security requirements

Developer action elements:

5.2.19.1. ASE_REQ.2.1D

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

5.2.19.2. ASE_REQ.2.2D

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

Content and presentation of evidence elements:

5.2.19.3. ASE_REQ.2.1C

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

5.2.19.4. ASE_REQ.2.2C

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

5.2.19.5. ASE_REQ.2.3C

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

5.2.19.6. ASE_REQ.2.4C

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

5.2.19.7. ASE_REQ.2.5C

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

5.2.19.8. ASE_REQ.2.6C

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

5.2.19.9. ASE_REQ.2.7C

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

5.2.19.10. ASE_REQ.2.8C

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

5.2.19.11. ASE_REQ.2.9C

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

5.2.20. ASE_TSS.1 TOE summary specification

Developer action elements:

5.2.20.1. ASE_TSS.1.1D

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

Content and presentation of evidence elements:

5.2.20.2. ASE_TSS.1.1C

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

5.2.21. ATE_COV.2 Analysis of coverage

Developer action elements:

5.2.21.1. ATE_COV.2.1D

244 **The developer shall provide an analysis of the test coverage.**

Content and presentation of evidence elements:

5.2.21.2. ATE_COV.2.1C

245 **The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.**

5.2.21.3. ATE_COV.2.2C

246 **The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.**

5.2.22. ATE_DPT.1 Testing: basic design

Developer action elements:

5.2.22.1. ATE_DPT.1.1D

247 **The developer shall provide the analysis of the depth of testing.**

Content and presentation of evidence elements:

5.2.22.2. ATE_DPT.1.1C

248 **The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.**

5.2.22.3. ATE_DPT.1.2C

249 **The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.**

5.2.23. ATE_FUN.1 Functional testing

Developer action elements:

5.2.23.1. ATE_FUN.1.1D

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

5.2.23.2. ATE_FUN.1.2D

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

Content and presentation of evidence elements:

5.2.23.3. ATE_FUN.1.1C

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

5.2.23.4. ATE_FUN.1.2C

253 **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.**

5.2.23.5. ATE_FUN.1.3C

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

5.2.23.6. ATE_FUN.1.4C

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

5.2.24. ATE_IND.2 Independent testing - sample

Developer action elements:

5.2.24.1. ATE_IND.2.1D

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

Content and presentation of evidence elements:

5.2.24.2. ATE_IND.2.1C

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

5.2.24.3. ATE_IND.2.2C

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

5.2.25. AVA_VAN.3 Focused vulnerability analysis

Developer action elements:

5.2.25.1. AVA_VAN.3.1D

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

Content and presentation of evidence elements:

5.2.25.2. AVA_VAN.3.1C

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

5.3. Security Requirements Rationale

	O1.FLUJO	**O2.ROLES**	**O3.AUDITORIA**
FMT_SMF.1 FDP_IFC.2 / ENT FDP_IFF.1 / ENT FDP_IFC.2 / SAL FDP_IFF.1 / SAL 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		X	

	O1.FLUJO	O2.ROLES	O3.AUDITORIA
FIA_UID.2 FIA_UAU.2			
FAU_GEN.1 FAU_SAR.1 FAU_SAR.2 FMT_SMF.1			X

Table 4. Security requirements rationale

5.3.1. Non satisfied dependencies justification

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

5.3.2. Functional security requirements rationale

262 The flow objective O1.FLUJO is satisfied due to the existence of a complete flow control policy (FDP_IFC.2 / ENT for incoming mail and FDP_IFC.2 / SAL for outgoing mail) with the security attributes expressed in FDP_IFF.1 / ENT for incoming mail and FDP_IFF.1 / SAL for outgoing mail 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.

263 The objective O2.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.2 and FIA_UAU.2. Security attributes are managed in accordance with FMT_MSA.1 / ACC and FMT_MSA.3 / ACC. Security attributes based acces control and complete control are enforced by FDP_ACF.1 y FDP_ACC.2.

264 The objective O3.AUDITORIA is satisfied through the functions FAU_GEN.1, FAU_SAR.1 y FAU_SAR.2. Auditing is configurable as stated in FMT_SMF.1

5.3.3. Assurance security requirements rationale

265 The desired security assurance for the TOE is the one provided by EAL4 + ALC_FLR.1 assurance level.

266 EAL4 has been chosen so that the final user can be totally confident that the product has been developed using a systematic engineering approach and development best practices, demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential.

6. TOE summary specification

6.1. FMT_SMR.2 Restrictions on security roles

6.1.1. Administration roles

267 There are 5 distinct administrator roles:

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

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

269 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 PSTmail.

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

271 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

272 Table 3 shows the functions accessible to each administration role: “Root Administrator”, “Security Administrator”, “Services Administrator” and “Monitoring Administrator”.

273 Local Administrator establishes statical config on the internal unit PSTi. Statical config has following attributes:

- Network parameters of both units
- Trusted root certification authorities certificates
- Gateway private key and certificate

- Root Administrators CNs

6.3. FIA_UID.2 User identification before any action

274 Administrators, except the Local ones, have access to security functionality through admAPI functions. In order to access any of admAPI functions, an SSL connection with PSTi must be made. The CN of the certificate sent to establish the SSL connection is used to identify the administrator.

275 Local Administrator identification is done through a password. Local Administrator authentication is exclusively done by means of a password that the local administrator supplies the first time he enters the local configuration interface. Identification is implicit when accessing this interface.

6.4. FIA_UAU.2 User authentication before any action

276 Administrators, except the Local ones, have access to security functionality through admAPI functions. In order to access any of admAPI functions, an SSL connection with PSTi must be made. The CN of the certificate sent to establish the SSL connection is used to identify the administrator.

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

278 Local administrators are authenticated by means of a password.

6.5. FMT_MSA.1 / IFF Management of security attributes

279 Incoming and outgoing message filters and policy are set through admAPI commands. In order to access any of admAPI commands, an SSL connection with PSTi must be made. The CN of the certificate sent to establish the SSL connection is used to authenticate the administrator.

280 For accessing these commands "Services Administration" role is required.

281 The managed attributes for incoming mail are the ones shown in section 5.1.2.1 Incoming mail flow.

282 The managed attributes for outgoing mail are the ones shown in section 5.1.2.2 Outgoing mail flow.

6.6. FMT_MSA.1 / ACC Management of security attributes

283 The local administrator establishes by means of the local configuration interface, the CN of Root administrators in the statical config. Physical access to local configuration interface is restricted through organizational policies of the environment.

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

285 “Root Administrator” role is required for accessing this command.

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

287

6.7. FMT_MSA.3 / IFF Static attribute initialization

6.7.1. Incoming and outgoing message filters and policy

288 Initialization provides a configuration without channels and any other configuration element (included users and supervisors). This precludes any flow nor incoming nor outgoing, 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

289 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

290 Administrators access security functionality through admAPI functions. In order to access any of admAPI functions, an SSL connection with PSTi must be made. The CN of the certificate sent to establish the SSL 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 SSL connection is interrupted.

6.10. FDP_ACC.2 Complete access control

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

6.11. FDP_IFC.2 / ENT Complete information flow control

292 PSTmail's incoming mail service sends a mail message from the External Network to the Internal Network if following conditions are met:

- The message is present in an External Network mailbox for which an incoming mail channel exists in the incoming mail channels configuration.
- The channel to which the messaged belongs is in ON state.
- The message complies with the filtering conditions established for the channel.

293 Incoming mail channels configuration includes the definition of the above mentioned elements: External Network mailboxes that will be checked, channel state (ON / OFF), filtering conditions that will be applied to each channel. This is described in greater detail in section 5.1.2.1 Incoming mail flow.

294 Channel configuration is set through admAPI commands. “Services Administrator” permission is required for accessing these commands.

6.12. FDP_IFF.1 / ENT Simple security attributes

295 See Section 6.11, “FDP_IFC.2 / ENT Complete information flow control”.

6.13. FDP_IFC.2 / SAL Complete information flow control

296 PSTmail's outgoing mail service sends a mail message from the Internal Network to the External Network if following conditions are met:

- The channel the message is intended to be sent through is in ON state.
- Message is properly signed.
- Message has been signed with a certificate issued by a trusted CA.
- The supervisor signing the message, identified by the CN of the certificate, is in the list of the entitled supervisors for the channel.
- The message complies the filtering conditions configured for the channel.

297 Outgoing mail channel configuration includes the supervisors entitled to authorize outgoing messages through this channel, the filtering conditions and the ON / OFF channel state. This configuration is described in greater detail in section 5.1.2.2 Outgoing mail flow.

298 This configuration is set by means of admAPI commands. “Services Administrator” role is required to access this commands.

299 Outgoing mail channel selection for each message is done as follows:

- If the message header field ‘Reply_to:’ is present and its value matches the 'external sender' of any configured channel, the channel is selected.
- Otherwise, the default 'external sender' of the message original sender (user or supervisor) is used.

6.14. FDP_IFF.1 / SAL Simple security attributes

300 See Section 6.13, “FDP_IFC.2 / SAL Complete information flow control”.

6.15. FAU_GEN.1 Audit data generation

301 PSTmail generates two distinct audit data types:

- System events
- Transfers logging

6.15.1. System events

302 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.

303 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.

304 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.

305 GlobalSystemStartUp and GlobalSystemShutdown are the events that signal begin and end of auditing functions.

6.15.2. Transfers logging

306 Incoming and outgoing mail transfer data are logged to an external database through PSTaud. “Security Administrator” role is required for setting the configuration data needed for accessing PSTaud.

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

308 All transfer events log following information: time and date of the transfer, type (incoming or outgoing mail), channel ID, message source and destination and other relevant information as message size, etc.

6.16. FAU_SAR.1 Audit review

309 The TOE implements this requirement only for system events.

310 “Security Administrator” role is required for accessing security system event files.

311 “Services Administrator” role is required for accessing operation system event files.

312 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

313 The TOE implements this requirement only for system events.

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