Autek Ingeniería S.L.U.

Madrid (SPAIN)
Tel.: +34 91 597 46 29
www.autek.es

PSTgateways Framework Security Target Lite

15/12/2025

Table of contents

1. Introduction

1.1. Security Target Reference

Title:	PSTgateways Framework Security Target Lite
Security Target Version:	1.0
Author:	Autek Ingeniería, S.L.U.
Security Target Date:	15/12/2025

Table 1: Security Target Reference

1.2. TOE Reference

TOE Name:	PSTgateways Framework
TOE Version:	4.16.8-A
TOE Alias:	PSTgateways Framework
Manufacturer:	Autek Ingeniería, S.L.U.

Table 2: TOE Reference

1.3. TOE Overview

1 'PSTgateways' is a family of boundary protection devices. They are application-level gateways, which allow the secure transmission of information between networks located in two different security domains.

2 The PSTgateways systems provide real network separation by using two individual appliances (each one connected to one of the aforementioned networks). Each appliance acts as the communication end-point in its associated security domain. This architecture provides a complete break of the TCP/IP stack protocols.

3 The two appliances constitute the only communication path between the internal (high security domain) and the external network (low security domain). The communication between them is performed through a passive data transfer device which is part of the PSTgateways technology.

4 All PSTgateways systems share a common architecture and a common base software (PSTgateways Framework) but differ in the set of 'data flow services' (or simply 'services') that they support. Each service supports the transfer of a type of information (e.g.: file transfer, e-mail, etc.), using standard protocols to communicate with both data networks. The services are completely independent from each other, and when possible offer a one way data flow.

5 All services are organised into channels, allowing independent and parallel handling of multiple data flows with individual settings per channel.

6 The following diagram illustrates the general PSTgateways deployment components:

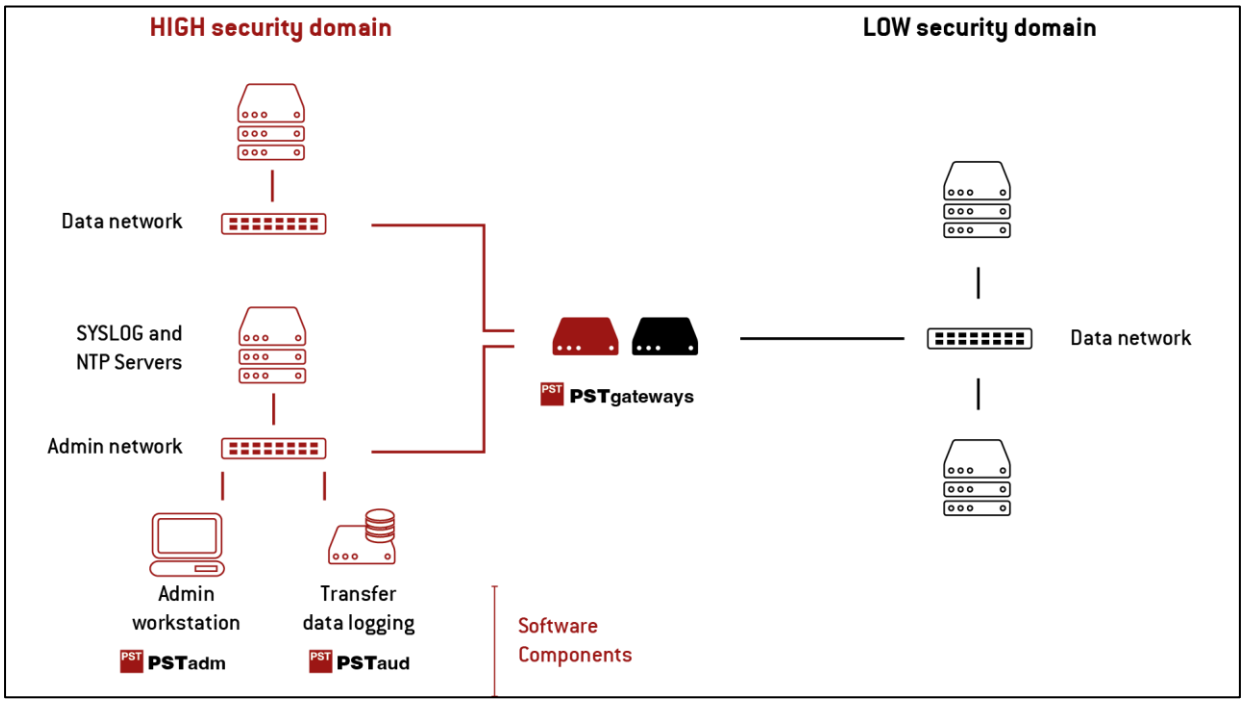


Figure 1: Deployment components of PSTgateways

7 A PSTgateways system consists of:

a. PSTgateways appliances: two appliances (PSTi and PSTe), each consisting of hardware and firmware elements:

i. The PSTgateways appliance's hardware includes the server and other specific HW components required (not part of the TOE)

ii. Each firmware includes the following appliance specific (PSTi or PSTe) components:

1. A minimum operating system.
2. The local administration console, named '**Shell**'.
3. The common (service-independent) software component of PSTgateways, named '**Core**'.
4. The service modules.

b. A firmware management tool for each appliance, named '**Restore**'

c. Additional software intended for administration and audit event management: 'PSTadm' and 'PSTaud' software components. This software is to be deployed on general purpose workstations.

8 The described common (service-independent) software component of the PSTgateways product ('Core'), together with the local administration console ('Shell'), the firmware management tool ('Restore') and their dependencies, constitute the TOE[1] to be evaluated (PSTgateways Framework), which is described in this Security Target document.

1.3.1. TOE Usage and major security features

[1] This statement refers to the software part of the TOE. The TOE is also formed by a documentation part that is described in the section "1.4.1 Physical scope" of this document.

9 The TOE constitutes the main software components common to all products of the PSTgateways family. PSTgateways implement controlled and secure data flows between two networks located in different security domains:

a. 'High Security Domain' network: also referred to as ‘internal network’, located in a security domain that handles a high level of information sensitivity and also has a high level of implemented security. This domain is used also for the administration of the PSTgateways product.

b. 'Low Security Domain' network: also referred to as ‘external network’, located in a security domain with a lower level of information access control measures.

10 The TOE, comprised of the common software of the PSTgateways product (‘Core’), the local administration console (‘Shell’) and the firmware management tool (‘Restore’), is responsible of:

a. Identify and authenticate TOE administrative users.

b. Generate and manage System Events (classified into Operation System Events and Security System Events) and Data Transfer Logging Events (the latter produced by the services modules).

c. Manage all available services, including activation, deactivation and configuration actions, on behalf of conveniently authorised administrators.

d. Monitor the services status and condition.

e. Allow every configured service data flow, while ensuring that no traffic that hasn't explicitly been allowed can traverse from one domain to the other.

f. Apply Administration access controls based on:

i. user authentication using digital certificates.

ii. allowed source IP in the High Security Domain network.

g. Apply data transfer and administration access controls based on allowed MAC addresses. This control can be applied:

i. in the High Security Domain networks (both administration and data internal interfaces).

ii. in the Low Security Domain network (data external interface).

h. Verify the firmware integrity and manage firmware upgrades.

11 The TOE also guarantees that only authorised privileged users can manage its critical functions (audit record management, log access, user management, service and data flow admin) and that a strong authentication mechanism is performed for these users before they are allowed to access the TOE.

12 Access to admin functions and log records is provided only from the High Security Domain network, by using two software tools (PSTadm and PSTaud) which are not part of the TOE. The

administration network can be configured in isolation from or shared with the data network (both in the High Security Domain).

13 The TOE can be configured in a High Availability mode, which requires the use of redundant appliances, and allows the services to stay functional in the event of hardware failures. The two appliances on each domain keep their state and configuration synchronised so that in case of failure the secondary appliances take over the service. Both standalone and high availability configurations are included in the evaluated configuration.

14 The TOE firmware management tool ('Restore') allows an administrator to verify the integrity of the installed firmware (that contains the TOE 'Core' and the TOE 'Shell'). It also allows to verify the integrity and authenticity of any firmware update issued by the manufacturer.

15 All features described in this section are included in the evaluated configuration.

1.3.2. TOE Type

16 The TOE is a distributed software product that constitutes the base framework of a boundary protection device, particularly a secure application level gateway.

1.3.3. Required non-TOE hardware/software/firmware

1.3.3.1. Provided by the manufacturer

17 The following table contains the list of elements that are delivered alongside with the TOE, pre-installed by the manufacturer and ready to use:

Component	Type	Description
Internal Appliance(s) (PSTi)	HW	Server(s) HW hosting the SW belonging to the operational environment for the High Security Domain. These servers are identified with a label that reads "PSTi". The hardware includes the server, a passive data transfer device and a secure key storage cryptodevice. The supported hardware versions are: S6 and above. *NOTE: This appliance also hosts a pre-installed instance of the PSTi firmware.*
External Appliance(s) (PSTe)	HW	Server(s) HW hosting the SW belonging to the operational environment as well as the TOE software for the Low Security Domain. These servers are identified with a label that reads "PSTe". The supported hardware versions are: S6 and above. *NOTE: This appliance contains a pre-installed instance of the PSTe firmware.*
Trusted Platform	SW	Minimum operating system pre-installed in the appliances that allow the PSTgateways software to run.
Service(s)	SW	The TOE works in conjunction with the Data Flow

		Services Modules, which handle the particularities of the different protocols supported by the data flows. These components are pre-installed alongside with the TOE.
Administration Console Software (PSTadm)	SW	PSTadm 4.16.6 or above
Data Transfer Logging Service (PSTaud)	SW	PSTaud 4.16.6 or above.

Table 3: List of HW and SW elements provided by the manufacturer

18 **NOTE**: When in High Availability configuration, a second pair of PSTgateways appliances (PSTi and PSTe) is needed.

1.3.3.2. Not provided by the manufacturer

19 The following table contains the list of elements that are not provided by the manufacturer and must be supplied by the user:

Component	Type	Description
PKI Infrastructure	PKI	A Public Key Infrastructure (PKI) is needed to provide the mandatory certificates that are used to bi-directionally authenticate and secure the communication channel between the TOE and the PSTadm and PSTaud components.
Administration Workstation	HW + SW	A general-purpose computer with the following operating system: Windows 10, Windows Server 2016 or above. PSTadm software will be installed in this computer. This computer can be shared to administrate different PSTgateways instances. Also, different instances of Administration Workstation can be used to simultaneously manage a PSTgateways instance.
Data Transfer Logging Server	HW + SW	A general-purpose computer with the following operating system: Windows 10, Windows Server 2016 or above. PSTaud software will be installed in this computer. A single instance of PSTaud software can be used to receive Data Transfer Logging Events from different PSTgateways products.
Syslog Server(s)	HW + SW	One or two SYSLOG server(s) compatible with standards [RFC3164] and [RFC5424] that are used to store System Events. The use of TLS 1.2 or TLS 1.3 to protect this communication is also supported.
NTP Server(s)	HW + SW	One or more NTP time synchronisation servers.
VGA Monitors	HW	Used to display the local console of the

		appliance(s)
USB keyboards	HW	Used to provide inputs to the local console of the appliance(s)

Table 4: List of needed HW and SW elements not provided by the manufacturer

1.4. TOE Description

1.4.1. Physical scope

20 The TOE is composed of the following elements:

TOE Component	Details	
PSTgateways Framework 'Core' Version 4.16.8	File name	psti
	File format	binary
	SHA256 hash	f6f98ebb1774779a19893e157a6ecc2413c1b185e21b82b0dc07dcabc8401078
	Distribution	(See Table 6)
	File name	servicesi
	File format	binary
	SHA256 hash	ce18b5dc70bfcd89aa0ba67af7f4d66c3ca90681844234844d677a1e468ab34d
	Distribution	(See Table 6)
	File name	pste
	File format	binary
	SHA256 hash	bfb7887d6048664a735ee07c7427a7ae7e0b7f212635e02027083e242201cbdd
	Distribution	(See Table 6)
	File name	servicese
	File format	binary
	SHA256 hash	d7e42c2bc52e9e4385414521be69a95668f9829b835aa1d1857741a2c9cf28ac
	Distribution	(See Table 6)
PSTgateways Framework 'Shell' Version 1.6.3	File name	pstshelli
	File format	binary
	SHA256 hash	a21b18aec6a64f4836894f2a3b771617723de95116f8ca5d34c7eb6e53f66862
	Distribution	(See Table 6)
	File name	pstshelle
	File format	binary

	SHA256 hash	553a70adeb38cd131784c9d2a95e896297e5ce95c8b8579efe596406914796ac
	Distribution	(See Table 6)
PSTgateways Framework 'Restore' Version 2.4.2	File name	restore
	File format	binary
	SHA256 hash	0d0c7096c6b7716fabdc7be459c255be6186688cbf7078db5865551b3d6401c9
	Distribution	(See Table 6)
PSTgateways Framework Dependencies Version 3.5.4	File name	libssl.so
	File format	binary
	SHA256 hash	3f3d7fa76a3c47c7fd303416f769d1ecfebb10428904e048e1111d3a50593ea3
	Distribution	(See Table 6)
	File name	libcrypto.so
	File format	binary
	SHA256 hash	eda3b2a95a3db44826eadd3355b64c448d244e8bf3e2571151fa19dc61955238
	Distribution	(See Table 6)
PSTgateways Installation and Deployment Guide Reference: 550-01 Version R12	File name	ig_550-01_r12.pdf
	File format	PDF
	SHA256 hash	60742fe3fa1eae6228adc0dc77170e75f729f171b2cd37562aa0232617da8f3c
	Distribution	(See Table 6)
PSTgateways Operation Guide Reference: 550-02 Version R11	File name	og_550-02_r11.pdf
	File format	PDF
	SHA256 hash	d522050bf47356c624f89edcd0d8ceb7aeaa60b07837dc52e8350212097f6841
	Distribution	(See Table 6)
PSTgateways Framework Secure Use Procedure Reference: 1227-25 Version R0	File name	sug_1227-25_r0.pdf
	File format	PDF
	SHA256 hash	d238a394c71a3bb6199a694136dd32e8fb53bf0b33d887606d167074093f2e85
	Distribution	E-mail

Table 5 Elements of the TOE

21 Due to the distributed and intertwined nature of the TOE, the physical components of the TOE are contained in physical entities that contain both physical components of the TOE and other

non-TOE components. In order to uniquely identify the physical components of the TOE, the relationship between the TOE components and the physical entities that contain them is listed in this section, alongside with an explicit distinction between them.

22 The TOE components included in the persistent storage of each appliance (PSTi and PSTe) are pre-installed by personnel from Autek Ingeniería S.L.U. The appliances are then packed and sent to the customer using a shipping service.

23 The TOE components are also included in three read-only media (DVD/CD) (see below) that are sent to the customer using a shipping service and whose integrity can be verified against a hash that is sent inside an email that is digitally signed by Autek Ingeniería S.L.U.

24 The physical components of all PSTgateways products are depicted in the following table[2]:

Physical Entity	Element type	Details	
Internal appliance (PSTi)	Hardware	Description	PSTgateways internal appliance
		Version	S6 or above
		TOE components	N/A
	Firmware	Description	Persistent storage of internal appliance.
		Version	(See Table 8)
		Hash	(See Table 8)
		TOE components	**PSTgateways Framework 'Core'** version 4.16.8 (PSTi part)
			PSTgateways Framework 'Shell' version 1.6.3 (PSTi part)
			PSTgateways Framework 'Dependencies' version 3.5.4 (PSTi part)
External appliance (PSTe)	Hardware	Description	PSTgateways external appliance
		Version	S6 or above
		TOE components	N/A
	Firmware	Description	Persistent storage of external appliance.
		Version	(See Table 8)
		Hash	(See Table 8)
		TOE components	**PSTgateways Framework 'Core'** version 4.16.8 (PSTe part)

[2] This is a general description. The particular version and hash of each PSTgateways product element that has been evaluated, are depicted in the Table 8 of section 1.4.3 Evaluated configuration.

			PSTgateways Framework 'Shell' version 1.6.3 (PSTe part)
DVD-ROM Internal appliance (PSTi)	DVD-ROM image	Description	PSTgateways internal appliance DVD-ROM.
		Version	(See Table 8)
		Hash	(See Table 8)
		TOE components	**PSTgateways Framework 'Restore'** version 2.4.2
			PSTgateways Framework 'Dependencies' version 3.5.4
	Firmware image	Description	Image of the PSTi firmware. **Note:** The same as 'Internal appliance (PSTi)' firmware
DVD-ROM External appliance (PSTe)	DVD-ROM image	Description	PSTgateways external appliance DVD-ROM.
		Version	(See Table 8)
		Hash	(See Table 8)
		TOE components	**PSTgateways Framework 'Restore'** version 2.4.2
			PSTgateways Framework 'Dependencies' version 3.5.4
	Firmware image	Description	Image of the PSTe firmware. **Note:** The same as 'External appliance (PSTe)' firmware.
CD-ROM PST software	CD-ROM image	Description	PSTgateways administration software and user documentation.
		Version	(See Table 8)
		Hash	(See Table 8)
		TOE components	**PSTgateways - Installation and Deployment Guide'** (Version: See Table 5)
Others	Email message	Description	Email with CD-ROM hashes and TOE Secure Use Procedure
		Version	(See Table 8)
		Hash	(See Table 8)
		TOE components	**PSTgateways Framework Secure Use Procedure** (Version: See Table 5)

Table 6: Distribution of the TOE

1.4.2. Logical scope

25 The TOE functionality is implemented in the following software components:

a. The **PSTgateways Framework 'Core' component**, version 4.16.8, which is the common (service-independent) software component of the PSTgateways products. Part of the 'Core' runs on the internal appliance (PSTi) and part on the external appliance (PSTe).

b. The **PSTgateways Framework 'Shell' component** version 1.6.3, which is the local administration console for each appliance. Part of the 'Shell' runs on the internal appliance (PSTi) and part on the external appliance (PSTe).

c. The **PSTgateways Framework 'Restore' component**, version 2.4.2, which is the firmware management tool ('Restore') for the internal (PSTi) and external (PSTe) appliances.

d. The **PSTgateways Framework 'Dependencies'**, version 3.5.4, which are the cryptographic libraries used by the other TOE components to perform cryptographic operations.

26 The following table includes the components of the TOE that implement the declared security functionality:

TOE: PSTgateways Framework 4.16.8-A		
Component	Version	Description
Core	4.16.8	The common (service-independent) software component of the PSTgateways products. This element is distributed in two parts: 'Core' PSTe part (running in the external appliance), 'Core' PSTi part (running in the internal appliance) and their dependencies.
Shell	1.6.3	The local administration console. This element is distributed in two parts: 'Shell' PSTe part (running in the external appliance), 'Shell' PSTi part (running in the internal appliance) and their dependencies.
Restore	2.4.2	The firmware management tool for the internal (PSTi) and external (PSTe) appliances and their dependencies.

Table 7: Elements constituting the TOE

27 **NOTE**: PSTgateways products share a common base framework and differ in the supported data flows, called 'services'. The evaluated configuration is described in the section "1.4.3 - Evaluated configuration".

28 The security functions that are implemented by the TOE are described in the following subsections, grouped by type.

1.4.2.1. TOE Administration

29 The TOE administration can only be performed by defined administrator users, whose associated role is explained in the following paragraphs.

30 The TOE implements a hierarchy of administrator roles:

a. One local administrator role, which is a human user with physical access to the TOE, and whose password for using the local administration console ('Shell') is initialised during the initial configuration process. The local administrator

functions are always exercised from the appliance local physical console. The local administrator capabilities are:

i. System status check.

ii. Access to firmware components version information.

iii. Firmware updates.

iv. Local configuration: configuration of initial parameters (that are rarely modified after the initial setup procedure). This configuration can only be performed in the internal appliance (PSTi) and implies the detention of all data flow services:

1. The minimal parameters of the local configuration that must be set are:

a. IP configuration of each network interface

b. PKI-related configuration.

2. Other optional[3] local configuration parameters are:

a. Configuration, on the High Security domain interface(s), of MAC address filtering for internal data interface, internal administration interface and external data interface.

b. NTP Server configuration

c. High Availability configuration.

d. Changing of the default local console session parameters.

v. Import and export the local configuration data

b. Four remote administrator roles:

i. Root administrator, who manages other administration roles and can impose restrictions on what IP addresses in the internal or dedicated administrative network can access the remote administration API. He can also change the default maximum inactivity time between remote modification commands. He can also import and export the administration configuration data.

ii. Security administrator, which can perform the configuration of the log management policy for Operation System Events and Security System Events, the configuration of the server data for the Data Transfer Logging Events (PSTaud), the configuration of syslog server(s), the system time synchronisation, the remote system reboot and the import and export of the audit events configuration data. The security

[3] 'Optional' means that either it is not necessary to configure the parameter or there is a default value for it.

administrator can also remotely access the Security System Events, view values of local parameters and backup Security System Events.

iii. Service administrator that can configure and manage data flow services. The service administrator can also remotely access the Operation System Events and import/export the configuration of the data flow services and/or its associated channel configuration data, and has access to the following additional functions:

1. Access to global system status
2. Backup of Operation System Events
3. Reset of Service data flow statistics

iv. Monitoring administrator, which can access the general device status data, perform monitoring actions of the services and channels and reset service statistics.

31 The remote administrators can perform their functions by means of the admAPI. This API is accessible by using a TLS channel and so the administration data communication is managed in a channel that is isolated from the service data flows. This admAPI is only exposed:

a. In a dedicated administrative interface connected to a dedicated network in the High Security Domain, provided that the dedicated administrative interface has been configured.

b. In the internal network (High Security Domain), if the dedicated administrative interface is not in use.

1.4.2.2. Identification and authentication of users

32 For the local administrator, the identification is implicitly made by the fact that physical access to the console is required and the physical environmental restrictions will apply. Authentication of that user against the 'Shell' component is performed by using a password that has previously been initialised during the initial configuration process. For the 'Shell' component, the only action allowed to the local administrator without authentication is the system status check (any other action is not allowed before the Local Administrator has been authenticated to the system). The 'Restore' component is accessible without authentication because the local user has to boot from the appliance's DVD and that physical access is considered an implied authentication.

33 The mutual identification and authentication between the remote users[4] and the TOE relies on a PKI infrastructure provided externally to the TOE, from which the following certificates and configuration parameters have to be provisioned in the TOE to support this mechanism:

a. One or more CA certificate chains, used to validate certificates presented to the TOE identification and authentication of remote administrators. These

[4] The term 'remote user' of the TOE must be understood as a human user that is accessing the TOE's PSTadm API (using PSTadm) that uses a certificate to authenticate himself to the TOE.

certificates must be configured by the local administrator using the local administration console ('Shell') of the internal appliance (PSTi).

b. One appliance certificate, including its private key, used by the TOE to identify and authenticate itself to the remote administrators. The signing CA chain of this certificate must be made available to the remote users to allow them to verify it. This certificate must be configured by the local administrator using the local administration console ('Shell') of the internal appliance (PSTi).

c. Common Name of certificates associated to the remote administrator users must be provisioned in the TOE:

   i. Root administrators: the local administrator, using the local administration console ('Shell') of the internal appliance (PSTi), can configure up to 5 root administrators common names (CN), which must match the CN of the certificates used by the root administrators of the TOE.

   ii. Security, Service and Monitoring administrators: the root administrator, accessing admAPI, can configure the common names of the non-root remote administrators, which must match the CN of the certificates used by these administrators of the TOE.

34 For remote administrator users, the identification is made through the use of the Common Name of user certificates. The user is required to establish a TLS session with the TOE prior to communicate with it. During this establishment, he must present his certificate to the TOE and the TOE must be able to validate it. The TOE identifies the user using his certificate's Common Name (CN) and authenticates him by verifying his certificate (the TOE has been provisioned with the CA Certificate of the issuing CA by the local administrator during the initial configuration procedure, so it can also authenticate the user). The TOE also authenticates itself to the user during the TLS session establishment by using its appliance certificate[5]. If the identification or the authentication fails, the user is not allowed to interact with the TOE.

1.4.2.3. Audit

35 The TOE generates two types of audit events: System Events and Data Transfer Logging Events, as detailed in the following subsections.

1.4.2.3.1. System Events

36 System Events are generated by the TSF and stored in local event files in the internal appliance PSTi. They are also sent to the configured syslog server(s). These events can also be accessed by using admAPI. There are two types of System Events:

a. Security System Events.

b. Operation System Events.

37 The System Events contain the following information:

[5] The appliance certificate is also provided by the customer and is signed by a CA chain that has to be available to the remote users. The appliance certificate must include the private key.

a. Priority: includes the Facility, one value for each event type (Security or Operation), and Severity, which can take one of the following values: Debug (7), Informational (6), Notice (5), Warning (4), Error (3) and Critical (2).

b. Date and time.

c. Source IP: IP address of the internal appliance.

d. Tag: Device identifier, consisting in the Common Name of the internal appliance (PSTi) certificate.

e. System event and specific event information, containing the details of the event.

f. Those events generated as a result of an administrator action include the administrator identifier (Common Name of his certificate).

38 The TOE stores the System Events in files that are rotated accordingly with the established policy that is based on file size and maximum file number. The latest event file is overwritten when the maximum file number is reached (a System Event is generated in this case).

39 The TOE provides access to the System Events by the use of the admAPI that can be securely accessed by the remote PSTadm workstation. This information is in the form of a human-readable text log file. The access through PSTadm requires the previous establishment of a secure communication channel (using TLS 1.2 or higher). The access to Security System Events is restricted to the Security Administrator roles and the access to the Operation System Events is restricted to Service Administrator roles.

40 The System Events can also be sent by the TSF to syslog servers located in the High Security Domain: one for the Operation System Events and one for the Security System Events (Both types of events can be sent to the same server). These transfer operations can also be configured to be protected by TLS 1.2 or higher, that provides mutual authentication, integrity protection and confidentiality protection.

1.4.2.3.2. Data Transfer Logging Events

41 Data Transfer Logging Events are directly related with each data flow transfer. Each of these events is associated to a particular service data transfer and the information in them is specific for each service. The Data Transfer Logging Events are sent by the TSF to the configured PSTaud server and they are not accessible through the admAPI.

42 Data Transfer Logging Events are sent by the TSF to the PSTaud server located in the High Security Domain using the audAPI provided by the PSTaud server, if the Security Administrator has configured the CN (Common Name) of the certificate associated to the remote PSTaud service. The TSF securely transmits these events to the PSTaud server by establishing a secure communication channel (TLS 1.2 or higher) with it, which provides mutual authentication, integrity protection and confidentiality protection. This information is stored by the PSTaud server and is presented to the user accessing the PSTaud software in a structured way.

1.4.2.4. TOE access protection

43 The TOE is able to limit the maximum number of administrative connections to prevent DoS attacks coming from the internal network.

1.4.2.5. Protection of the TOE

44 The integrity protection of the TOE firmware is provided through the following mechanisms:

a. The TOE is installed in and runs from a read-only partition, so modifications of the TOE are not possible.

b. For each appliance, the local administrator can verify the partition integrity (and therefore the TOE integrity that is located inside it) by booting from the appliance DVD and using the provided TOE firmware management tool ('Restore') to perform the verification of the integrity of the appliance's firmware.

45 Every TOE firmware upgrade comes inside a firmware image with an associated signature file. This firmware image signature is verified by the TOE firmware management tool ('Restore') prior to its installation.

46 The TOE verifies the signature of the license associated to the PSTgateways particular product. The following features are activated by license:

a. Available services.

b. High availability mode.

47 For some specific services, some parametrisation data can also be loaded from the local administration console ('Shell'). In this case, the parametrisation data is protected by the use of a digital signature.

1.4.2.6. High availability

48 The TOE can operate in a High Availability configuration by using two redundant appliances (one in each security domain). The following functionalities apply only when the High Availability configuration is in place.

49 In High Availability operation mode, one of the internal appliances ("PSTi") must be configured as primary. From that point on, all administration tasks are performed over the primary PSTi, with the exception of "RebootSystem" command and monitoring tasks, which can be performed also on the secondary PSTi.

50 The TOE uses a synchronisation channel using a dedicated TLS channel between the two instances of the PSTi appliances (located in the High Security Domain) to maintain synchronisation between the redundant parts of the system.

51 The High Availability feature can be configured in two modes, that are enabled exclusively by the license associated to the system:

a. Active-Active mode: the primary and secondary appliances share the workload of the service. The configuration of how this sharing operates depends on each service.

b. Active-Passive mode: the secondary appliances have no data interfaces enabled and they take over the workload when a failure on the primary appliances is detected.

52 The TOE keeps synchronised the configuration, global operating status as well as service operational status.

53 When the TOE detects a fault condition on any of the PSTgateways systems, it reconfigures the system to rebalance the data flow service load to the healthy system.

54 When the fault condition disappears:

a. In Active-Active mode, the TOE will re-establish the original system configuration.

b. In Active-Passive mode, the element that took over the load will continue to do so.

1.4.3. Evaluated configuration

55 The TOE has been evaluated using the following PSTgateways product:

PSTgateways COTS distribution 4.13.1		
Physical Entity	**Elements**	**Description**
Internal appliance (PSTi)	Hardware	PSTi-S6.03
	Firmware	**Version:** PSTgateways COTS 4.13.1 – Internal appliance (PSTi-S6) **SHA-256:** fe38492ea98538befc582c3621d069febf5df237eaf01e7ad8080e83a59d8de9
External appliance (PSTe)	Hardware	PSTe-S6.03
	Firmware	**Version:** PSTgateways COTS 4.13.1– External appliance (PSTe-S6) **SHA-256:** 60b5e975b9ddcd9f1bbcd0e73944c6f74a3d555da326f2546dbd8c83f29554e6
DVD-ROM Internal appliance (PSTi)	DVD-ROM image	**Version:** PSTgateways COTS 4.13.1 – Internal appliance (PSTi-S6) **SHA-256:** 5069f74c0d3aa369a4b08dc78a2a59809005ba9d2672876b939c1c9af6103669
	PSTi firmware image	(*) The same as 'Internal appliance (PSTi)' firmware
DVD-ROM External appliance (PSTe)	DVD-ROM image	**Version:** PSTgateways COTS 4.13.1 – External appliance (PSTe-S6) **SHA-256:** e332b532fac391d0991ec4161d64796563840ecb974672bda5c761403f738648
	PSTe firmware image	(*) The same as 'External appliance (PSTe-S6)' firmware
DVD-ROM PST	PSTgateways	**Version:** PSTgateways software 4.16.6

software	software CD-ROM image	**SHA-256**: 77ec512bd28b7dd3823e5f32dbad204e820194e7073b96967315f3424339d102
PSTgateways Documentation	'PSTgateways - Installation and Deployment Guide'	**Ref:** 550-01 **Version:** 12 **SHA-256:** 60742fe3fa1eae6228adc0dc77170e75f729f171b2cd37562aa0232617da8f3c
	'PST boundary protection devices – Operation Guide'	**Ref:** 550-02 **Version:** 11 **SHA-256:** d522050bf47356c624f89edcd0d8ceb7aeaa60b07837dc52e8350212097f6841
	'PSTgateways Framework Secure Use Procedure'	**Ref:** 1227-25 **Version:** R0 **SHA-256:** d238a394c71a3bb6199a694136dd32e8fb53bf0b33d887606d167074093f2e85

Table 8: Evaluated configuration

56 The TOE has been evaluated using the following configuration options:

a. The configuration of the system has followed the rules in the document 'PSTgateways Framework Secure Use Procedure' (see Table 8).

b. Both HA and non-HA modes of the system were evaluated.

c. In HA mode, both Active-Active and Active-Passive operation modes were evaluated.

d. Only key sizes that provide a cryptographic strength of 128 bits or higher were used in the evaluation.

2. Conformance claims

2.1. CC conformance claim

57 This Security Target (ST) complies with Common Criteria (CC) Version 3.1 Revision 5 and is conformant to the presentation and content requirements that it establishes.

58 The functional requirements and assurance requirements defined in this ST is conformant with:

a. Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version v3.1r5, extended with the components defined in the section “5 Extended components definition” of this document.

b. Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version v3.1r5.

2.2. PP conformance claim

59 This ST does not claim conformance with any protection profile.

2.3. Package claim

60 This ST is conformant to assurance package EAL4 augmented with ALC_FLR.3 and AVA_VAN.5 defined in Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version v3.1r5.

3. Security problem definition

3.1. Assets

Asset	Description
A.INBOUND_DATA_FLOW	The control of data flows and restriction rules for the information going from the established endpoints located in the Low Security Domain network through the system to the established endpoints located in the High Security Domain network.
A.OUTBOUND_DATA_FLOW	The control of data flows and restriction rules for the information going from the established endpoints located in the High Security Domain network through the system to the established endpoints located in the Low Security Domain network.
A.TSF_DATA	The protection of the integrity and the enforcement of authorised access to all security-relevant data handled by the TOE: local and remote configuration data and audit events.

Table 9: Assets

3.2. Threats

Threat	Description
T.INTOUTLEAK	A user operating in the internal network sends data that is not explicitly allowed by the system to the external network.
T.EXTOUTLEAK	A user operating in the external network extracts data from the internal network.
T.EXTINFEED	A user operating in the external network sends data that is not explicitly allowed by the system to the internal network.
T.INTINFEED	A user operating in the internal network succeeds in introducing data coming from the external network into the internal network that is not explicitly allowed by the system.
T.UACCESS	A user (operating in the internal network or in the external network) gains access to the TSF_DATA.

Table 10: Threats

3.3. Organisational security policies

OSP	Description
P.AUDIT	The TOE will implement a mechanism to log its activity.
P.AVAIL	When high availability mode has been enabled, a high availability mode of operation must be possible where a peer element can take over the services of a failing element.
P.CRYPT	The communications for remote administration and logging of auditing data must be encrypted. Also, the information processed by the system which is stored on temporary storage in both appliances (internal and external) must be encrypted.
P.INTEGRITY	The firmware integrity of the system must be protected, including the installation and updates operations. The system must also provide a way to

	authenticate the origin of a firmware image. Additionally, the system must provide the user a way to verify the firmware integrity on demand.
P.NETSEP	Both internal and external networks must remain separate. There should be no possibility of establishing TCP / IP connections between the two networks.
P.ROLES	The product shall implement a hierarchy of user roles that allows efficient segmentation of administrative privileges and also allows separation of access to different types of audit events. These roles and the associated capabilities will be implemented through the authentication features that allow the policies and access control functions that regulate the authorised exercise of the indicated capabilities to be established.

Table 11: Organisational Security Policies (OSPs)

3.4. Assumptions

Assumption	Description
H.ADMINNOEVIL	The TOE Administrators (administrators that have been authorised accordingly to the administrative role hierarchy) are not malicious and will not try to circumvent any security protection of the TOE or execute any malicious action.
H.NETS	The internal network is an isolated network, that has been secured and, thus, it is considered trusted. The external network has security controls and measures, but may be connected to other TCP/IP networks that are considered not secure.
H.PHYSEC	The TOE is deployed in a physically secure environment. Only authorised personnel have physical access to the TOE.
H.SECPLAT	The platform (TOE environment) will be designed and securely configured so as to avoid attacks through the platform itself.
H.SECUREPKI	The PKI infrastructure is provided by the operational environment and it is assumed that its operation is securely implemented: the key generation and distribution is performed in a way that ensures that the keys are correctly protected in every step of the process (generation and distribution).
H.SINGLECHAN	There are no channels for information to flow between the networks apart from the TOE itself.

Table 12: Assumptions

4. Security Objectives

4.1. Security objectives for the TOE

61 The following table describes the security objectives for the TOE:

Id	Definition
O.AUDIT	The TOE will implement a mechanism to log its operational actions, security actions and data transfer details in the form of audit events that provide reliable timestamps. The access to the audit event trail must be assigned and managed by the TOE. The audit data must be protected from unauthorised deletion, modification of access, both in transit and in the assigned storage.
O.AVAIL	The TOE must optionally (when High Availability mode is enabled) provide a failover solution where the services of a failing element are taken over by a redundant element.
O.FLOW	The TOE implements the following information flow policy: • It should not be possible for information to exit the internal network except for that which is transferred through the gateway itself using the running licensed services. • The entry of information from the external network to the internal network should not be possible, except for that which is transferred through the gateway itself using the running licensed services.
O.PROTECT	The TOE shall provide mechanisms to: • Verify its own integrity. • Access the system installed firmware version. • Verify the integrity and authenticate the origin of a firmware update. • Update the system firmware. • Protect from disclosure the private keys when exporting them to removable storage.
O.ROLES	The TOE shall implement a hierarchy of user roles that allows efficient segmentation of administrative privileges and also allows separation of access to different types of audit events.
O.SECADMIN	The TOE shall provide a secure administration interface and mechanisms that enforce the following: • The TOE shall authenticate all administrators of the TOE before any action (except those explicitly defined) on the TOE can be performed. • The TOE shall enforce that every administrative user role has access only to its associated administration functionalities. • The TOE 'Shell' shall provide a mechanism to authenticate local users by the use of a passphrase. This mechanism should prevent the use of weak passwords and eavesdropping of the passphrase. • The TOE shall implement a mechanism to avoid brute force attacks on the local users authentication interface. • The TOE shall implement a mechanism to limit the number of concurrent remote administrative sessions.

	• The TOE shall implement mechanisms to avoid that an unattended administrative sessions keeps open indefinitely.
O.SECCOMM	The TOE must provide a secure communication channel that is cryptographically protected in integrity and confidentiality for: • The remote administration connections. • The connections to servers receiving the 'Data Transfer Logging Events' data. • The connection to remote syslog servers configured to use TLS The TOE also protects the keys used to implement this protection.

Table 13: List of security objectives for the TOE

4.2. Security objectives for the operational environment

62 The following table describes the security objectives for the operational environment:

Id	Definition
OE.ADMINNOEVIL	The authorised administrators of the TOE must have the necessary knowledge to correctly operate and configure it and they should not perform any malicious actions on the TOE.
OE.CRYPT	The temporary storage of both appliances (PSTe and PSTi) stores the temporary data of the corresponding appliance. The operating system encrypts this storage with a session key that is generated every time the appliance boots up.
OE.FIRMRO	The firmware of the system is always mounted as a read-only partition.
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 may be connected to other TCP/IP networks that are considered not secure.
OE.NETSEP	Network separation. The architecture of the network must ensure that there is no connection between external and internal networks. The hardware architecture must be designed in a way that each appliance is only connected to one of the networks. Communication between these appliances must be exclusively made using a passive information exchange device.
OE.PHYSEC	No access will be granted to the hardware of either of the two appliances (except for the Local Administrator). It is assumed that the obvious ways to circumvent the system (for example, connect both appliances directly through a network cable) are ruled out by physical or organisational 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.SECUREPKI	The PKI infrastructure is provided by the operational environment and it is assumed that its operation is securely implemented: the key generation and distribution is performed in a way that ensures that the keys are correctly protected in every step of the process (generation and distribution).

Table 14: Security objectives for the operational environment

4.3. Security objectives rationale

4.3.1. Tracing

63 The following table contains the relationships between the security objectives and the threats, OSPs and assumptions.

	Security Objective	Organisational Security Policies						Threats					Assumptions					
		P.AUDIT	P.AVAIL	P.CRYPT	P.INTEGRITY	P.NETSEP	P.ROLES	T.INTOUTLEAK	T.EXTOUTLEAK	T.EXTINFEED	T.INTINFEED	T.UACCESS	H.ADMINNOEVIL	H.NETS	H.PHYSEC	H.SECPLAT	H.SECUREPKI	H.SINGLECHAN
Security Objectives for the TOE	O.AUDIT	X																
	O.AVAIL		X															
	O.FLOW							X	X	X	X							
	O.PROTECT				X													
	O.ROLES						X					X						
	O.SECADMIN						X					X						
	O.SECCOMM			X								X						
Security Objectives for the Operational Environment	OE.ADMINNOEVIL							X	X	X	X	X	X					
	OE.CRYPT			X								X						
	OE.FIRMRO				X							X						
	OE.NETS													X				
	OE.NETSEP					X		X	X	X	X							X
	OE.PHYSEC				X			X	X	X	X	X	X		X			
	OE.SECPLAT											X				X		
	OE.SECUREPKI			X			X					X					X	

Table 15: Tracing from Security Objectives to Threats, OSPs and assumptions

4.3.2. Justification

4.3.2.1. Threats to objectives mapping justification

64 T.INTOUTLEAK is mitigated by the objective O.FLOW, which defines the implementation of the necessary controls to avoid the leakage of unauthorised information from the internal network to the external network. Also, OE.PHYSEC helps in the mitigation of this threat because it prevents the physical circumvention of the controls. Additionally, OE.NETSEP makes

sure that the physical implantation and connection of the solution into the customer networks matches the required separation of networks. OE.ADMINNOEVIL also contributes to the mitigation of this threat because it prevents that a malicious administrator could circumvent all the controls implemented by the aforementioned objectives.

65 T.EXTOUTLEAK is mitigated by the objective O.FLOW, which defines the implementation of the necessary controls to avoid the leakage of unauthorised information from the internal network to the external network. Also, OE.PHYSEC helps in the mitigation of this threat because it prevents the physical circumvention of the controls. Additionally, OE.NETSEP makes sure that the physical implantation and connection of the solution into the customer networks matches the required separation of networks. OE.ADMINNOEVIL also contributes to the mitigation of this threat because it prevents that a malicious administrator could circumvent all the controls implemented by the aforementioned objectives.

66 T.EXTINFEED is mitigated by the objective O.FLOW, which defines the implementation of the necessary controls to avoid the introduction of unauthorised information from the external network to the internal network. Also, OE.PHYSEC helps in the mitigation of this threat because it prevents the physical circumvention of the controls. Additionally, OE.NETSEP makes sure that the physical implantation and connection of the solution into the customer networks matches the required separation of networks. OE.ADMINNOEVIL also contributes to the mitigation of this threat because it prevents that a malicious administrator could circumvent all the controls implemented by the aforementioned objectives.

67 T.INTINFEED is mitigated by the objective O.FLOW, which defines the implementation of the necessary controls to avoid the introduction of unauthorised information from the external network to the internal network. Also, OE.PHYSEC helps in the mitigation of this threat because it prevents the physical circumvention of the controls. Additionally, OE.NETSEP makes sure that the physical implantation and connection of the solution into the customer networks matches the required separation of networks. OE.ADMINNOEVIL also contributes to the mitigation of this threat because it prevents that a malicious administrator could circumvent all the controls implemented by the aforementioned objectives.

68 T.UACCESS is mitigated mainly by O.ROLES and O.SECADMIN objectives, which require the implementation of necessary role definition and access controls to ensure that access to TSF Data is only allowed to the authorised user(s). Also, OE.PHYSEC helps in the mitigation of this threat because it restricts physical access to the TOE, eliminating the threats associated to it. Additional, the fact that all administrative and audit transfer communications are protected (O.SECCOM) adds some mitigation to the threat, due to the fact that it makes more difficult for an attacker to impersonate a legitimate administrator or access TSF Data in transit. OE.CRYPT contributes by encrypting TSF Data on disk, mitigating the risk of TSF Data disclosure even in the event of a physical removal of the disk. OE.ADMINNOEVIL and OE.PHYSEC also contribute to the mitigation of this threat because it prevents that a malicious administrator could circumvent all the control implemented by the aforementioned objectives. Finally, the objectives associates to the protection of the integrity of the TOE (OE.FIRMRO and OE.SECPLAT) also contribute to the mitigation by reducing the risk of an attacker that access the TSF Data by tampering the functionality of the system itself. OE.SECUREPKI contributes to the secure implementation of the associated cryptography based on externally-provided certificates.

4.3.2.2. OSP to objectives mapping justification

69 P.AUDIT is directly enforced by O.AUDIT.

70 P.AVAIL is directly enforced by O.AVAIL.

71 P.CRYPT is enforced by OE.CRYPT in the encryption of the persistent or temporary data storage. Regarding the encryption of information in transit, it is enforced by O.SECCOMM. Additionally, OE.SECUREPKI contributes to this policy by ensuring the cryptographic operations that use externally-provided certificates are not compromised by an incorrect protection of these certificates when handled outside the TOE.

72 P.INTEGRITY, which defines the policy of protecting the system's firmware integrity, is enforced by OE.FIRMRO (by ensuring that the firmware is not modifiable in execution), by OE.PHYSEC (which ensures that no physical access is allowed to the installed firmware image) and by O.PROTECT (which ensures that the firmware integrity and authenticity can be verified for both the installed firmware and a firmware update coming from the vendor).

73 P.NETSEP is directly enforced by the implementation of OE.NETSEP.

74 P.ROLES is enforced by O.ROLES and O.SECADMIN. Additionally, OE.SECUREPKI contributes to this policy by ensuring the identification of user identification and authentication is not compromised by an incorrect protection of the associated externally-provided certificates.

4.3.2.3. Assumptions to objectives mapping justification

75 H.ADMINNOEVIL is upheld by OE.ADMINNOEVIL but also by OE.PHYSEC, which guarantees that physical access to the TOE is only granted to the authorised local administrator.

76 H.NETS is completely sustained by OE.NETS.

77 H.PHYSEC is upheld totally by OE.PHYSEC.

78 H.SECPLAT is totally upheld by OE.SECPLAT.

79 H.SECUREPKI is totally upheld by OE.SECUREPKI.

80 H.SINGLECHAN is completely sustained by OE.NETSEP.

5. Extended components definition

5.1. Security Audit (FAU)

5.1.1. Security Audit Event Storage (FAU_STG)

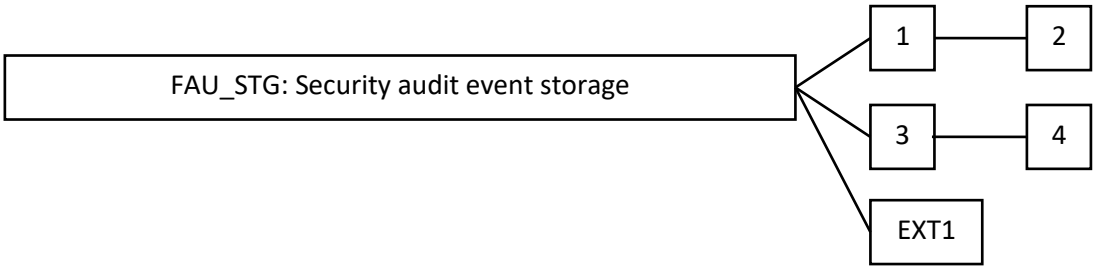
Family Behaviour

81 This family defines the requirements for the TSF to be able to create and maintain a secure audit trail. Stored audit records refers to those records within the audit trail, and not the audit records that have been retrieved (to temporary storage) through selection.

Rationale

82 This family is extended with component EXT1 to define the requirements for the TSF to be able to securely transmit audit data between the TOE and an external IT entity.

Component levelling



83 FAU_STG.EXT1 Security Audit Event Storage requires the TSF to use a trusted channel implementing a secure protocol.

Management: FAU_STG.EXT1

84 The following actions could be considered for the management functions in FMT:

a. The TSF shall have the ability to configure the cryptographic functionality.

Audit: FAU_STG.EXT1

85 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. No audit necessary.

5.1.1.1. FAU_ STG.EXT1 Security Audit Event Storage

Hierarchical to:	No other components
Dependencies:	FAU_GEN.1 Audit data generation
	FTP_ITC.1 Inter-TSF Trusted Channel

FAU_STG.EXT1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1

FAU_STG.EXT1.2 The TSF shall be able to store generated audit data on the TOE itself. In addition [selection:

- The TOE shall consist of a single standalone component that stores audit data locally,
- The TOE shall be a distributed TOE that stores audit data on the following TOE components: [assignment: identification of TOE components],
- The TOE shall be a distributed TOE with storage of audit data provided externally for the following types of audit events: [assignment: list of audit event types for which the TOE transmits their generated audit data and a description of the destination of such transmission].]

FAU_STG.EXT1.3 The TSF shall [selection: drop new audit data, overwrite previous audit records according to the following rule: [assignment: rule for overwriting previous audit records], [assignment: other action]] when the local storage space for audit data is full.

5.2. Cryptographic Support (FCS)

5.2.1. TLS Client Cryptographic Protocol (FCS_TLSC_EXT)

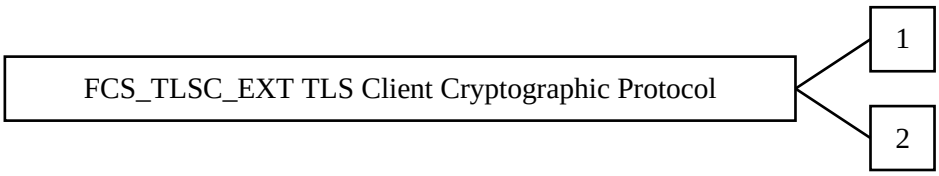
Family Behaviour

86 The component in this family addresses the ability for a client to use TLS to protect data between the client and a server using the TLS protocol.

Rationale

87 This family is introduced because no similar family is available in [CCPART2].

Component levelling



88 FCS_TLSC_EXT.1 TLS Client requires that the client side of TLS be implemented as specified.

89 FCS_TLSC_EXT.2 TLS Client requires that the client side of the TLS implementation include mutual authentication.

Management: FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

90 The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

91 The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a. Failure of TLS session establishment

b. TLS session establishment

c. TLS session termination

5.2.1.1. FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

Hierarchical to:	No other components
Dependencies:	FCS_CKM. 1 Cryptographic Key Generation
	FCS_CKM.2 Cryptographic Key Distribution
	FCS_COP.1 Cryptographic operation
	FCS_RBG_EXT.1 Random Bit Generation
	FIA_X509_EXT.1 X.509 Certificate Validation
	FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_TLSC_EXT.1.1 The TSF shall implement [selection: TLS 1.2 [RFC5246], TLS 1.1 [RFC4346], TLS 1.3 [RFC8446]] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [assignment: list of optional ciphersuites and reference to RFC in which each is defined] and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF, if configured to do so, shall verify that the presented identifier matches [selection: the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN, IPv6 address in the CN or SAN, IPv4 address in SAN, IPv6 address in the SAN, the identifier per RFC 5280 Appendix A using [selection: id-at-commonName, id-at-countryName, id-at-dnQualifier, id-at-generationQualifier, id-at-givenName, id-at-initials, id-at-localityName, id-at-name, id-at-organizationalUnitName, id-at-organizationName, id-at-pseudonym, id-at-serialNumber, id-at-stateOrProvinceName, id-at-surname, id-at-title, none] and no other attribute types].

FCS_TLSC_EXT.1.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [selection:

- Not implement any administrator override mechanism
- Require administrator authorisation to establish the connection if the TSF fails to [selection: match the reference identifier, validate

certificate path, validate expiration date, determine the revocation status] of the presented server certificate

FCS_TLSC_EXT.1.4 The TSF shall [selection: not present the Supported Elliptic Curves/Supported Groups Extension, present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups: [selection: secp224r1, secp256r1, secp384r1, secp521r1, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1] and no other curves/groups] in the Client Hello.

5.2.1.2. FCS_TLSC_EXT.2 TLS Client support for Mutual Authentication

Hierarchical to:	No other components
Dependencies:	FCS_CKM. 1 Cryptographic Key Generation
	FCS_CKM.2 Cryptographic Key Distribution
	FCS_COP.1 Cryptographic operation
	FCS_RBG_EXT.1 Random Bit Generation
	FCS_TLSC_EXT.1 TLS Client Protocol without mutual authentication
	FIA_X509_EXT.1 X.509 Certificate Validation
	FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_TLSC_EXT.2.1 The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

5.2.2. TLS Server Cryptographic Protocol (FCS_TLSS_EXT)

Family Behaviour

92 The component in this family addresses the ability for a server to use TLS to protect data between a client and the server using the TLS protocol.

Rationale

93 This family is introduced because no similar family is available in [CCPART2].

Component levelling

94 FCS_TLSS_EXT.1 TLS Server requires that the server side of TLS be implemented as specified.

95 FCS_TLSS_EXT.2: TLS Server requires the mutual authentication be included in the TLS implementation.

Management: FCS_TLSS_EXT.1, FCS_TLSS_EXT.2

96 The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FCS_TLSS_EXT.1, FCS_TLSS_EXT.2

97 The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a. Failure of TLS session establishment

b. TLS session establishment

c. TLS session termination

5.2.2.1. FCS_TLSS_EXT.1 TLS Server Protocol without Mutual Authentication

Hierarchical to:	No other components
Dependencies:	FCS_CKM. 1 Cryptographic Key Generation
	FCS_CKM.2 Cryptographic Key Distribution
	FCS_COP.1 Cryptographic operation
	FCS_RBG_EXT.1 Random Bit Generation
	FIA_X509_EXT.1 X.509 Certificate Validation
	FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_TLSS_EXT.1.1 The TSF shall implement [selection: TLS 1.2 [RFC5246], TLS 1.1 [RFC4346], TLS 1.3 [RFC8446]] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [assignment: list of optional ciphersuites and reference to RFC in which each is defined] and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [selection: TLS 1.1, TLS 1.2, TLS 1.3, none].

FCS_TLSS_EXT.1.3 The TSF shall perform key establishment for TLS using [selection: RSA with key size [selection: 2048 bits, 3072 bits, 4096 bits], Diffie-Hellman parameters with size [selection: 2048 bits, 3072 bits, 4096 bits, 6144 bits, 8192 bits], Diffie-Hellman groups [selection: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, no other groups], ECDHE curves [selection: secp224r1, secp256r1, secp384r1, secp521r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1] and no other curves]].

FCS_TLSS_EXT.1.4 The TSF shall support [selection: no session resumption or session tickets, session resumption based on session IDs according to RFC 4346 (TLS1.1) or RFC 5246 (TLS1.2) or RFC 8446) (TLS1.3), session resumption based on session tickets according to RFC 5077].

5.2.2.2. FCS_TLSS_EXT.2 TLS Server support for Mutual Authentication

Hierarchical to:	No other components
Dependencies:	FCS_CKM. 1 Cryptographic Key Generation
	FCS_CKM.2 Cryptographic Key Distribution
	FCS_COP.1 Cryptographic operation
	FCS_RBG_EXT.1 Random Bit Generation
	FCS_TLSS_EXT.1 TLS Client Protocol without mutual authentication
	FIA_X509_EXT.1 X.509 Certificate Validation
	FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_TLSS_EXT.2.1 The TSF shall support TLS communication with mutual authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.2.2 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the client certificate is invalid. The TSF shall also [selection:

- Not implement any administrator override mechanism
- require administrator authorisation to establish the connection if the TSF fails to [selection: match the reference identifier, validate certificate path, validate expiration date, determine the

revocation status] of the presented client certificate
].

FCS_TLSS_EXT.2.3 The TSF shall not establish a trusted channel if the identifier contained in a certificate does not match an expected identifier for the client. The TSF shall parse the identifier from the certificate and match the identifier against the expected identifier of the client as described in the TSS.

5.2.3. Random Bit Generation (FCS_RBG_EXT)

Family Behaviour

98 Components in this family address the requirements for random bit/number generation. This is a new family defined for the FCS class.

Rationale

99 This family is introduced because no similar family is available in [CCPART2].

Component levelling

100 FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

Management: FCS_RBG_EXT.1

101 The following actions could be considered for the management functions in FMT:

a. The TSF shall have the ability to configure the cryptographic functionality.

Audit: FCS_RBG_EXT.1

102 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Minimal: failure of the randomisation process.

5.2.3.1. FCS_RBG_EXT.1 Random Bit Generation

Hierarchical to:	No other components
Dependencies:	No other components

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [selection: Hash_DRBG (any),

HMAC_DRBG (any), CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment: number of software-based sources] software-based noise source, [assignment: number of platform-based sources] platform-based noise source] with a minimum of [selection: 128 bits, 192 bits, 256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

5.3. Identification and Authentication (FIA)

5.3.1. Password Management (FIA_PMG_EXT)

Family Behaviour

103 The TOE defines the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained.

Rationale

104 This family is introduced because no similar family is available in [CCPART2].

Component levelling

FIA_PMG_EXT Password Management	1

105 FIA_PMG_EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

Management: FIA_PMG_EXT.1

106 No management functions

Audit: FIA_PMG_EXT.1

107 No specific audit requirements.

5.3.1.1. FIA_PMG_EXT.1 Password Management

Hierarchical to:	No other components
Dependencies:	No other components

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of [assignment: allowed character classes]
b) Minimum password length shall be configurable to between [assignment: minimum number of characters supported by the TOE] and [assignment: number of characters greater than or equal to 15] characters.

5.3.2. User Authentication (FIA_UAU)

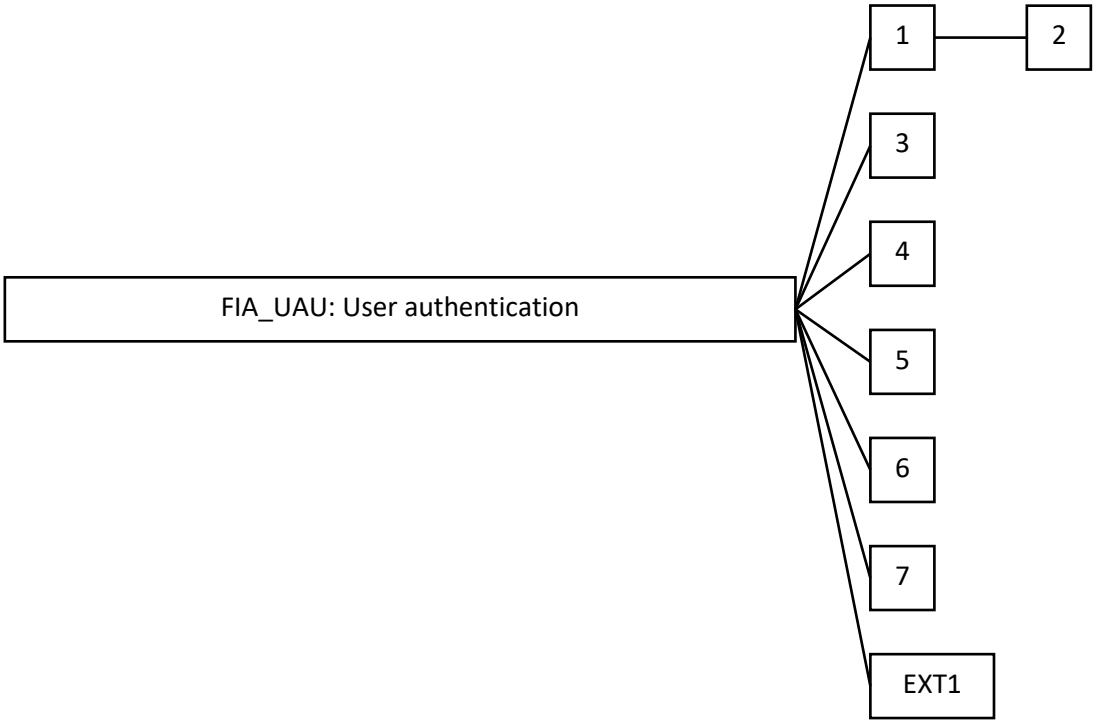
Family Behaviour

108 This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based.

Rationale

109 This family is extended with component EXT1 to provide requirements for a locally based administrative user authentication mechanism.

Component levelling



110 FIA_UAU.EXT1 A password-based authentication mechanism provides administrative users a locally based authentication mechanism.

Management: FIA_UAU.EXT1

111 The following actions could be considered for the management functions in FMT:

a. None

Audit: FIA_UAU.EXT1

112 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Minimal: All use of the authentication mechanism

5.3.2.1. FIA_UAU.EXT1 Password-based Authentication Mechanism

Hierarchical to:	No other components
Dependencies:	No other components

FIA_UAU.EXT1.1 The TSF shall provide a local [selection: password-based, SSH public key-based, certificate-based, [assignment: other authentication mechanism(s)]] authentication mechanism to perform local administrative user authentication.

5.3.3. User Identification and Authentication (FIA_UIA_EXT)

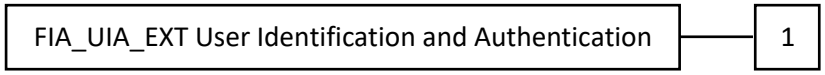
Family Behaviour

113 The TSF allows certain specified actions before the non-TOE entity goes through the identification and authentication process.

Rationale

114 This family is introduced because no similar family is available in [CCPART2].

Component levelling



115 FIA_UIA_EXT.1 User Identification and Authentication requires Administrators (including remote Administrators) to be identified and authenticated by the TOE, providing assurance for that end of the communication path. It also ensures that every user is identified and authenticated before the TOE performs any mediated functions

Management: FIA_UIA_EXT.1

116 The following actions could be considered for the management functions in FMT:

a. Ability to configure the list of TOE services available before an entity is identified and authenticated

Audit: FIA_UIA_EXT.1

117 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. All use of the identification and authentication mechanism

b. Provided user identity, origin of the attempt (e.g. IP address)

5.3.3.1. FIA_UIA_EXT.1 User Identification and Authentication

Hierarchical to: No other components

Dependencies: FTA_TAB.1 Default TOE Access Banners

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the user to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [selection: no other actions, automated generation of cryptographic keys, [assignment: list of services, actions performed by the TSF in response to non-TOE requests]].

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

5.3.4. Authentication using X.509 certificates (FIA_X509_EXT)

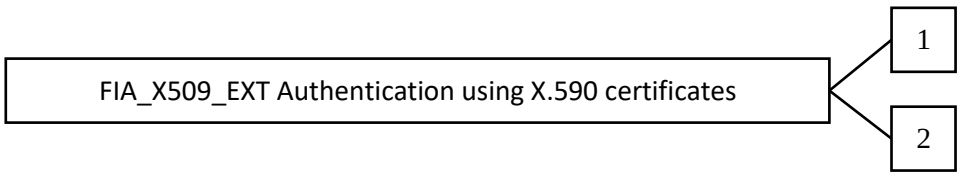
Family Behaviour

118 This family defines the behaviour, management, and use of X.509 certificates for functions to be performed by the TSF. Components in this family require validation of certificates according to a specified set of rules and use of certificates for authentication for protocols and integrity verification.

Rationale

119 This family is introduced because no similar family is available in [CCPART2].

Component levelling



120 FIA_X509_EXT.1 X509 Certificate Validation, requires the TSF to check and validate certificates in accordance with the RFCs and rules specified in the component.

121 FIA_X509_EXT.2 X509 Certificate Authentication, requires the TSF to use certificates to authenticate peers in protocols that support certificates, as well as for integrity verification and potentially other functions that require certificates.

Management: FIA_X509_EXT.1, FIA_X509_EXT.2

122 The following actions could be considered for the management functions in FMT:

a. Remove imported X.509v3 certificates

b. Approve import and removal of X.509v3 certificates

Audit: FIA_X509_EXT.1, FIA_X509_EXT.2

123 The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a. Minimal: No specific audit requirements are specified

5.3.4.1. FIA_X509_EXT.1 X.509 Certificate Validation

Hierarchical to: No other components

Dependencies: FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5, no revocation method]
- The TSF shall validate the certificate according to the following additional rules: [assignment: rules that govern contents of the fields that need to be verified].

FIA_X509_EXT.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.3.4.2. FIA_X509_EXT.2 X509 Certificate Authentication

Hierarchical to: No other components

Dependencies: FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [selection: DTLS, HTTPS, IPsec, TLS, SSH, [assignment:

other protocols], no protocols], and [selection: code signing verification for system software updates, [assignment: other uses], no additional uses].

FIA_X509_EXT.2.2 When the TSF cannot determine the validity of a certificate, the TSF shall [selection: allow the Administrator to choose whether to accept the certificate in these cases, accept the certificate, not accept the certificate].

5.4. Protection of the TSF (FPT)

5.4.1. Protection of Administrator Passwords (FPT_APW_EXT)

Family Behaviour

124 Components in this family ensure that the TSF will protect plaintext credential data such as passwords from unauthorised disclosure.

Rationale

125 This family is introduced because no similar family is available in [CCPART2].

Component levelling

126 FPT_APW_EXT.1 Protection of Administrator passwords requires that the TSF prevent plaintext credential data from being read by any user or subject.

Management: FPT_APW_EXT.1

127 The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FPT_APW_EXT.1

128 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. No audit necessary.

5.4.1.1. FPT_APW_EXT.1 Protection of Administrator Passwords

Hierarchical to:	No other components
Dependencies:	No other components

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

5.4.2. Protection of TSF Data (FPT_SKP_EXT)

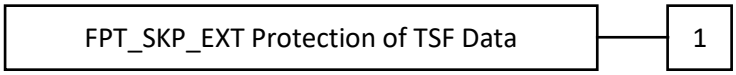
Family Behaviour

129 Components in this family address the requirements for managing and protecting TSF data, such as cryptographic keys.

Rationale

130 This family is introduced because no similar family is available in [CCPART2].

Component levelling



131 FPT_SKP_EXT.1 Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject. It is the only component of this family.

Management: FPT_SKP_EXT.1

132 The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FPT_SKP_EXT.1

133 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

5.4.2.1. FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

Hierarchical to:	No other components
Dependencies:	No other components

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.4.3. Time stamps (FPT_STM)

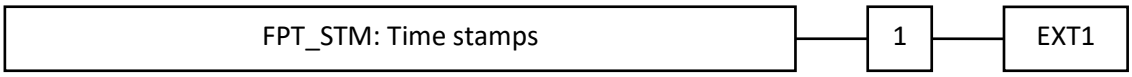
Family Behaviour

134 This family addresses requirements for a reliable time stamp function within a TOE.

Rationale

135 This family is extended with component EXT1 to introduce requirements describing the source of time used in timestamps.

Component levelling



136 FPT_STM.EXT1 Reliable Time Stamps is hierarchical to FPT_STM.1: it requires that the TSF provide reliable time stamps for TSF and identifies the source of the time used in those timestamps.

Management: FPT_STM.EXT1

137 The following actions could be considered for the management functions in FMT:

a. Management of the time

b. Administrator setting of the time.

Audit: FPT_STM.EXT1

138 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Discontinuous changes to the time.

5.4.3.1. FPT_STM.EXT1 Reliable Time Stamps For Its Own Use

Hierarchical to:	FPT_STM.1
Dependencies:	No other components

FPT_STM.EXT1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM.EXT1.2 The TSF shall [selection: allow the Security Administrator to set the time, synchronise time with an NTP server].

5.4.4. TSF Self-Test (FPT_TST)

Family Behaviour

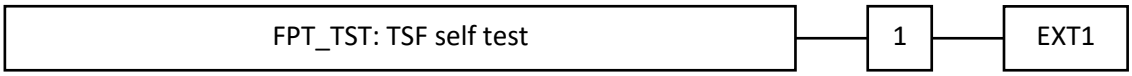
139 The family defines the requirements for the self-testing of the TSF with respect to some expected correct operation. Examples are interfaces to enforcement functions, and sample arithmetical operations on critical parts of the TOE. These tests can be carried out at start-up, periodically, at the request of the authorised user, or when other conditions are met. The actions to be taken by the TOE as the result of self testing are defined in other families.

140 The requirements of this family are also needed to detect the corruption of TSF data and TSF itself (i.e. TSF executable code or TSF hardware component) by various failures that do not necessarily stop the TOE's operation (which would be handled by other families). These checks must be performed because these failures may not necessarily be prevented. Such failures can occur either because of unforeseen failure modes or associated oversights in the design of hardware, firmware, or software, or because of malicious corruption of the TSF due to inadequate logical and/or physical protection.

Rationale

141 This family is extended with component EXT1 to address the requirements for self-testing the TSF for selected correct operation.

Component levelling



142 FPT_TST.EXT1 TSF Self-Test requires a suite of self-tests to be run during initial start-up in order to demonstrate correct operation of the TSF.

Management: FPT_TST.EXT1

143 The following actions could be considered for the management functions in FMT:

a. No management functions.

Audit: FPT_TST.EXT1

144 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Minimal: no action.

b. Basic:

i. Failure of self-test.

c. Detailed:

i. Indication that TSF self-test was completed.

ii. Failure of self-test.

5.4.4.1. FPT_TST.EXT1 TSF Testing

Hierarchical to: FPT_TST.1

Dependencies: No other components

FPT_TST.EXT1.1 The TSF shall run a suite of the following self-tests [selection: during initial start-up (on power on), periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self-tests should occur]] to demonstrate the correct operation of the TSF: [assignment: list of self-tests run by the

TSF].

5.4.5. Trusted Update (FPT_TUD_EXT)

Family Behaviour

145 Components in this family address the requirements for updating the TOE firmware and/or software.

Rationale

146 This family is introduced because no similar family is available in [CCPART2].

Component levelling

147 FPT_TUD_EXT.1 Trusted Update requires management tools be provided to update the TOE firmware and software, including the ability to verify the updates prior to installation.

Management: FPT_TUD_EXT.1

148 The following actions could be considered for the management functions in FMT:

a. Ability to update the TOE and to verify the updates

b. Ability to update the TOE and to verify the updates using the digital signature capability (FCS_COP.1) and [selection: no other functions, [assignment: other cryptographic functions (or other functions) used to support the update capability]]

c. Ability to update the TOE, and to verify the updates using [selection: digital signature, published hash, no other mechanism] capability prior to installing those updates

Audit: FPT_TUD_EXT.1

149 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Minimal: no action.

b. Basic:
   i. Any failure to verify the integrity of the update.

c. Detailed:
   i. Initiation of the update process.
   ii. Any failure to verify the integrity of the update

5.4.5.1. FPT_TUD_EXT.1 TSF Trusted Update

Hierarchical to: No other components

Dependencies: FCS_COP.1

FPT_TUD_EXT.1.1 The TSF shall provide [assignment: Administrators] the ability to query the currently executing version of the [assignment: TOE parts] and [selection: the most recently installed version of the TOE firmware/software; no other TOE firmware/software version].

FPT_TUD_EXT.1.2 The TSF shall provide [assignment: Administrators] the ability to manually initiate updates to [assignment: TOE parts] and [selection: support automatic checking for updates, support automatic updates, no other update mechanism].

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the [assignment: TOE parts] using a [selection: X.509 certificate, digital signature, published hash] prior to installing those updates.

5.5. TOE Access (FTA)

5.5.1. Limitation of concurrent administrator sessions (FTA_MCS_EXT)

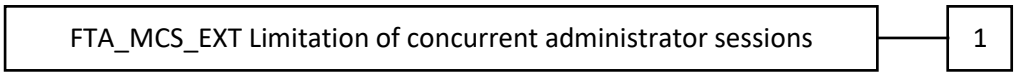
Family Behaviour

150 This family defines requirements to place limits on the number of concurrent administrative sessions established with the TOE.

Rationale

151 The extended FTA_MCS_EXT family is based on the FTA_MCS family, but it places limits on the number of concurrent administrative sessions instead of on the number of concurrent sessions that belong to the same user.

Component levelling



152 FTA_MCS_EXT.1 Basic limitation of concurrent administrative sessions, provides limitations that apply globally to administrative sessions established by administrative users of the TSF.

Management: FTA_MCS_EXT.1

153 The following actions could be considered for the management functions in FMT:

a. None.

Audit: FTA_MCS_EXT.1

154 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. None.

5.5.1.1. FTA_MCS_EXT.1 Basic limitation of concurrent administrative sessions

Hierarchical to:	No other components
Dependencies:	FIA_UID.1 Timing of identification

FTA_MCS_EXT.1.1 The TSF shall restrict the maximum number of concurrent administrative sessions.

5.5.2. TSF-initiated Session Locking (FTA_SSL)

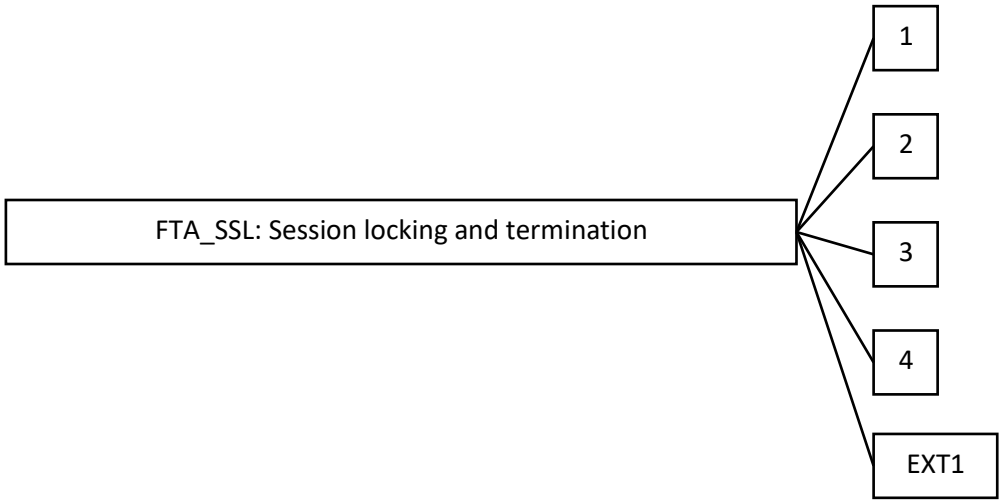
Family Behaviour

155 This family defines requirements for the TSF to provide the capability for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

Rationale

156 This family is extended with component EXT1 to address the requirements for TSF-initiated locking for local interactive sessions.

Component levelling



157 FTA_SSL.EXT1 TSF-initiated session locking, requires system initiated locking of an interactive session after a specified period of inactivity.

Management: FTA_SSL.EXT1

158 The following actions could be considered for the management functions in FMT:

a. Specification of the time of user inactivity after which lock-out occurs for an individual user.

Audit: FTA_SSL.EXT1

159 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Any attempts at unlocking an interactive session.

5.5.2.1. FTA_SSL.EXT1 TSF-initiated Session Locking

Hierarchical to:	No other components
Dependencies:	FIA_UAU.1 Timing of authentication

FTA_SSL.EXT1.1 The TSF shall, for local interactive sessions, [selection:

- lock the session - disable any activity of the Administrator's data access/display devices other than unlocking the session, and requiring that the Administrator re-authenticate to the TSF prior to unlocking the session;
- terminate the session]

after an Administrator-specified time period of inactivity.

6. Security Requirements

6.1. Security functional requirements

160 The following conventions have been followed for the instantiation of the security functional requirements:

a. Assignments: **bold font**

b. Selections: underlined font

c. Iterations: addition of a "/" and a short iteration description in capital letters to the SFR component identifiers (in the form "SFR_ID/IT_DESC").

d. Refinements:

i. Refinements indicating additions: *[+ italic font enclosed by '[+ ' and ']']*

ii. Refinements indicating removals: ~~crossed out~~.

161 The representation of two combined operations is observed whenever possible: for example, a selection inside an assignment can be represented as **underlined bold font**.

162 Only bibliographic references are exempted from these conventions. They are easily identified because they are always represented as alphanumeric short references embedded in square brackets (e.g: [REF1]) without bold, underlined or other markings.

163 When operation requires a list, either bullets or a comma-separated enumeration is used.

6.1.1. FAU: Security Audit

6.1.1.1. FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 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 not specified level of audit; and
- **All the Operation System Events, described in Table 16**
- **All the Security System Events, described in Table 17**
- **All Data Transfer Logging Events**

Application Note: The two events that indicate the starting and ending of audit functions are GlobalSystemStartUp and GlobalSystemShutdown.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST:

- **For Operation System Events and Security System Events: specific additional information associated to the event**
- **For Data Transfer Logging Events: information related to the particular transfer that depends on the associated service.**

Application Note:
For System Events:
- The type of event indicates whether it is a 'Security' or 'Operation' Event. The type of event is encoded in the SYSLOG facility field [RFC3164].
- Subject identity contains the internal appliance identity (IP and CN of its certificate) and, for the events generated by and administrator, the Administrator CN
- The outcome is not a field in in this type of events because it is implicitly defined by the event type
- The severity of the event can take the following values: Debug (7), Informational (6), Notice (5), Warning (4), Error (3) and Critical (2).

For Data Transfer Logging Events:
- Subject identity contains the internal appliance identity (CN of its certificate)
- The outcome is not a field in in this type of events because it is implicitly defined by the event type

Operation System Event	Severity	Description
AuditLocalStorageFailure	Failure	A serious failure occurred in audit local storage.
AuditLocalStorageNotice	Notice	Issue in audit local storage.
AuditLocalStorageWarning	Warning	Audit local storage is in 'Warning' state.
AuditServerCommandFailed	Warning	PSTaud issued an error response.
AuditServerConnect	Informational	Connection to PSTaud established.
AuditServerConnectFail	Notice	Connection to PSTaud failed.
AuditServerDiagOk	Notice	Connection to PSTaud established and checked availability.
AuditServerDisconnect	Informational	Connection to PSTaud interrupted.
AuditServerNotConfigured	Warning	Audit not configured.
AuditServerUnavailable	Warning	Failed to send data to PSTaud for longer than configured. Can be due to connection failure or database inserting error.
GlobalConfigUpdate	Informational	Configuration update received.
GlobalLinkDown	Informational	External appliance link lost.
GlobalEventLocalStorageIssue	Notice	Issue in events local storage.
GlobalEventServerUnavailable	Warning	Unable to send events to a server.
GlobalEventServerConnect	Informational	Connected to an events server.
GlobalEventServerDisconnect	Informational	Disconnection from events server.
GlobalEventServerConnectFail	Notice	Failed to connect to an events server.
GlobalLinkFailure	Error	Unexpected link failure with external appliance.
GlobalLinkUp	Informational	External unit link established.
GlobalPrimaryClusterFailed	Warning	Primary element has found an error that prevents synchronisation in cluster mode.
GlobalPrimaryClusterOk	Informational	Cluster works correctly.

GlobalPrimaryConnectFail	Notice	Connection to secondary cluster element failed.
GlobalPrimaryConnected	Informational	Secondary cluster element connection established.
GlobalPrimaryDisconnected	Informational	Secondary cluster element disconnected.
GlobalPrimaryFullMode	Informational	Primary cluster element assumes the entire cluster load.
GlobalPrimaryNormalMode	Informational	Primary cluster element assumes the configured cluster load..
GlobalSecondaryClusterFailed	Warning	Secondary element has found an error that avoids synchronisation in cluster mode.
GlobalSecondaryClusterOk	Informational	Cluster works correctly.
GlobalSecondaryConnectFail	Notice	Connection to primary cluster element failed.
GlobalSecondaryConnected	Informational	Primary cluster element connection established.
GlobalSecondaryDisconnected	Informational	Primary cluster element disconnected.
GlobalSecondaryFullMode	Informational	Secondary cluster element assumes the entire cluster load.
GlobalSecondaryNormalMode	Informational	Secondary cluster element assumes the configured cluster load.
GlobalSecondarySync	Informational	Secondary element has updated the configuration given by the primary element.
GlobalSystemShutdown	Informational	System has been shut down.
GlobalSystemStartup	Informational	System started normally.
GlobalVersionFailure	Error	Software versions mismatch.
ServiceStart	Informational	Service has started.
ServiceStop	Informational	Service was stopped.

Table 16: List of Operation System Events

Security System Event	Severity	Description
AdminConnect	Informational	Administration connection established.
AdminCommandRejection	Informational	Persistent action command was rejected.
AdminConnectRejection	Informational	A connection attempt was rejected.
AdminDisconnect	Informational	Administration connection interrupted.
AdminLocalCommand	Informational	Local action command issued.
AdminLocalCommandRejection	Informational	Local action command was rejected.
AdminWriteCommand	Informational	Persistent action command issued.
AuditServerConnectionSecFail	Warning	Connection to PSTaud failed for security reasons.
GlobalEventServerConnectSecFail	Warning	Connection to event server failed for security reasons.
GlobalPrimaryConnectionSecFail	Error	Connection to secondary cluster element failed for security reasons.
GlobalSecondaryConnectionSecFail	Error	Connection to primary cluster element failed for security reasons.

Table 17: List of Security System Events

6.1.1.2. FAU_GEN.2 User identity association

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

6.1.1.3. FAU_SAR.1/Sec Audit review

FAU_SAR.1.1/Sec The TSF shall provide **Security Administrators** with the capability to read **Security System Events** from the audit records.

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

6.1.1.4. FAU_SAR.1/Op Audit review

FAU_SAR.1.1/Op The TSF shall provide **Service Administrators** with the capability to read **Operation System Events** from the audit records.

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

6.1.1.5. FAU_SAR.1/TD Audit review

FAU_SAR.1.1/TD The TSF shall provide **PSTAud users** with the capability to read **Data Transfer Logging Events** from the audit records.

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

Application Note: The TSF sends the Data Transfer Logging Events to the configured PSTAud server, where they will be made available to the appropriate users by the PSTAud software (non TOE). The TSF does not provide other means for users to access the transfer data events.

6.1.1.6. FAU_SAR.2 Restricted audit review

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

6.1.1.7. FAU_STG.EXT1 Security Audit Event Storage

FAU_STG.EXT1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG.EXT1.2 The TSF shall be able to store generated audit data on the TOE itself. In addition:

- The TOE shall be a distributed TOE that stores *[+ system security and operation]* audit data on the following TOE components: **PSTi part of the 'Core' component**.
- The TOE shall be a distributed TOE with storage of audit data provided externally for the following types of audit events:
  - **Operation System Events and Security System Events: transmitted by the TOE to the configured syslog server(s)**

- **Data Transfer Logging Events: transmitted by the TOE to the configured and authenticated PSTaud server.**

FAU_STG.EXT1.3 The TSF shall overwrite previous *[+ system security and operation]* audit records according to the following rule: **an administrator-defined log file size and number of log files** when the local storage space for audit data is full.

6.1.1.8. FAU_STG.1 Protected audit trail storage

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

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

6.1.2. FCS: Cryptographic support

6.1.2.1. FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Password-Based Key Derivation Function 2 (PBKDF2) with HMAC-SHA256 and 2048 iteration value** and specified cryptographic key sizes **256 bits** that meet the following: [RFC8018].

6.1.2.2. FCS_CKM.2 Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall ~~distribute cryptographic keys in accordance with a specified cryptographic key distribution method~~ *[+ perform cryptographic key establishment in accordance with a specified cryptographic key establishment method:]*

- ***Elliptic curve-based key establishment schemes, supporting the curves* secp384r1, secp521r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1**

that meets the following:

- ***Elliptic curve-based key establishment schemes: the specification in*** [RFC5246] **/** [RFC8446] **and** [SP80056A]**.**

Application Note: Key distribution in the context of the TOE refers to key establishment in TLS protocols.

6.1.2.3. FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **single overwrite consisting of zeroes** that meets the following: **No Standard**.

6.1.2.4. FCS_COP.1 Cryptographic Operation

6.1.2.4.1. FCS_COP.1/Cipher-AES Cryptographic Operation

FCS_COP.1.1/Cipher-AES The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm **AES in CBC, GCM and CCM modes** and cryptographic key sizes **256 bits** that meet the following: **AES as specified in** [FIPS197]**, CBC mode as specified in** [SP80038A]**, GCM mode as specified in** [SP80038D]**, CCM mode as specified in** [SP80038C]**.**

6.1.2.4.2. FCS_COP.1/Cipher-CHACHA20 Cryptographic Operation

FCS_COP.1.1/Cipher-CHACHA20 The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm **CHACHA20-POLY1305** and cryptographic key sizes **256 bits** that meet the following: [RFC7905].

6.1.2.4.3. FCS_COP.1/Cipher-RSA Cryptographic Operation

FCS_COP.1.1/Cipher-RSA The TSF shall perform **decryption** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **4096 bits** that meet the following: [RFC8017].

6.1.2.4.4. FCS_COP.1/Hash-SHA Cryptographic Operation

FCS_COP.1.1/Hash-SHA The TSF shall perform **hashing calculation** in accordance with a specified cryptographic algorithm **SHA2** and cryptographic key sizes **256 and 384 bits** that meet the following: [FIPS180_4].

Application Note: 'key size' must be understood as 'hash size'.

6.1.2.4.5. FCS_COP.1/KeyedHash Cryptographic Operation

FCS_COP.1.1/KeyedHash The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC** and cryptographic key sizes **256 and 384 bits** *[+ and message digest sizes 256 and 384 bits]* that meet the following: [FIPS198_1].

6.1.2.4.6. FCS_COP.1/Signature-ECDSA Cryptographic Operation

FCS_COP.1.1/Signature-ECDSA The TSF shall perform **cryptographic signature services (generation and verification)** in accordance with a specified cryptographic algorithm **ECDSA** and

cryptographic key sizes **between 256 and 521 bits** that meet the following: **none.**

6.1.2.4.7. FCS_COP.1/Signature-RSA Cryptographic Operation

FCS_COP.1.1/Signature-RSA The TSF shall perform **cryptographic signature generation and verification** in accordance with a specified cryptographic algorithm **RSA Digital Signature Algorithm** and cryptographic key sizes **between 3072 and 15360 bits** that meet the following: **none.**

6.1.2.5. FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

FCS_TLSC_EXT.1.1 The TSF shall implement TLS 1.2 [RFC5246], TLS 1.3 [RFC8446] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

- **TLS 1.2:**
  - **TLS_ECDHE_ECDSA_WITH_AES_256_CCM (as specified in** [RFC7251]**)**
  - **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (as specified in** [RFC5289]**)**
  - **TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (as specified in** [RFC7905]**)**
  - **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (as specified in** [RFC5289]**)**
  - **TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (as specified in** [RFC7905]**)**
- **TLS 1.3 (ECDH):**
  - **TLS_AES_256_GCM_SHA384 (as specified in** [RFC8446]**)**
  - **TLS_CHACHA20_POLY1305_SHA256 (as specified in** [RFC8446]**)**

and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches the identifier per RFC 5280 Appendix A using id-at-commonName and no other attribute types.

Application Note: The TOE will check the Common Name of the certificate:

- In connections to PSTaud server.
- In connections to a syslog server only if the Security Administrator has provisioned the CN of the syslog server certificate.

FCS_TLSC_EXT.1.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also Not implement any administrator override mechanism.

Application Note: The validity verification performed by the TOE is explained in the TSS section

FCS_TLSC_EXT.1.4 The TSF shall offer RSA with key size 3072, 4096, 7680 and 15360 bits, ECDHE curves secp384r1, secp521r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 and no other curves in the Client Hello.

6.1.2.6. FCS_TLSC_EXT.2 TLS Client support for Mutual Authentication

FCS_TLSC_EXT.2.1 The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

6.1.2.7. FCS_TLSS_EXT.1 TLS Server Protocol without Mutual Authentication

FCS_TLSS_EXT.1.1 The TSF shall implement TLS 1.2 [RFC5246], TLS 1.3 [RFC8446] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

- **TLS 1.2:**
  - **TLS_ECDHE_ECDSA_WITH_AES_256_CCM (as specified in** [RFC7251]**)**
  - **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (as specified in** [RFC5289]**)**
  - **TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (as specified in** [RFC7905]**)**
  - **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (as specified in** [RFC5289]**)**
  - **TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (as specified in** [RFC7905]**)**
- **TLS 1.3 (ECDH):**
  - **TLS_AES_256_GCM_SHA384 (as specified in** [RFC8446]**)**
  - **TLS_CHACHA20_POLY1305_SHA256 (as specified in** [RFC8446]**)**

and no other ciphersuites.

Application Note: The TOE only supports mutually authenticated TLS connections. Nevertheless, FCS_TLSS_EXT.1 SFRs are included because they describe the authentication of the server to the client that also happens when mutual authentication is being enforced. A separate set of SFRs (FCS_TLSS_EXT.2) will describe the authentication of the client to the server.

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1.

FCS_TLSS_EXT.1.3 The TSF shall perform key establishment for TLS using RSA with key sizes 3072, 4096, 7680 and 15360 bits and ECDHE curves secp384r1, secp521r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 and no other curves.

FCS_TLSS_EXT.1.4 The TSF shall support no session resumption or session tickets.

6.1.2.8. FCS_TLSS_EXT.2 TLS Server support for Mutual Authentication

FCS_TLSS_EXT.2.1 The TSF shall support TLS communication with mutual authentication of TLS clients using X.509v3 certificates.

Application Note: The TOE only supports mutually authenticated TLS connections. FCS_TLSS_EXT.1 SFRs are included because they describe the authentication of the server to the client that also happens when mutual authentication is being enforced, while FCS_TLSS_EXT.2 SFRs describe the authentication of the client to the server, required in mutual authentication.

FCS_TLSS_EXT.2.2 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the client certificate is invalid. The TSF shall also not implement any administrator override mechanism.

FCS_TLSS_EXT.2.3 The TSF shall not establish a trusted channel if the identifier contained in a certificate does not match an expected identifier for the client. The TSF shall parse the identifier from the certificate and match the identifier against the expected identifier of the client as described in the TSS.

6.1.2.9. FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using CTR_DRBG (AES).

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from **1** software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

6.1.3. FDP: User Data Protection

6.1.3.1. FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the **User Access Control Policy** on

- **Subjects: the TSFs that handle authorised user access to TSF Data and functions on behalf of that users.**
- **Objects: The TSF functions specified in Table 18**

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 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.

6.1.3.2. FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **User Access Control Policy** to objects based on the following:

- **Subjects: The TSFs that handle the operations requested by authorised users through the admAPI, exposed on the High Security Domain network, on behalf of those users, and the local admin through the local admin console ("SHELL")**
- **Objects: TSF functionality specified in Table 18**
- **Security Attributes:**
  - **User identity, which can be verified using the following security attributes:**
    - **CN of the certificate assigned to the user**
    - **authorised CA(s)**
    - **CA revocation method**
  - **user role**
  - **functionality use case identifier**
  - **IP address of the IP of the PSTadm workstation accessing the TSF (only if the administrative IP restriction is activated)**
  - **MAC address of a PSTadm workstation accessing an internal network interface for remote administrators (only if the MAC filtering feature is activated)**

Application Note: Use case identifiers have the form 'COMPONENT-UC##' in Table 18, where COMPONENT is a TOE component: SHELL, RESTORE or CORE.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **The TSF shall verify for each operation requested by the user that his role is allowed the requested operation, following the association depicted in Table 18**.
- **If the administrative IP restriction is activated, the TSF will verify that the IP address of the IP of the PSTadm workstation accessing the TSF must match one of the allowed administrative IP address.**
- **If the MAC filtering feature is enabled, the MAC address of a PSTadm workstation accessing an administrative/internal network interface for**

remote administrators access must match one of the MACs in the administrative/internal interface allowed MAC addresses list.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

Subjects	The TSFs that handle the operations requested by authorised users through the admAPI, on behalf of that users.
Rules	The TSF will restrict access to the TSF functions based on the user administrator role, matching the assignments of this table

	User				
Objects (TSF Functions)	**Local Admin.**	**Root Admin.**	**Security Admin.**	**Service Admin.**	**Monitoring Admin.**
SHELL-UC01: Local configuration[6]	X				
SHELL-UC02: Access to global system status	X				
RESTORE-UC01: Firmware installation/updates/verification[7]	X				
CORE-UC01: View values of local configuration data			X		
CORE-UC02: System monitoring (Access to global system status, services status, channels status and monitoring data)				X	X
CORE-UC03: Start, Stop and Forced Stop of a service				X	
CORE-UC04: Configuration of data flow services (and channels) and backup				X	
CORE-UC05: Monitoring Configuration (System Events Management and Configuration of the server connection and security data for the Data Transfer Logging service and syslog server(s))			X		
CORE-UC06: Remote administration configuration and backup (non-root administrator role configuration,		X			

[6] Application Note: Includes the modification or visualisation of local configuration data, like High Security Domain MAC address filtering configuration or remote Root Administrator's CN configuration, as specified in subsection 1.4.2.1, using the SHELL component.

[7] Application Note: Firmware installation/updates/verification is available only to the Local Admin role using the RESTORE component. This component does not provide user access control itself . Instead, it relies on the security objective for the operational environment OE.PHYSEC to guarantee that only authorised local administrators will have access to it.

maximum inactivity time between remote modification commands configuration and Modification of IP access restriction configuration data)					
CORE-UC07: Access to (and backup of) Operation System Event data				X	
CORE-UC08: Access to (and backup of) Security System Event data			X		
CORE-UC09: Reset of Service data flow statistics				X	X
CORE-UC10: Remote system commands (Date/time configuration and Remote reboot of the appliances)			X		

Table 18: Access to TSF functionality by user role

Application Note: Each configuration use case includes the functionality of importing and exporting configuration data, which is accessible by the role.

6.1.3.3. FDP_IFC.2/IN Complete information flow control

FDP_IFC.2.1/IN The TSF shall enforce the **Input Data Flow Policy** on

- **Subjects: The TSF functions that handle the service data flow that comes from the external network endpoints (through the service modules) and goes to the internal network endpoints (through the service modules).**
- **Information: The information managed by the service modules connected to the TOE**

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

FDP_IFC.2.2/IN 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.

6.1.3.4. FDP_IFC.2/OUT Complete information flow control

FDP_IFC.2.1/OUT The TSF shall enforce the **Output Data Flow Policy** on

- **Subjects: The TSF functions that handle the service data flow that comes from the internal network endpoints (through the service modules) and goes to the external network endpoints (through the service modules).**
- **Information: The information managed by the service modules connected to the TOE**

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

FDP_IFC.2.2/OUT 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.

6.1.3.5. FDP_IFF.1/IN Simple Security Attributes

FDP_IFF.1.1/IN The TSF shall enforce the **Input Data Flow Policy** based on the following types of subject and information security attributes:

- **Subjects: The TSF functions that handle the service data flow that comes from the external network endpoints (through the service modules) and goes to the internal network endpoints (through the service modules).**
- **Information: The information managed by the service modules connected to the TOE**
- **Security attributes: the associated service of the data flow.**

FDP_IFF.1.2/IN The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **The data flow belongs to a licensed inbound service.**
- **The associated service is in running state.**
- **If the MAC filtering feature is enabled, the MAC address of the network endpoints must match one of MACs in each interface allowed MAC addresses list.**

FDP_IFF.1.3/IN The TSF shall enforce the **None**.

FDP_IFF.1.4/IN The TSF shall explicitly authorise an information flow based on the following rules: **None**.

FDP_IFF.1.5/IN The TSF shall explicitly deny an information flow based on the following rules: **None**.

6.1.3.6. FDP_IFF.1/OUT Simple Security Attributes

FDP_IFF.1.1/OUT The TSF shall enforce the **Output Data Flow Policy** based on the following types of subject and information security attributes:

- **Subjects: The TSF functions that handle the service data flow that comes from the internal network endpoints (through the service modules) and goes to the external network endpoints (through the service modules).**
- **Information: The information managed by the service modules connected to the TOE**
- **Security attributes: the associated service of the data flow.**

FDP_IFF.1.2/OUT The TSF shall permit an information flow between a controlled subject

and controlled information via a controlled operation if the following rules hold:

- **The data flow belongs to a licensed outbound service.**
- **The associated service is in running state.**
- **If the MAC filtering feature is enabled, the MAC address of the network endpoints must match one of the MACs in each interface allowed MAC addresses list.**

FDP_IFF.1.3/OUT The TSF shall enforce the **None**.

FDP_IFF.1.4/OUT The TSF shall explicitly authorise an information flow based on the following rules: **None**.

FDP_IFF.1.5/OUT The TSF shall explicitly deny an information flow based on the following rules: **None**.

6.1.4. FIA: Identification and Authentication

6.1.4.1. FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when **1** unsuccessful authentication attempts occur related to **the Local Administrator login in the local console ('Shell')**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall:

- **Increase the login delay time by doubling the previous login delay time (starting by the 'minimum login delay time') unless the 'maximum login delay time' has already been reached.**
- **Prevent the offending Administrator from trying to login into the TOEs 'Shell' until the login delay time has elapsed**.

Application Note: The 'login delay time' is the time that has to be elapsed between unsuccessful login attempts for the local administration login to be available. As the SFR defines, this time is increasing until a successful login occurs, in which case it is reset to its initial value. Both 'minimum login delay time' and 'maximum login delay time' are configurable parameters.

6.1.4.2. FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for *[+local console ('Shell')]* administrative passwords:

a) Passwords shall be able to be composed of **two of the following categories:**

- **Letters, which must include uppercase and lowercase**
- **Letters and numbers, which must include letters (uppercase or lowercase) as well as numbers**
- **letters and symbols, which must include letters (uppercase or lowercase) as well as printable symbols**

b) Minimum password length shall be configurable to between **8** and **50** characters.

Application Notes:
- Which two categories must be met by the password and the minimum password length are configurable by the local administrator.
- The default minimum password length is 12.

6.1.4.3. FIA_UAU.EXT1 Password-based Authentication Mechanism

FIA_UAU.EXT1.1 The *TSF [+'Shell' component]* shall provide a local password-based authentication mechanism to perform local administrative user authentication.

6.1.4.4. FIA_UIA_EXT.1 User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall allow the following actions *[+only to the local administrator]* prior to requiring the user to initiate the identification and authentication process:
- Display the warning banner in accordance with FTA_TAB.1;
- **Show general status information and firmware version of the appliance**
- **Allow to run the 'Restore' component of the TOE**

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

Application Note: The defined actions only apply to local users, which map to the 'Shell' user and the human user operating the Firmware Management Utility ('Restore' component).

6.1.4.5. FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only **obscured feedback** to the administrative user while the authentication is in progress *[+ at the local administration console ('Shell')]*.

Application Note: 'Obscured feedback' implies the TSF does not produce a visible display of any authentication data entered by a user (such as the echoing of a password), although an obscured indication of progress may be provided (such as an asterisk for each character). It also implies that the TSF does not return any information during the authentication process to the user that may provide any indication of the authentication data.

6.1.4.6. FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation *[+ supporting a minimum path length of two certificates]*.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5, no revocation method
- The TSF shall validate the certificate according to the following additional rules:
  - **The certificate shall not be expired**
  - **The CN of the certificate shall be verified**
  - **The key associated with the remote peer's certificate must have a strength equal to or greater than that associated with the local certificate**
  - **CA certificates configured by the local administrator shall have the Certificate Signing purpose in the KeyUsage field.**
  - **Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.**
  - **Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.**
  - **OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.**
  - **CRL certificates configured by the local administrator or presented by CRL servers in HTTP responses shall have the CRL Signing purpose in the KeyUsage field.**

Application Note:

- The CN verification is optional in TLS connections where the TOE is acting as TLS client.
- The certificate's key strength verification is performed when the TOE is acting as TLS server.

FIA_X509_EXT.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

6.1.4.7. FIA_X509_EXT.2 X509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for TLS, code signature verification for system software updates, license verification and service parametrisations verification.

FIA_X509_EXT.2.2 When the TSF cannot determine the validity of a certificate, the TSF shall not accept the certificate.

6.1.5. FMT: Security Management

6.1.5.1. FMT_MOF.1/LocalConfFuncs Management of Security Functions Behaviour

FMT_MOF.1.1/LocalConfFuncs The TSF shall restrict the ability to enable, disable the functions

- **MAC filtering in the High Security Domain**
- **NTP time synchronisation**
- **High Availability mode**
- **Available Data Services**

to **the Local Administrator**.

6.1.5.2. FMT_MOF.1/RootConfFuncs Management of Security Functions Behaviour

FMT_MOF.1.1/RootConfFuncs The TSF shall restrict the ability to enable, disable the functions

- **IP of Administration users restrictions**

to **the Root Administrator**.

6.1.5.3. FMT_MSA.1/LocalConfAttr Management of security attributes

FMT_MSA.1.1/LocalConfAttr The TSF shall enforce the **User Access Control Policy** to restrict the ability to query, modify, delete the security attributes

- **Allowed MACs list**
- **CN of Root Administrators**
- **Authorised CA(s)**
- **CA revocation method**

to the **Local Administrator**

6.1.5.4. FMT_MSA.1/RootConfAttr Management of security attributes

FMT_MSA.1.1/RootConfAttr The TSF shall enforce the **User Access Control Policy** to restrict the ability to query, modify, delete the security attributes

- **Allowed administration IP list**
- **CN of remote non-root administrators**
- **Role(s) assigned to each remote non-root administrator**

to the **Root Administrator**.

6.1.5.5. FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **User Access Control Policy, Input Data Flow Policy, Output Data Flow Policy** to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow ~~the~~ **no role** to specify alternative initial values to override the default values when an object or information is created.

Application Note: The TSF does not allow any role (roles are defined in FMT_SMR.2.1) to override the default values. Thus, even though "no role" is not explicitly available in the FMT_MSA.3.2 definition nor in FMT_SMR.2.1, it is used here to appropriately describe the TSF behaviour regarding the override of its default values.

6.1.5.6. FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to **manage** the **TSF Data** to:

- **The Local Administrators**
- **The Root Administrator**
- **The Security Administrators**
- **The Service Administrators**
- **The Monitoring Administrators**

Application Note: The identifier 'TSF Data' must be interpreted as all configuration data accessible by the referred roles as described in Table 18. The word 'manage' must be interpreted as the operation described in Table 18 for the each particular 'TSF Data'.

6.1.5.7. FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- **Ability to enable/disable the following functions:**
  - **MAC filtering in the High Security Domain**
  - **NTP time synchronisation**
  - **High Availability mode**
  - **Available Data Services**
  - **IP of Administration users restrictions**
- **Ability to configure the following security attributes:**
  - **Allowed MACs list**
  - **CN of Root Administrators**
  - **Authorised CA(s)**
  - **CA revocation method (one method per CA)**
  - **Appliance certificate and associated private key**
  - **Allowed administration IP list**
  - **CN of remote non-root administrators**
  - **CN associated to the PSTaud server**
  - **CN associated to the syslog server(s)**
  - **Role(s) assigned to each remote non-root administrator**
  - **'Shell' 'Minimum login delay time' and 'Maximum login delay time' parameters (for FIA_AFL.1)**
  - **'Shell' inactivity timeout.**
  - **Timeout for remote administrators (other than monitoring**

administrator) session inactivity
- **'Shell' banner message**
- **Password policy values (the two required character groups and minimum number of characters)**

- **Ability to configure the following attributes:**
  - **System Events management behaviour including destination server, severity levels and log rotation parameters**
- **Ability to administer the TOE locally and remotely**
- **Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates (manual updates)**
- **Ability to verify license files using digital signatures capability prior to import them**
- **Ability to verify service parameterization files using digital signatures capability prior to import them**
- **Ability to start and stop licensed data flow services**
- **Ability to manage data flow channels (activation, deactivation and priority modification)**
- **Ability to manage the cryptographic keys**
- **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors (initial configuration setup)**
- **Ability to import X.509v3 certificates to the TOE's trust store (appliance and CA certificates)**

6.1.5.8. FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles:
- **Local administrator**
- **Root Administrator**
- **Security Administrator**
- **Service Administrator**
- **Monitoring Administrator**

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions:
- **The maximum number of Root Administrator is five**
- **Root Administrators only can be added by a Local Administrator**
- **The Root Administrator is the only role that can create new (non-root and non-local) administrators and assign their roles.**
- **There are no other restrictions on the roles that can be assigned to a particular Administrator**

are satisfied.

Application Note: For the Local Administrator, the association of the user to this role is made implicitly, because this user is able to physically access the TOE and by knowing the password to access the administrative

console. For remote administrators, the concept of user is the "remote administration application" that uses the certificate in the user's certificate store to identify (by the use of its CN) and authenticate himself to the TOE. The TSF can associate the user to its role because the association CN-Role is previously configured and stored in the TSF Data.

6.1.6. FPT: Protection of the TSF

6.1.6.1. FPT_APW_EXT.1 Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

6.1.6.2. FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

- **Failure on any of the primary components, that prevents the system from providing a data flow service**
- **Failure on any of the secondary components, that prevents the system from providing a data flow service**

Application Note: This security requirement only applies when the High Availability mode is enabled.

6.1.6.3. FPT_ITC.1 Inter-TSF Confidentiality During Transmission

FPT_ITC.1.1 The TSF shall protect ~~all TSF data~~ *[+the private key associated to the appliance's certificate]* transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

Application Note: This refinement applies only to the exportation of the appliance's private key. See subsection "7.6.8 Export of keys protection".

6.1.6.4. FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from <u>disclosure, modification</u> when it is transmitted between separate *[+ internal appliances TOE's 'Core' modules operating in HA mode]* ~~parts of the TOE~~.

Application Note: This instantiation applies to the information transmission between the primary and secondary internal (PSTi) 'Core' modules in HA

mode. The protection is accomplished by using a TLS channel.

6.1.6.5. FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

Application Note: The TSF does not use any pre-shared keys. It does, however, establish TLS symmetric session keys.

6.1.6.6. FPT_STM.EXT1 Reliable Time Stamps For Its Own Use

FPT_STM.EXT1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM.EXT1.2 The TSF shall allow the Security Administrator to set the time, synchronise time with an NTP server.

6.1.6.7. FPT_TRC.1 Internal TSF consistency

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2 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 **all the active data flow services**.

6.1.6.8. FPT_TST.EXT1 TSF Testing

FPT_TST.EXT1.1 The TSF shall run a suite of the following self-tests at the request of the authorised user to demonstrate the correct operation of the TSF: **integrity of the installed TOE's 'Core' and 'Shell' components**.

Application Note: This operation is performed by using the TOE's firmware management tool ('Restore'). The integrity verification is made by the integrity verification of the complete firmware image, which contains the mentioned software components of the TOE.

6.1.6.9. FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide **Local Administrator and Security Administrators** the ability to query the currently executing version of the **appliance's firmware, TOE 'Core' version, TOE 'Shell' version and TOE 'Restore' version** and no other TOE firmware/software version.

FPT_TUD_EXT.1.2 The TSF shall provide the **Local Administrator in both the PSTi and PSTe appliances** the ability to manually initiate updates to **TOE's 'Core' and 'Shell',** and no other update mechanism.

FPT_TUD_EXT.1.3 The TSF shall provide means to *[+ verify the integrity and]* authenticate firmware/software updates to the **TOE's 'Core' and 'Shell'** using a digital signature prior to installing those updates.

6.1.7. FRU: Resource utilisation

6.1.7.1. FRU_FLT.1 Degraded fault tolerance

FRU_FLT.1.1 The TSF shall ensure the operation of:

- **All security functionality except the admAPI commands that have persistent effects described in Table 18.**

when the following failures occur:

- **Failure of the secondary element due to a failure of the external (PSTe) or internal (PSTi) unit**
- **Failure of the primary element due to a failure of the external (PSTe) or internal (PSTi) unit**

6.1.8. FTA: TOE Access

6.1.8.1. FTA_MCS_EXT.1 Basic limitation of concurrent administrative sessions

FTA_MCS_EXT.1.1 The TSF shall restrict the maximum number of concurrent administrative sessions.

6.1.8.2. FTA_SSL.EXT1 TSF-initiated Session Locking

FTA_SSL.EXT1.1 The TSF shall, for local interactive sessions

- terminate the session

after an Administrator-specified time period of inactivity.

Application Note: the period of inactivity is configurable by the local administrator.

6.1.8.3. FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an *[+ remote administrator]* interactive session after a **configurable elapsed time of remote administrator inactivity**.

Application Note: 'user inactivity' must be understood as the time since the last remote administrator command that causes any modification on the TSF Data. Thus, this not applies to the 'monitoring administrator'

role. The configuration of this parameter is left to the root administration role.

6.1.8.4. FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.1.8.5. FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Before establishing a*[+ local administration console ('Shell')]* user session, the TSF shall display an *[+ configurable]* advisory warning message regarding unauthorised use of the TOE.

Application Note: This requirement is intended to apply to interactive administrative sessions between a human user and a TOE (i.e. the local administrator sessions). IT entities establishing connections or programmatic connections (e.g., remote procedure calls over a network) are not covered by this requirement.

6.1.9. FTP: Trusted Path/Channels

6.1.9.1. FTP_ITC.1/Syslog Inter-TSF Trusted Channel

FTP_ITC.1.1/Syslog The TSF shall *[+be capable of using TLS to]* provide a communication channel between itself and ~~another trusted IT product~~ [+ an authorised remote syslog server] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/Syslog The TSF shall permit the TSF to initiate communication via the trusted channel.

FTP_ITC.1.3/Syslog The TSF shall initiate communication via the trusted channel for **transferring Security System Events and Operation System Events to the remote syslog server**.

6.1.9.2. FTP_ITC.1/PSTaud Inter-TSF Trusted Channel

FTP_ITC.1.1/PSTaud The TSF shall *[+be capable of using TLS to]* provide a communication channel between itself and ~~another trusted IT product~~ [+ an authorised remote PSTaud server] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/PSTaud The TSF shall permit the TSF to initiate communication via the

trusted channel.

FTP_ITC.1.3/PSTaud The TSF shall initiate communication via the trusted channel for **transferring Data Transfer Logging Events to the remote PSTaud server**.

6.1.9.3. FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall *[+ be capable of using TLS to]* provide a communication path between itself and *[+ authorised]* remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification, disclosure.

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **Administrator authentication**, **all remote administration actions**.

6.2. Security assurance requirements

164 Table 19 contains the security assurance requirements for the TOE. These requirements have been chosen from [CCPART3]. The set of security assurance requirements define an Evaluation Assurance Level 4 ("EAL4 - methodically designed, tested, and reviewed") augmented with ALC_FLR.3 ("Systematic flaw remediation") and AVA_VAN.5 ("Advanced methodical vulnerability analysis").

Assurance Class	Assurance Component
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Class ASE: Security Target Evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition

	ASE_TSS.1 TOE summary specification
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Class AVA: Vulnerability Assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Table 19: TOE Security Assurance Requirements

6.3. Security requirements rationale

6.3.1. Security functional requirements rationale

6.3.1.1. Tracing

165 The following table provides a tracing showing which SFRs address which security objectives for the TOE.

SFR	O.AUDIT	O.AVAIL	O.FLOW	O.PROTECT	O.ROLES	O.SECADMIN	O.SECCOMM
FAU_GEN.1	X						
FAU_GEN.2	X						
FAU_SAR.1/Sec	X				X	X	
FAU_SAR.1/Op	X				X	X	
FAU_SAR.1/TD	X				X	X	
FAU_SAR.2	X						
FAU_STG.EXT1	X						
FAU_STG.1	X						
FCS_CKM.1				X			
FCS_CKM.2							X
FCS_CKM.4				X			X
FCS_COP.1/Cipher-AES				X			X
FCS_COP.1/Cipher-CHACHA20							X
FCS_COP.1/Cipher-RSA				X			X
FCS_COP.1/Hash-SHA				X			X
FCS_COP.1/KeyedHash							X
FCS_COP.1/Signature-ECDSA							X
FCS_COP.1/Signature-RSA				X			X
FCS_TLSC_EXT.1							X
FCS_TLSC_EXT.2							X
FCS_TLSS_EXT.1							X
FCS_TLSS_EXT.2							X
FCS_RBG_EXT.1							X
FDP_ACC.2						X	
FDP_ACF.1						X	
FDP_IFC.2/IN			X				
FDP_IFC.2/OUT			X				
FDP_IFF.1/IN			X				
FDP_IFF.1/OUT			X				
FIA_AFL.1						X	
FIA_PMG_EXT.1						X	
FIA_UAU.EXT1						X	

FIA_UAU.7						X	
FIA_X509_EXT.1						X	X
FIA_X509_EXT.2						X	X
FIA_UIA_EXT.1						X	
FMT_MOF.1/LocalConfFuncs					X	X	
FMT_MOF.1/RootConfFuncs					X	X	
FMT_MSA.1/LocalConfAttr			X		X	X	
FMT_MSA.1/RootConfAttr			X		X	X	
FMT_MSA.1/ SecadminConfAttr			X		X	X	
FMT_MSA.1/ ServiceadminConfAttr			X		X	X	
FMT_MSA.1/ MonitoringadminConfAttr			X		X	X	
FMT_MSA.3			X				
FMT_MTD.1					X	X	
FMT_SMF.1						X	
FMT_SMR.2					X		
FPT_APW_EXT.1						X	
FPT_FLS.1		X					
FPT_ITC.1				X			
FPT_ITT.1		X					
FPT_SKP_EXT.1							X
FPT_STM.EXT1	X						
FPT_TRC.1		X					
FPT_TST.EXT1				X			
FPT_TUD_EXT.1				X			
FRU_FLT.1		X					
FTA_MCS_EXT.1						X	
FTA_SSL.EXT1						X	
FTA_SSL.3						X	
FTA_SSL.4						X	
FTA_TAB.1						X	
FTP_ITC.1/Syslog	X						X
FTP_ITC.1/PSTaud	X						X
FTP_TRP.1						X	X

Table 20: Tracing of SFRs to the security objectives for the TOE

6.3.1.2. Justification

166 The following paragraphs provide a justification for each security objective for the TOE, showing that the objective is completely and effectively addressed by the SFRs.

167 **O.AUDIT**: FAU_GEN.1 completely implements the generation of System Events (Operation System Events and Security System Events) and Data Transfer Logging Events. The content of the audit events are also described by FAU_GEN.1. FAU_GEN.2 specifies the association between the event and the generated entity. The protection of the audit trail from unauthorised access is ensured by FAU_SAR.2 whereas FAU_SAR.1/Sec and FAU_SAR.1/Op and FAU_SAR.1/TD define the roles that can access the different audit events. The protection of the storage of the audit trail is provided by FAU_STG.EXT1 and FAU_STG.1. FPT_STM.EXT1

ensures that reliable timestamps can be added to the events. The protection of the data in transit is implemented by FTP_ITC.1/Syslog and FTP_ITC.1/PSTaud.

168 **O.AVAIL**: FRU_FLT.1 specifies the available functions in case of failure. The availability of the system (when configured in HA mode) is ensured by the preservation of a secure state in case of failure (FPT_FLS.1) and the internal consistency of TSF data between the involved parts when a failover occurs (FPT_TRC.1). Additionally, FPT_ITT.1 implements the necessary security on the communications to ensure that no tamper of synchronisation information can happen between the primary and secondary elements.

169 **O.FLOW**: The control of the data flow through 2 information control flow policies are defined by FDP_IFC.2/IN and FDP_IFC.2/OUT. The rules implementing the security objectives are enforced by FDP_IFF.1/IN and FDP_IFF.1/OUT. FMT_MSA.1/LocalConfAttr and FMT_MSA.1/RootConfAttr define additional controls that can be configured by the local administrator and root administrator roles respectively. FMT_MSA.1/SecadminConfAttr defines additional controls that can be configured by the security administrator. FMT_MSA.1/ServiceadminConfAttr defines additional controls that can be configured by the service administrator. FMT_MSA.1/MonitoringadminConfAttr defines additional controls that can be configured by the monitoring administrator. FMT_MSA.3 ensures that the initialisation of security attributes provides restrictive default values, ensuring that the flow control is enforced from the beginning of operation.

170 **O.PROTECT**: FPT_TUD_EXT.1 ensures that the user can verify the current (installed) version of the system firmware containing the TOE installed TOE parts. The TSF is able to verify the authenticity and integrity of a firmware distribution/update by using the following cryptographic functions: FCS_COP.1/Cipher-RSA and FCS_COP.1/Cipher-AES (decryption of firmware image), FCS_COP.1/Signature-RSA (firmware signature verification). The mechanisms to verify the integrity of the TOE 'Core' and 'Shell' modules parts are provided by FPT_TST.EXT1 which also uses FCS_COP.1/Hash-SHA hashing functions for binary comparison of firmware images. Additionally, the protection of the certificate private when exporting it to an external removable storage is accomplished by FPT_ITC.1 which uses FCS_COP.1/Cipher-AES FCS_CKM.1 and FCS_CKM.4 as the supporting cryptographic operations.

171 **O.ROLES**: The implementation of a hierarchy of administrator roles is enforced by several SFRs. Primarily, the SFR FMT_MTD.1 defines the different roles that can manage TSF Data and FMT_SMR.2 ensures that the TOE is able to associated roles to particular authorised users. Several SFRs define the functions (FMT_MOF.1/LocalConfFuncs and FMT_MOF.1/RootConfFuncs) and attributes (FMT_MSA.1/LocalConfAttr, FMT_MSA.1/RootConfAttr, FMT_MSA.1/SecadminConfAttr, FMT_MSA.1/ServiceadminConfAttr, FMT_MSA.1/MonitoringadminConfAttr) that every role can access. Finally, FAU_SAR.1/Sec and FAU_SAR.1/Op and FAU_SAR.1/TD define the different access levels to audit events by the different roles. This set of requirements defines an efficient segmentation of administrative privileges and a sufficient separation of access to different types of audit events.

172 **O.SECADMIN**: This security objective is enforced by SFRs in different areas:

a. The enforcing of access from a role only to its authorised TSF Data and functions is implemented through the use of an access control security policy, defined in FDP_ACC.2 and enforced by FDP_ACF.1 which also defines the

security attributes and functions that can be accessed and the access operation allowed. Also, several SFRs define the functions (FMT_MOF.1/LocalConfFuncs and FMT_MOF.1/RootConfFuncs) and attributes (FMT_MSA.1/LocalConfAttr, FMT_MSA.1/RootConfAttr, FMT_MSA.1/SecadminConfAttr, FMT_MSA.1/ServiceadminConfAttr, FMT_MSA.1/MonitoringadminConfAttr) that every role can access from the overall set of management functions defined in FMT_SMF.1. Managing TSF Data is restricted to the defined roles (FMT_MTD.1). The overall set of functions

b. Regarding access and management of audit events, FAU_SAR.1/Sec and FAU_SAR.1/Op and FAU_SAR.1/TD define the different access levels to audit events by the different roles.

c. The secure identification and authentication operations set needed for a secure administration is provided by the implementation of FIA_AFL.1, FIA_PMG_EXT.1, FIA_UAU.EXT1, FIA_UAU.7 and FIA_UIA_EXT.1.

d. The protection of administrative credentials helps in securing the administration operations, and is defined in FPT_APW_EXT.1

e. The implementation of the following requirements guarantees a secure session management process: FTA_SSL.EXT1, FTA_SSL.3 and FTA_SSL.4 provide de means to ensure that no local session is kept open, while FTA_TAB.1 provides de adequate banner warnings to the users.

f. The implementation of secure communications, avoids impersonation of remote administrators (FTP_TRP.1) and contributes to implement secure administration processes.

g. The validation and association of certificates (implemented by FIA_X509_EXT.1 and FIA_X509_EXT.2) provides the needed identification and authentication of remote administrator users.

h. The limitation on the number of concurrent remote administrative sessions reduces the probability of unauthorised administrative access to the TOE, and is defined in FTA_MCS_EXT.1.

173 **O.SECCOMM**: The cryptographic protection of the communications channels is defined for the remote administration connections, the connections to servers receiving the 'Data Transfer Logging Events', the connection to syslog servers over TLS (when supported) and the connection between the primary PSTi and the secondary PSTi (HA mode only). FTP_TRP.1 ensures that these secure channels are implemented for user connections and FTP_ITC.1/Syslog and FTP_ITC.1/PSTaud ensures that the protection is in place for audit event transfer connections. The protection is provided by the implementation of the TLS protocol, provided by FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1 and FCS_TLSS_EXT.2 and the operations needed to validate and authenticate the associated certificates, provided by FIA_X509_EXT.1 and FIA_X509_EXT.2. The multiple necessary cryptographic operations required by the TLS protocol are implemented by FCS_COP.1/Cipher-AES, FCS_COP.1/Cipher-CHACHA20, FCS_COP.1/Hash-SHA, FCS_COP.1/KeyedHash, FCS_COP.1/Signature-ECDSA and FCS_COP.1/Signature-RSA. The required key management for these operations is provided by

FCS_CKM.2 and FCS_CKM.4 and the protection of the keys is ensured by FPT_SKP_EXT.1. The needed secure entropy source is provided by FCS_RBG_EXT.1.

6.3.2. Security functional requirements dependency rationale

174 The following table provides an analysis of dependency fulfilment of the defined SFR as well as an explanation of unsatisfied or indirectly-satisfied dependencies, whenever applicable:

SFR	Dependencies	Resolution	
FAU_GEN.1	FPT_STM.1	The FPT_STM.1 dependency has been satisfied with FPT_STM.EXT1	
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 The FIA_UID.1 dependency has been satisfied with FIA_UIA_EXT.1	
FAU_SAR.1/Sec	FAU_GEN.1	FAU_GEN.1	
FAU_SAR.1/Op	FAU_GEN.1	FAU_GEN.1	
FAU_SAR.1/TD	FAU_GEN.1	FAU_GEN.1	
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1/Sec + FAU_SAR.1/Op + FAU_SAR.1/TD	
FAU_STG.EXT1	FAU_GEN.1 FTP_ITC.1	FAU_GEN.1 FTP_ITC.1/Syslog + FTP_ITC.1/PSTaud	
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	
FCS_CKM.1	FCS_CKM.2|FCS_COP.1 FCS_CKM.4	FCS_COP.1/Hash-SHA FCS_CKM.4	
FCS_CKM.2	FDP_ITC.1|FDP_ITC.2|FCS_CKM.1 FCS_CKM.4	Instead of FCS_CKM.1 the required generation of the key is provided by FCS_RBG_EXT.1 FCS_CKM.4	
FCS_CKM.4	FDP_ITC.1|FDP_ITC.2|FCS_CKM.1	For keys used to encrypt exported password:	FCS_CKM.1
		For keys used in the TLS handshake primitives:	FCS_RBG_EXT.1 + FCS_CKM.2 instead of FCS_CKM.1
FCS_COP.1/Cipher-AES	FDP_ITC.1|FDP_ITC.2|FCS_CKM.1 FCS_CKM.4	For keys used to encrypt exported password:	FCS_CKM.1 FCS_CKM.4
		For keys used in the TLS handshake primitives:	FCS_RBG_EXT.1 + FCS_CKM.2 instead of FCS_CKM.1 FCS_CKM.4
		For firmware decryption, the dependencies need not to be met	
FCS_COP.1/Cipher-RSA	FDP_ITC.1|FDP_ITC.2|FCS_CKM.1 FCS_CKM.4	The dependencies need not to be met	

FCS_COP.1/Hash-SHA	FDP_ITC.1|FDP_ITC.2|FCS_CKM.1 FCS_CKM.4	The dependencies need not to be met.	
FCS_COP.1/KeyedHash	FDP_ITC.1|FDP_ITC.2|FCS_CKM.1 FCS_CKM.4	For use to generate keys:	Key is provided externally, so FCS_CKM.1 is not needed FCS_CKM.4
		For use within the TLS protocol:	FCS_RBG_EXT.1 + FCS_CKM.2 instead of FCS_CKM.1 FCS_CKM.4
FCS_COP.1/Signature-ECDSA	FDP_ITC.1|FDP_ITC.2|FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 FCS_CKM.4	
FCS_COP.1/Signature-RSA	FDP_ITC.1|FDP_ITC.2|FCS_CKM.1 FCS_CKM.4	The dependencies need not to be met.	
FCS_TLSC_EXT.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1 FCS_RBG_EXT.1 FIA_X509_EXT.1 FIA_X509_EXT.2	FCS_CKM.1 ('Key generation') is met by 'Key establishment', which is provided by FCS_CKM.2+FCS_RBG_EXT.1	
		FCS_CKM.2 FCS_COP.1/Cipher-AES FCS_COP.1/Cipher-CHACHA20 FCS_COP.1/Hash-SHA FCS_COP.1/KeyedHash FCS_COP.1/Signature-ECDSA FCS_COP.1/Signature-RSA FCS_RBG_EXT.1 FIA_X509_EXT.1 FIA_X509_EXT.2	
FCS_TLSC_EXT.2	FCS_CKM.1 FCS_CKM.2 FCS_COP.1 FCS_RBG_EXT.1 FCS_TLSC_EXT.1 FIA_X509_EXT.1 FIA_X509_EXT.2	FCS_CKM.1 ('Key generation') is met by 'Key establishment', which is provided by FCS_CKM.2+FCS_RBG_EXT.1	
		FCS_CKM.2 FCS_COP.1/Cipher-AES FCS_COP.1/Cipher-CHACHA20 FCS_COP.1/Hash-SHA FCS_COP.1/KeyedHash FCS_COP.1/Signature-ECDSA FCS_COP.1/Signature-RSA FCS_RBG_EXT.1 FCS_TLSC_EXT.1 FIA_X509_EXT.1 FIA_X509_EXT.2	

FCS_TLSS_EXT.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1 FCS_RBG_EXT.1 FIA_X509_EXT.1 FIA_X509_EXT.2	FCS_CKM.1 ('Key generation') is met by 'Key establishment', which is provided by FCS_CKM.2+FCS_RBG_EXT.1
		FCS_CKM.2 FCS_COP.1/Cipher-AES FCS_COP.1/Cipher-CHACHA20 FCS_COP.1/Hash-SHA FCS_COP.1/KeyedHash FCS_COP.1/Signature-ECDSA FCS_COP.1/Signature-RSA FCS_RBG_EXT.1 FIA_X509_EXT.1 FIA_X509_EXT.2
FCS_TLSS_EXT.2	FCS_CKM.1 FCS_CKM.2 FCS_COP.1 FCS_RBG_EXT.1 FCS_TLSS_EXT.1 FIA_X509_EXT.1 FIA_X509_EXT.2	FCS_CKM.1 ('Key generation') is met by 'Key establishment', which is provided by FCS_CKM.2+FCS_RBG_EXT.1
		FCS_CKM.2 FCS_COP.1/Cipher-AES FCS_COP.1/Cipher-CHACHA20 FCS_COP.1/Hash-SHA FCS_COP.1/KeyedHash FCS_COP.1/Signature-ECDSA FCS_COP.1/Signature-RSA FCS_RBG_EXT.1 FCS_TLSS_EXT.1 FIA_X509_EXT.1 FIA_X509_EXT.2
FCS_RBG_EXT.1	None	N/A
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 FMT_MSA.3
FDP_IFC.2/IN	FDP_IFF.1	FDP_IFF.1/IN
FDP_IFC.2/OUT	FDP_IFF.1	FDP_IFF.1/OUT
FDP_IFF.1/IN	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/IN FMT_MSA.3
FDP_IFF.1/OUT	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/OUT FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	The FIA_UAU.1 dependency has been satisfied with FIA_UIA_EXT.1
FIA_PMG_EXT.1	None	N/A
FIA_UAU.EXT1	None	N/A
FIA_UAU.7	FIA_UAU.1	The FIA_UAU.1 dependency has been satisfied with FIA_UIA_EXT.1
FIA_UIA_EXT.1	FTA_TAB.1	FTA_TAB.1
FIA_X509_EXT.1	FIA_X509_EXT.2	FIA_X509_EXT.2
FIA_X509_EXT.2	FIA_X509_EXT.1	FIA_X509_EXT.1
FMT_MOF.1/LocalConfFuncs	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 FMT_SMF.1
FMT_MOF.1/RootConfFuncs	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 FMT_SMF.1

FMT_MSA.1/LocalConfAttr	FDP_ACC.1|FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.2 FMT_SMR.2 FMT_SMF.1
FMT_MSA.1/RootConfAttr	FDP_ACC.1|FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.2 FMT_SMR.2 FMT_SMF.1
FMT_MSA.1/SecadminConfAttr	FDP_ACC.1|FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.2 FMT_SMR.2 FMT_SMF.1
FMT_MSA.1/ServiceadminConfAttr	FDP_ACC.1|FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.2 FMT_SMR.2 FMT_SMF.1
FMT_MSA.1/MonitoringadminConfAttr	FDP_ACC.1|FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.2 FMT_SMR.2 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.2
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 FMT_SMF.1
FMT_SMF.1	None	N/A
FMT_SMR.2	FIA_UID.1	The FIA_UID.1 dependency has been satisfied with FIA_UIA_EXT.1
FPT_APW_EXT.1	None	N/A
FPT_FLS.1	None	N/A
FPT_ITC.1	None	N/A
FPT_ITT.1	None	N/A
FPT_SKP_EXT.1	None	N/A
FPT_STM.EXT1	None	N/A
FPT_TRC.1	FPT_ITT.1	FPT_ITT.1
FPT_TST.EXT1	None	N/A
FPT_TUD_EXT.1	FCS_COP.1	FCS_COP.1/Cipher-RSA FCS_COP.1/Signature-RSA FCS_COP.1/Hash-SHA
FRU_FLT.1	FPT_FLS.1	FPT_FLS.1
FTA_MCS_EXT.1	FIA_UID.1	The FIA_UID.1 dependency has been satisfied with FIA_UIA_EXT.1
FTA_SSL.EXT1	FIA_UAU.1	The FIA_UAU.1 dependency has been satisfied with FIA_UIA_EXT.1
FTA_SSL.3	None	N/A
FTA_SSL.4	None	N/A
FTA_TAB.1	None	N/A
FTP_ITC.1/Syslog	None	N/A
FTP_ITC.1/PSTaud	None	N/A
FTP_TRP.1	None	N/A

Table 21 SFR dependencies

6.3.3. Security assurance requirements rationale

175 The desired security assurance level for the TOE is EAL4 + ALC_FLR.3 + AVA_VAN.5.

176 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.

177 The ALC_FLR.3 augmentation has been added to demonstrate that the vendor has an effective procedure for flaw remediation and distribution, which allows the user to send identified flaws, to follow the flaw remediation process and to receive corrective fixes.

178 The addition of AVA_VAN.5 is intended to demonstrate that the TOE is resistant to penetration attackers with a High attack potential.

7. TOE summary specification

7.1. Auditing

179 The TSF generates two types of events:

- System Events
- Data Transfer Logging Events

7.1.1. System events

180 System events are generated by the TSF. The generated system events are enumerated in FAU_GEN.1.

181 These events are divided into two types: security and operation. The configuration parameters described in this section are configured independently for Security System Events and Operation System Events. Therefore, the behaviour of the TSF regarding the management of Security System Events is also independent from the management of the Operation System Events.

182 The Security System Events and Operation System Events are stored in two local storage containers (in the form of human-readable text log files) in the internal appliance (PSTi). The Security Administrator role (see FDP_ACF.1 and Table 18) can use the TSF management functions (as specified in FMT_SMF.1) to configure the rotation policy of these log files.

183 The TSF detects when a log file reaches its configured maximum size and, if that is the case, the log file is renamed and stored and a new log file is created. If the maximum number of log files is reached, then the oldest log file is deleted to allow the more recent log file be created (FAU_STG.EXT1) and an audit event (GlobalEventLocalStorageIssue) is generated (FAU_GEN.1).

184 The System Events are also sent via syslog protocol (using TCP, UDP and TLS) to a server belonging to the operational environment. The TSF has a management function (defined in FMT_SMF.1) that handles the parameters associated to this function (destination server, severity levels and log rotation parameters), which can be modified by the Security Administrator role (see FDP_ACF.1 and Table 18). The destination syslog server for Operation System Events and for Security System Events can be the same or different.

185 The use of TLS on top of syslog protocol to transfer System Events is also one of the functions of the TSF (FTP_ITC.1/Syslog), although its activation is optional and must be done by a Security Administrator. The cryptographic operations needed to implement this secure channel are explained in the subsection “7.7.2 Certificate validations”. Upon failure of authentication of a syslog server, a Security System Event (GlobalEventServerConnectSecFail) is generated (FAU_GEN.1).

186 The TSF only allows some remote TSF Administrator roles (see FDP_ACF.1 and Table 18 for the role permissions needed to access Operation System Events and Security System Events) to read information from System Events (FAU_SAR.1/Sec, FAU_SAR.1/Op and FAU_SAR.2), thus avoiding the stored log files to be deleted or modified (FAU_STG.1).

187 The information included in System Events is depicted in FAU_GEN.1. In addition, those events generated as a consequence of a remote user interaction include the user identification

(FAU_GEN.2). The events generated by the interaction of a local administrator user are exclusive of him, so they can be implicitly mapped to him (FAU_GEN.2).

188 There are two events that indicate the starting and ending of audit functions (as described in FAU_GEN.1), labelled GlobalSystemStartUp and GlobalSystemShutdown.

7.1.2. Data Transfer Logging Events

189 The TSF obtains Data Transfer Logging Events by extracting this information from the particular service modules and sending them to the Data Transfer Logging Events (PSTaud) server. The Data Transfer Logging Events contain, apart from the basic required information, other structured data (FAU_GEN.1) that is specific to the originating service (FAU_GEN.1).

190 The TSF includes the internal appliance (PSTi) identity (CN of its certificate) in each Data Transfer Logging Event (FAU_GEN.2).

191 The TSF sends these events by the use of a secure TLS channel (FTP_ITC.1/PSTaud) to the Data Transfer Logging server (PSTaud). The TSF has a management function (defined in FMT_SMF.1) that handles the parameters associated to this function (destination server and TCP port, CN of authorised PSTaud server), which can be modified by the Security Administrator role (see FDP_ACF.1 and Table 18). The cryptographic operations needed to implement this secure channel are explained in the subsection “7.7.2 Certificate validations“. Upon failure of authentication of the Data Transfer Logging Server (PSTaud), a Security System Event (AuditServerConnectionSecFail) is generated (FAU_GEN.1).

192 The TSF will protect those audit trails (Data Transfer Logging Events) from deletion (FAU_STG.1) because the TOE does not offer any deletion operation to the administrators and it only deletes these events after they have been securely (FTP_ITC.1/PSTaud) transferred to the PSTaud server (FAU_STG.EXT1). If those audit trails (Data Transfer Logging Events) cannot be transferred to the PSTaud server, periodic Operation System Events (AuditLocalStorageWarning) are generated (FAU_GEN.1) to report that the audit storage is nearly full. If the maximum audit storage size is reached, then the services are stopped (FDP_IFF.1/IN and FDP_IFF.1/OUT) and an Operation System Event (AuditLocalStorageFailure) is generated (FAU_GEN.1).

7.2. Identification and authentication

7.2.1. Local administrators

193 The identification of the local administrator is performed implicitly by its physical Access to the TOE and by the use of the authorised local console password. The TOE does not implement any other identification functionality for this role.

194 The local administration console (‘Shell’) shows a banner to the user prior to allow him any other operation (FTA_TAB.1, FIA_UIA_EXT.1). This banner is configurable by the local administrator (FMT_SMF.1).

195 The TOE authenticates the local administrator by the use of a passphrase (FIA_UAU.EXT1) that the user must type on the local administration console (‘Shell’). The TSF force the configuration of that passphrase the first time that the ‘Shell’ is run. This passphrase is stored as a hash by the TSF (FPT_APW_EXT.1).

196 The TOE allows the Local Administrator to access system status check data previously to have been authenticated (FIA_UIA_EXT.1).

197 The password typed by the local administrator when accessing the 'Shell' component is hidden by the local administration console ('Shell'), so it never gets printed on it (FIA_UAU.7).

198 The local administrator passphrase must meet the requirements specified in FIA_PMG_EXT.1. This policy is configurable by the local administrator (FMT_SMF.1).

199 The TOE manage unsuccessful local console attempts by doubling the 'login delay time' (the time that the login facility is locked between unsuccessful login attempts) every time that an unsuccessful attempt occur (FIA_AFL.1), up to a maximum locking time.

7.2.2. Remote administrators

200 The identification of the remote user is performed by reading the CN (Common Name) of the certificate that the user presents to the TSF in the TLS session establishment phase. The TSF can identify the CN of this certificate because it must have been previously configured by:

a. For the Root Administrator(s): the local administrator of the TOE.

b. For the other remote administrators: the root administrator of the TOE.

201 The TSF authenticates the user by checking the validity of the certificate (FIA_X509_EXT.1) verifying the signature of the certificate (FIA_X509_EXT.2) presented in the in the TLS session establishment phase. It can do that because the CA that signed this certificate was previously configured in the TSF by the local administrator.

202 If the user is not correctly identified and authenticated, then the TSF aborts the connection establishment, so the user cannot perform any action on the TSF (FIA_UIA_EXT.1, where allowed actions do not apply to the remote users). Upon failure of authentication of a remote administrator, a Security System Event (AdminConnectRejection) is generated (FAU_GEN.1).

7.3. TOE administration

203 The TOE enforces access control to all TSF data and functions (FDP_ACC.2).

204 The first time the TOE is run, no administrator is configured, providing the most restrictive default values regarding the User Access Control Policy (FMT_MSA.3).

205 The TOE uses one local administrator role and 4 remote administrator roles as specified in FMT_MTD.1 and FMT_SMR.2, and it restricts the ability to manage the TSF Data to those roles (FMT_MTD.1). The management functions of the TSF are specified in FMT_SMF.1. The set of functions allowed for each role is described in FDP_ACF.1.

206 The association of users to roles (FMT_SMR.2) is implemented as follows:

a. The local administrator is the one that can physically access to the local administration console ('Shell'), so the assignment of the role is implicit.

b. The role association to the root administration user is assigned by the local administrator, who configures the CN for the root administrator certificate (FMT_MSA.1/LocalConfAttr).

c. The other non-local, non-root remote administrators, role associations are performed by the root administrator, who configures the CN of their associated certificates through the admAPI (FMT_MSA.1/RootConfAttr).

207 The local administrator must perform the following initial configuration tasks (FMT_MOF.1/LocalConfFuncs and FMT_MSA.1/LocalConfAttr define the security part of this configuration task):

a. Configures its own password (the first time it access the TOE's 'Shell').

b. Configures the local TSF data:

i. PKI Configuration.

ii. Network parameters for all network interfaces in both High Security and Low Security domains.

iii. High Availability appliance configuration (if HA mode is in place)

iv. NTP server configuration

v. Parametrisation of password policy.:

vi. Parametrization of session handling.

c. Configures the system license

d. Optionally applies service parametrization.

208 Some TSF functionality can be activated by the local administrator (FMT_MOF.1/LocalConfFuncs). In the case of the High Availability mode and available services, this functionality is usually pre-enabled in the vendor installation. It also can be enabled by importing a license file, signed by the vendor, by using the TOE's local administration console ('Shell'). For the rest of the functionality specified in FMT_MOF.1/LocalConfFuncs, it is enabled using some ad-hoc commands of the TOE's 'Shell'.

209 The local administrator can perform firmware management (integrity firmware verification and firmware installation/updates) as defined in FDP_ACF.1 and Table 18

210 All administrator roles can import and export the configuration data that they have access to (see FDP_ACF.1 and Table 18).

211 The TSF allows the managing of the non-local, non-root administrator roles to the root administrator only (see FDP_ACF.1 and Table 18)

212 FMT_MOF.1/RootConfFunc and FMT_MSA.1/RootConfAttr define what security functions the Root Administrator can enable and what security attributes he can modify.

213 The security configuration tasks (configuration of audit parameters and date/time configuration) is granted only to the Security Administrator role (see FMT_MSA.1/SecadminConfAttr, FDP_ACF.1 and Table 18)

214 The operations for service management are only allowed to the service administrators (see FDP_ACF.1 and Table 18)

215 Access to audit events is specified in FAU_SAR.1, FDP_ACF.1 and Table 18:

a. Security System Events can be accessed by the Security Administrator role

b. Operation System Events are accessible by the Service Administrator role

c. Data Transfer Logging Events are sent by the TOE to a PSTAud server (non TOE)

216 Additionally, the Monitoring Administrator role can access the general status of the devices, services and channels. He can also apply visualisation filters and reset service statistics (see FDP_ACF.1 and Table 18).

217 All remote administrators must establish a secure TLS 1.2/TLS1.3 secure connection channel (by using the PSTadm software) before performing any administrative tasks (FTP_TRP.1).

7.4. Service Data Flow management

218 The TSF controls the global services behaviour, both for inbound and outbound services, by the use of the following functions (FMT_SMF.1):

a. Start and Stop of each licensed service.

b. Creation, deletion and configuration of service channels.

c. Special parametrisation of some services, by using the associated local administration console ('Shell') context.

d. Monitoring the status of the inbound and outbound services as well as the status of the channels.

219 Initially, no service or data flow is running, providing the most restrictive default values regarding the Input Data Flow Policy and Output Data Flow Policy (FMT_MSA.3).

220 That way, the TSF can enforce that only data flows belonging to a licensed and running service can traverse the TOE in the service's direction: inbound (FDP_IFC.2/IN and FDP_IFF.1/IN) or outbound (FDP_IFC.2/OUT and FDP_IFF.1/OUT).

221 These data flow traverse from the TSF in one security domain to the TSF in the other security domain (depending on the data flow direction of the service) through the external PSTgateways passive data transfer device.

7.5. High availability

222 In the High Availability mode, two appliances in each security domain can provide service redundancy. There are two redundancy schemes, that are configured in the TSF exclusively through licensing:

a. Active-Active mode: the primary and secondary appliances share part of the workload of the service. The configuration of how this sharing operates depends on each service.

b. Active-Passive mode: the secondary appliances have no interface enabled and they assume the primary role when a failure on the primary appliance(s) is detected.

223 Should a failure[8] occur on any secondary element, the primary element will maintain all the security functionality (FRU_FLT.1).

224 Should a failure occur on any primary element, the secondary element will maintain all the security functionality, with the exception of the commands having a persistent effect (FRU_FLT.1):

a. RemoveChCfg

b. SetAdmCfg

c. SetMonitorCfg

d. SetSrvCfg

e. ShutdownSrv

f. StartSrv

g. StopSrv

h. UpdateChCfg

i. SetSystemTime

225 The complete functionality of the system is recovered when the failed element fault condition ends.

226 The synchronisation between the primary and secondary elements (FPT_TRC.1) includes the configuration, global operating status as well as service operational status, and is maintained through a dedicated secure TLS communication channel between the internal appliances (PSTi) in the High Security Domain (FPT_ITT.1), which implements encryption and mutual authentication. These communications allow both elements to keep their configurations in synch as well as detect fault conditions (FPT_FLS.1).

227 Upon failure recovery the TSF will:

a. In the case of an Active-Active configuration: automatically regain the initial state.

b. In the case of an Active-Passive configuration: the currently active TSF will continue its operation and the recovered TSF will act as the passive element.

7.6. Protection of the system

7.6.1. Backup and restore of system configuration

228 All use cases in Table 18 that imply access to TSF configuration data allow the administrator to backup and restore that configuration data. That means that all administrator roles can import and export the configuration data that they have access to (see FDP_ACF.1 and Table 18).

7.6.2. TSF integrity verification and secure installation/updates

[8] The Word 'failure' must be interpreted as a condition that affects one data flow service availability

229 Some administrator roles can access the TOE components versions (FPT_TUD_EXT.1) in the following ways:

a. The TOE 'Shell' version can be accessed by the local administrator, by using the TOE 'Shell' itself

b. The TOE 'Restore' version can be accessed by the local administrator by booting from the appliance's DVD

c. The TOE 'Core' version can be accessed:
   i. By a remote Security Administrator through the use of admAPI
   ii. By the local administrator by using the TOE 'Shell'.

230 The Local Administrator can use the firmware management tool ('Restore') to verify the installed firmware integrity (FPT_TUD_EXT.1, FPT_TST.EXT1) by hashing comparison of the installed firmware image against the firmware image located either in the appliance DVD or in an external USB memory. This process works as follows:

a. Upon start, the TOE 'Restore' component allows to load an encrypted firmware image and its corresponding signature file from the appliance's DVD itselft or from an external USB memory.

b. This firmware image is encrypted using symmetric cryptography (FCS-COP.1/Cipher-AES) with a key that is distributed along with the firmware image itself. This key is in turn protected using asymmetric cryptography using the manufacturer's private key, which is securely guarded.

c. The 'Restore' module performs a signature verification of the encrypted firmware image file using a certificate which is distributed alongside with the signature file. This certificate is validated against a CA certificate that is embedded in the TOE (FCS_COP.1/Signature-RSA), then decrypts the symmetric key needed to decrypt the firmware (FCS_COP.1/Cipher-RSA) using a different asymmetric key (which is embedded in the TOE), and then decrypts the firmware image using symmetric cryptography and the decrypted symmetric key (FCS_COP.1/Cipher-AES).

d. After the previous operations have finished successfully, the TOE 'Restore' component offers to the local user the possibility of perform the integrity verification. If the user launches it, the 'Restore' component calculates the hash of the installed image and the one of the decrypted image and compares them, returning the result of this comparison (FCS_COP.1/Hash-SHA).

231 The TOE firmware management tool ('Restore') allows the Local Administrator to perform firmware updates. The firmware updates are distributed encrypted and signed. The tool will perform signature verification (FCS_COP.1/Signature-RSA) and decryption (FCS_COP.1/Cipher-RSA+FCS_COP.1/Cipher-AES) prior to proceed with the update operation (FPT_TUD_EXT.1). The TOE firmware management tool ('Restore') also allows the Local Administrator to perform firmware installation.

232 The TOE local administration console ('Shell') of the internal appliance (PSTi) allows the Local Administrator to:

a. Verify the signature of a license file that enables some PSTgateways particular functions (available services and High Availability mode) (FMT_SMF.1). This verification is done by FCS_COP.1/Cipher-RSA.

b. Verify the signature of a service parametrization file that loads parametrization data for some specific services. This verification is done by FCS_COP.1/Cipher-RSA.

7.6.3. Time synchronisation

7.6.3.1. NTP synchronisation

233 The TOE allows the Local Administrator to configure the operating system of the server PSTi to synchronise its system time with up to five external NTP servers, located in the High Security Domain network (FPT_STM.EXT1).

234 The TOE will use the system time of PSTi as a reliable time reference for its time stamps.

235 Only the Local Administrator can enable or disable the NTP synchronisation.

236 The configuration data regarding the aforementioned NTP server(s) can be performed only by the Local Administrator (FMT_MOF.1/LocalConfFunc).

7.6.3.2. Manual synchronisation

237 The Security Administrator can synchronise, by using an admAPI command, the time of the operating system (system time) of PSTi with the PSTadm workstation time remotely (FPT_STM.EXT1).

238 The TOE will use the system time of PSTi as a reliable time reference for its time stamps.

7.6.4. Session management

7.6.4.1. Local session management

239 The Local Administrator can establish a session with the TSF 'Shell' component using the local administration console ('Shell'). The Local Administrator must authenticate himself to the TSF by the use of a passphrase (FIA_UAU.EXT1).

240 The Local Administrator can manually close its 'Shell' session, by the use of a console command (FTA_SSL.4). There is also a configurable inactivity period that causes the Local Administrator session to automatically be closed (FTA_SSL.EXT1).

241 The Local Administrator also can access the 'Restore' component of the TOE in each appliance (PSTi or PSTe) by booting from the appliance DVD. This session is terminated as soon as the Local Administrator reboots the system again.

7.6.4.2. Remote session management

242 The TSF will limit the Remote Administrator number of concurrent administrative sessions (FTA_MCS_EXT.1.1).

243 The administrative sessions can be manually closed by the interactive users controlling the PSTadm software session (FTA_SSL.4). Also, the TSF will close the session when the remote administrator hasn't sent a modification command[9] for a time lapse (FTA_SSL.3) that is configurable by the root administrator.

244 The Data Transfer Logging connections are initiated by the TSF and closed by it after all the transfer information has been sent (FTS_SSL.4).

7.6.5. Password protection

245 The TSF does not store Local Administrator password in plain-text: it stores the SHA256 hash of the Local Administrator passphrase (FPT_APW_EXT.1). In addition, read access of this credential information is not allowed to any role.

246 Also, the TSF protects the Local Administrator passphrase from been seen in the moment of authentication, by hiding the characters in the TOE's 'Shell' (FPT_APW_EXT.1).

7.6.6. Session key protection

247 The TSF uses session keys to protect the confidentiality of:

a. Communication between the remote administrative users (by using PSTadm to access TSF's admAPI) and the TSF.

b. Communication between the TSF and the Data Transfer Logging (PSTaud) server

c. Communication between the TSF and a syslog server supporting TLS

d. Communication between the primary and secondary elements, when High Availability mode is in place.

248 Session keys for remote admin and audit connections are securely exchanged by using TLS session establishment (FCS_CKM.2). This mechanism protects the session keys from external reading.

249 The private key associated to the internal appliance (PSTi) certificate is stored by the TSF and it is not readable by any user afterwards (FPT_SKP_EXT.1).

7.6.7. Data consistency

250 The TSF maintains TSF data consistency between the primary internal appliance and the secondary one (FPT_ITT.1), when the TOE is configured in HA mode.

251 The TSF data synchronisation in HA mode between the primary internal appliance and the secondary one is explained in section "7.5 High availability".

7.6.8. Export of keys protection

[9] For this reason the inactivity time does not affect to the remote administrators that only have the monitoring administrator role.

252 The TSF protects from disclosure the appliance private key when it is exported by the local administrator to an external removable storage (FPT_ITC.1). The appliance protects it by generating a pkcs12 container which contains the appliance's certificate and the associated encrypted private key. The private key is encrypted using the algorithm AES-256 (FCS_COP.1/Cypher-AES) employing an encryption key that is derived (FCS_CKM.1) from a passphrase that must be provided by the local administrator. The generated password is securely erased (FCS_CKM.4) right after its use.

7.7. Cryptography

253 The TSF uses cryptographic support for the following purposes:

a. To protect the confidentiality and integrity of the communications between the remote administrative users (by using PSTadm to access TSF's admAPI) and the TSF, using TLS1.2 or TLS1.3 channels.

b. To protect the confidentiality and integrity of the communications between the TSF and the Data Transfer Logging (PSTaud) server, using TLS1.2 or TLS1.3 channels.

c. To protect the confidentiality and integrity of the communications between the TSF and a configured syslog server(s) supporting TLS, using TLS1.2 or TLS1.3 channels.

d. To protect the confidentiality and integrity of the communications between the two internal appliances (PSTi) when configured in High Availability mode.

e. To mutually authenticate the TSF and the remote administrative users accessing the TOE through the admAPI.

f. To mutually authenticate the primary and secondary TOE 'Core' components when the TOE is configured in High Availability mode.

g. To mutually authenticate the TSF and the configured remote syslog server(s).

h. To mutually authenticate the TSF and the configured PSTaud server.

i. To decrypt firmware updates.

j. To verify the digital signature of firmware updates.

k. To verify integrity of firmware and firmware updates.

l. To verify the digital signature of the license.

m. To verify the digital signature of service parametrisations.

n. To protect the password of the Local Administrator.

254 The following subsections detail the cryptographic operations and parameters used in every group of functionality.

7.7.1. Password hashing

255 The only password that is stored in the TOE is the 'Local Administrator' password. The stored information is the SHA-256 hash of the concatenation of the plain-text password (FCS_COP.1/Hash-SHA).

Mechanism	Key type	Hash size (bits)
Password Hashing	SHA	256

Table 22: Cryptographic mechanisms implemented by the TOE's for password hashing

7.7.2. Certificate validations

256 The TSF will validate a certificate according to FIA_X509_EXT.1 in the following cases:

a. When a local administrator imports a CA certificate

b. When a local administrator imports an appliance certificate

c. When OCSP certificate is received as part of an OCSP response

d. When a CRL certificate is received as part of a CRL response

e. When a client certificate is received during the TLS session negotiation protocol

f. When a server certificate is received during the TLS session negotiation protocol

257 If the certification validation is not successful, the TSF will reject it.

7.7.3. TLS communications

258 The TSF supports exclusively TLS 1.2 and TLS 1.3 protocol versions (FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2), as described in Table 23.

259 The TSF implements the client side of the TLS protocol. In this case, during the TLS session establishment, it will only offer the ciphersuites and key sizes described in Table 23. The TSF acts as a TLS client (FCS_TLSC_EXT.1) in the following situations:

a. When connecting to a PSTaud server: in this case, the TSF connects to the PSTaud server using the parameters configured by the Security Administrator. It uses its appliance certificate to authenticate himself to the PSTaud server (FCS_TLSC_EXT.2 and FIA_X509_EXT.2). It also verifies the certificate presented by the PSTaud server (FIA_X509_EXT.1) and checks that the CN of the certificate is identical to the one that it has registered for the PSTaud server (FCS_TLSC_EXT.1).

b. When connecting to a syslog server: in this case, the TSF connects to the syslog server using the parameters configured by the Security Administrator. It uses its appliance certificate to authenticate himself to the syslog server (FCS_TLSC_EXT.2 and FIA_X509_EXT.2). It also performs the verification of the certificate presented by the syslog server (FIA_X509_EXT.2) and, only if the Security Administrator has configured the CN of the syslog server certificate,

checks that the CN of the certificate is identical to the one that it has registered for the syslog server (FCS_TLSC_EXT.1).

c. When connecting to the secondary TSF instance when configured in HA mode. In this case, the operation is identical to the connection to a PSTaud server, except for the fact that the CN of the certificate in the secondary TSF instance must match the one in its own appliance certificate.

260 The TSF implements the server side of the TLS protocol. In this case, during the TLS session establishment, it will only accept the ciphersuites and key sizes described in Table 23. Also, the TSF will only accept key sizes equal or larger than the one of its own appliance certificate. The TSF acts as a TLS server (FCS_TLSS_EXT.1, FCS_TLSS_EXT.2) in the following situations:

a. When a PSTadm user is connecting to the TSF: in this case, the TSF will verify the certificate presented by the PSTadm user (FIA_X509_EXT.1) and will check that the CN of the certificate matches one of the CN previously registered by the Local/Root Administrator. That way the TSF identifies and authenticates a remote administrator. It also uses its appliance certificate to authenticate himself to the PSTadm user (FCS_TLSS_EXT.1, FCS_TLSS_EXT.2, and FIA_X509_EXT.2).

b. When acting as secondary TSF instance and the primary TSF instance is connecting to it: in this case, the TSF will verify the certificate presented by the primary TSF instance (FIA_X509_EXT.1) and will check that the CN of its certificate matches the one in its own appliance certificate. It also uses its appliance certificate to authenticate himself to the primary TSF instance (FCS_TLSS_EXT.1, FCS_TLSS_EXT.2 and FIA_X509_EXT.2).

261 The following table depicts the all the cryptographic algorithms used by the TLS implementation of the TOE:

<table>
<tr><th rowspan="2">TLS Version</th><th rowspan="2">Ciphersuite description</th><th colspan="2">Signing Verification</th><th colspan="2">Encryption</th></tr>
<tr><th>Alg.</th><th>Key size (bits)</th><th>Alg.</th><th>Key size (bits)</th></tr>
<tr><td rowspan="5">TLS 1.2</td><td>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</td><td>ECDSA</td><td rowspan="3">256 .. 521</td><td>AES</td><td>256</td></tr>
<tr><td>TLS_ECDHE_ECDSA_WITH_AES_256_CCM</td><td>ECDSA</td><td>AES</td><td>256</td></tr>
<tr><td>TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256</td><td>ECDSA</td><td>CHACHA20</td><td>256</td></tr>
<tr><td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</td><td>RSA</td><td rowspan="2">3072 .. 15360</td><td>AES</td><td>256</td></tr>
<tr><td>TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256</td><td>RSA</td><td>CHACHA20</td><td>256</td></tr>
<tr><td rowspan="4">TLS 1.3</td><td rowspan="2">TLS_AES_256_GCM_SHA384</td><td>RSA</td><td>3072 .. 15360</td><td rowspan="2">AES</td><td rowspan="2">256</td></tr>
<tr><td>ECDSA</td><td>256 .. 521</td></tr>
<tr><td rowspan="2">TLS_CHACHA20_POLY1305_SHA256</td><td>RSA</td><td>3072 .. 15360</td><td rowspan="2">CHACHA20</td><td rowspan="2">256</td></tr>
<tr><td>ECDSA</td><td>256 .. 521</td></tr>
</table>

Table 23: Cryptographic algorithms used by the TLS implementation

262 According to Table 23, and after the TLS negotiation, the TSF will use the negotiated algorithms and key sizes for performing the following cryptographic operations during the TLS session:

a. Generation and distribution of keys (FCS_RBG_EXT.1, FCS_CKM.2)

b. Certificate verification (FIA_X509_EXT.1) and Authentication (FIA_X509_EXT.2), which will include signing verification of certificates and messages (FCS_COP.1/Signature-ECDSA and FCS_COP.1/Signature-RSA).

c. The confidentiality protection of the communication is performed by using the AES256 algorithm, and the session key is generated conforming to the TLS 1.2 or TLS 1.3 specification (FCS_COP.1/Cipher-AES).

d. The integrity protection of the data in transit is performed by using the corresponding HMAC algorithms, as specified in the corresponding TLS protocol (FCS_COP.1/KeyedHash).

e. The TLS implementation will ensure that symmetric session keys generated for each user session are securely destroyed (FCS_CKM.4).

7.7.4. Firmware management

263 All firmware updates are distributed encrypted and digitally signed, whether it is the original firmware distribution on the appliance DVD's or a firmware update.

264 The TOE firmware management tool ('Restore') allows the sign verification of the distributed encrypted firmware and its subsequent decryption. Sign verification is made by using the RSA Digital Signature Algorithm (FCS_COP.1/Signature-RSA). The decryption operation is made by using AES algorithm in CBC mode with a key size of 256 (FCS_COP.1/Cipher-AES).. The TOE uses its asymmetric key to decrypt the decryption key (FCS_COP.1/Cipher-RSA) prior to perform the firmware image decryption.

265 The TOE's 'Restore' module also allows the verification of the integrity of the installed firmware by comparing its hash (FCS_COP.1/Hash-SHA) with the hash of the previously decrypted and verified distributed image.

266 Table 24 contains the cryptographic functions used by the TOE firmware management tool ('Restore').

Mechanism	Key type	Key size (bits)
Digital Signature	RSA	4096
Decryption	RSA	4096
Hashing	SHA256	256

Table 24: Cryptographic mechanisms implemented by the TOE's 'Restore' module

8. Appendix

8.1. Index of figures

8.2. Index of tables

8.3. References

RFC3164 Lonvick C. The BSD syslog Protocol - Network Working Group. Internet Engineering Task Force (IETF) -; 2021.

RFC5424 Gerhards R. The Syslog Protocol. Internet Engineering Task Force (IETF) - Network Working Group; 2009.

CCPART2 [Anonymous]. Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1 Revision 5. 2017.

RFC5246 Dierks T. The Transport Layer Security (TLS) Protocol Version 1.2. Internet Engineering

Task Force (IETF) - Network Working Group; 2008.

RFC4346 Dierks T. The Transport Layer Security (TLS) Protocol Version 1.1. Internet Engineering Task Force (IETF) - Network Working Group; 2006.

RFC8446 Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. Internet Engineering Task Force (IETF); 2018.

RFC8018 K. Moriarty BKAR. PKCS #5: Password-Based Cryptography Specification. Version 2.1. Internet Engineering Task Force (IETF); 2017.

RFC8017 K. Moriarty BKJJAR. PKCS #1: RSA Cryptography Specifications Version 2.2. Internet Engineering Task Force (IETF); 2016.

SP80056A Elaine Barker RDLCARAV. Recommendation for Pair-Wise KeyEstablishment Schemes Using Discrete Logarithm Cryptography. National Institute of Standards and Technology (NIST); 2018.

FIPS197 National Institute of Standards and Technology ITL(. ADVANCED ENCRYPTION STANDARD (AES). Federal Information Processing Standards Publications (FIPS PUBS); 2001.

SP80038A Dworkin M. Recommendation for Block Cipher Modes of Operation. Methods and Techniques. National Institute of Standards and Technology (NIST); 2001.

SP80038D Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GSM) and GMAC. National Institute of Standars and Technology (NIST); 2007.

SP80038C Dworking M. Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. National Institute of Standards and Technology (NIST); 2007.

RFC7905 A. Langley WCNMJSSJ. ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS). Internet Engineering Task Force (IETF).

FIPS180_4 National Institute of Standards and Technology ITL(. Secure Hash Standard (SHS). Federal Information Processing Standards Publications (FIPS PUBS); 2015.

FIPS198_1 National Institute of Standards and Technology ITL(. The Keyed-Hash Message Authentication Code (HMAC). Federal Information Processing Standards Publications (FIPS PUBS); 2008.

RFC7251 D. McGrew DBMCRD. AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS. Internet Engineering Task Force (IETF); 2014.

RFC5289 Rescorla E. TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM). Internet Engineering Task Force (IETF) - Network Working Group; 2008.

RFC5288 J. Salowey ACDM. AES Galois Counter Mode (GCM) Cipher Suites for TLS. Internet Engineering Task Force (IETF) - Network Working Group; 2008.

RFC6655 D. McGrew DB. AES-CCM Cipher Suites for Transport Layer Security (TLS). Internet Engineering Task Force (IETF); 2012.

CCPART3 [Anonymous]. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, Version 3.1 Revision 5. 2017.

RFC4492 S. Blake-Wilson NBVGCHBM. Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS). Internet Engineering Task Force (IETF); 2006.

FIPS186_4 National Institute of Standards and Technology ITL(. Digital Signature Standard (DSS). Federal Information Processing Standards Publications (FIPS PUBS); 2013.

PST_SPROC Autek. PSTgateways - Secure Use Procedure - Ref: 1227-25. R0.