FSP 3000R7 Operating System

Common Criteria Certification

Security Target

Author:	ADVA Optical Networking SE
	TÜV Informationstechnik GmbH
Category:	CC Certification

Version:	1.9
Date:	2018-12-17
File Name:	FSP_3000_R7_Security_Target.docx
Document Number:	80000046683

Abstract

This document is the ST (Security Target) of the FSP 3000R7 Operating System Common Criteria Certification.

Keywords

CC, ST, Common Criteria, Security Target

Version	Author	Remarks
1.0	Radoslaw Matusiak Kazimierz Miotk Andreas Klar Stephan Slabihoud	First release
1.1	Radoslaw Matusiak Kazimierz Miotk Andreas Klar Stephan Slabihoud	Minor changes
1.2	Radoslaw Matusiak Kazimierz Miotk Andreas Klar Stephan Slabihoud	Final version
1.3	Radoslaw Matusiak Stephan Slabihoud	Changed TOE Objectives (O.TOE_ADMINISTRATION and O.SYSTEM_MONITORING); SNMPv3 Included
1.4	Radoslaw Matusiak Stephan Slabihoud	Minor changes
1.5	Radoslaw Matusiak Stephan Slabihoud	Added FPT_TST_EXT.1.
1.6	Radoslaw Matusiak	Updated documentation
1.7	Bernd Knauer	Updated documentation
1.8	Bernd Knauer	TOE Identification; user data definition harmonized (TOE is OS of NCU II); SNMPv3 only; update to R17.2.1
1.9	Bernd Knauer	Update to R17.2.3

Prepared for

ADVA Optical Networking SE
Headquarters
Campus Martinsried
Fraunhoferstraße 9a
82152 Martinsried/Munich
Germany

Phone: +49 (89) 89 06 65 0

http://www.advaoptical.com

Prepared by

TÜV Informationstechnik GmbH
Member of TÜV NORD Group

Langemarckstraße 20
45141 Essen
Germany

Phone: +49 (201) 8999 – 9

https://www.tuvit.de

Table of Contents

List of Tables

Page

List of Figures

Page

1 ST Introduction

This chapter presents ST and TOE identification information, summarizes the ST in narrative form and provides information for a potential user to determine whether the Scalable Optical Transport Solution FSP 3000 is of interest. A ST contains the security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. A ST principally defines:

a) A security problem expressed as a set of assumptions about the security aspects of the operational environment, a list of threats that the TOE is intended to counter, and any known rules with which the TOE must comply (chapter 3).
b) A set of security objectives and a set of security requirements to address the security problem (chapters 4 and 6).
c) The security functionality provided by the TOE that meets the set of requirements (chapter 7).

1.1 Security Target and TOE references

Table 1.1 – ST Identification

Title:	Scalable Optical Transport Solution FSP 3000R7 Operating System Common Criteria Certification Security Target
Short Title:	FSP 3000R7 Operating System ST
Version:	1.9
Date:	2018-12-17
Author:	ADVA Optical Networking SE
	TÜV Informationstechnik GmbH
CertID:	TBD

Table 1.2 – TOE Identification

TOE Identification:	Scalable Optical Transport Solution FSP 3000 Operating System and its related guidance documentation
TOE Short:	FSP 3000R7 Operating System (CC)
TOE Version:	R7 Rel.17.2.3
TOE Developer:	ADVA Optical Networking SE
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 ([CC])
Evaluation Assurance Level:	EAL2
PP Conformance:	none

1.2 TOE overview

The TOE overview summarizes the usage and major security features of the TOE. The TOE overview provides a context for the TOE evaluation by describing the product and defining the specific evaluated configuration.

The FSP 3000 is a scalable optical transport solution designed to respond to today's exploding bandwidth demands. It can be used by service providers or in an enterprise environment. The modular design of the FSP 3000 ensures that networks are built on a flexible WDM[1] foundation. The FSP 3000 represents Optical and Ethernet provisioning for seamless end-to-end connectivity from the access to the metro and on to long haul.

Figure 1.1 – FSP 3000 family

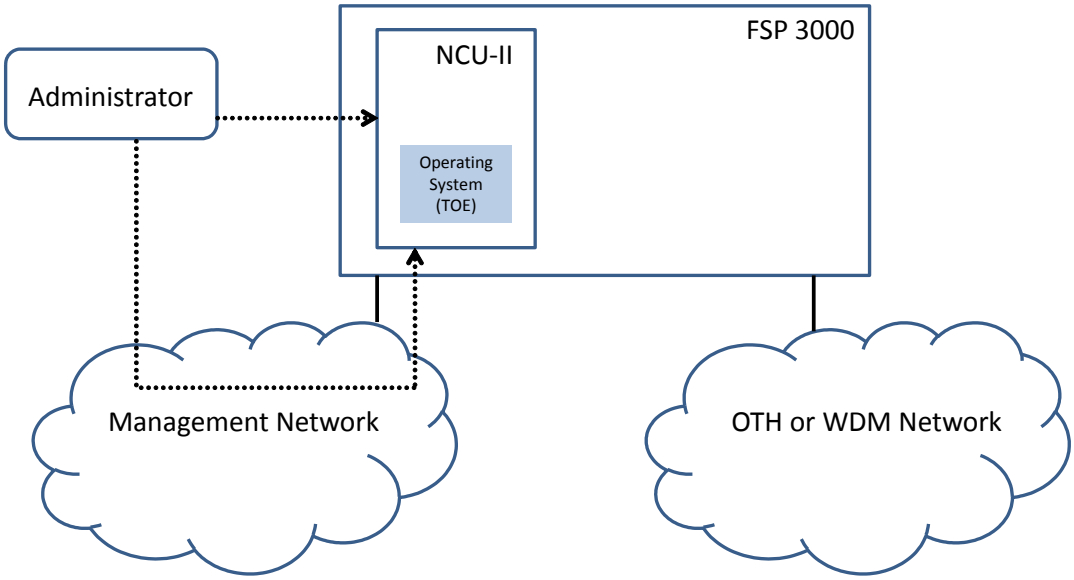
The TOE consists of the operating system of the NCU-II. The hardware (mainboard, casing, interface modules) is not in the scope of the evaluation unless addressed by any assumption relating the operational environment.

A summary of the TOE security functionality can be found in chapter 1.3.3. Further, a more detailed description is provided within the TOE Summary Specification in chapter 7.

All TOE components as well as the intended operational environment of the TOE are illustrated in Figure 1.2. As can be seen within the figure the operational environment also consists of a SDH or WDM network and a management network.

[1] Wavelength Division Multiplexing

Figure 1.2 – TOE Boundary



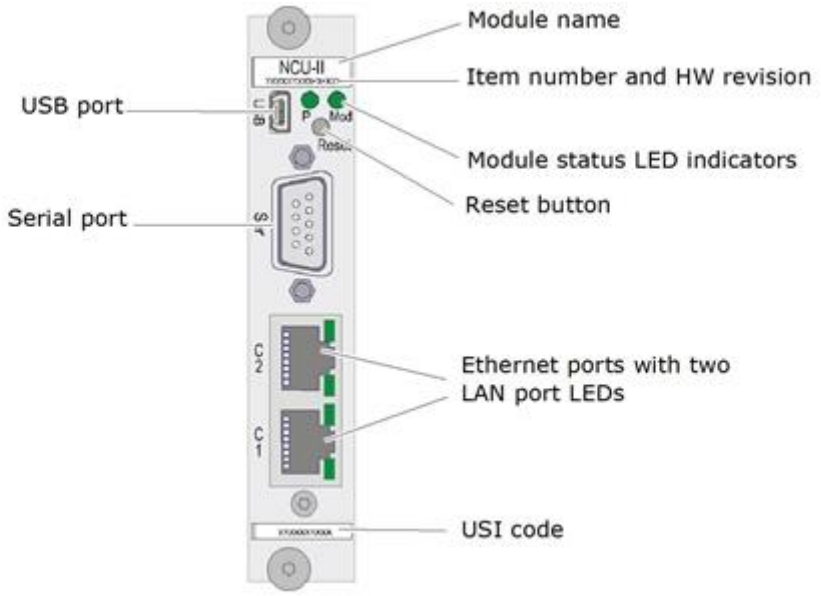
OTH - Optical Transport Hierarchy, WDM - Wavelength-Division

NCU-II – Network control unit II

1.2.1 Brief description of the TOE components

The TOE is the operating system of the FSP 3000R7 system that can be found in the NCU-II card (see Figure 1.3).

Figure 1.3 – NCU-II card



The NCU-II is the second generation network element control (NCU) unit, using a higher performance processor than the first generation (NCU-A, NCU-B, NCU-GDPS and NCU). It provides system management capabilities and network connection to the FSP 3000R7 system. It is a single-slot, 2.5 HU high plug-in module that acts as the hardware interface between the different modules of the system and the equipment connected to the NCU's management interfaces.

The NCU-II extends the functionality of the existing NCU with a higher performance processor, increased and enhanced RAM and a larger Compact Flash. The external connectors of the NCU-II include two RJ45 Ethernet ports, one serial USB and one serial DE9M interface.

The NCU-II can be accessed through a serial, USB or Ethernet port. The NCU-II must be configured for the specific operating environment. Depending on the capabilities of the network element, specific Right to Use (RTU) versions may be required.

The evaluated version of the operating system supports local or remote connections using SSH, HTTPS or SNMPv3 protocol at the Ethernet port of the NCU-II. The connection is encrypted to ensure the confidentiality if the transferred data.

The Ethernet ports labeled C1 and C2 are female 8P8C (RJ-45) receptacles and can be used to connect the NCU-II to a network management system or a management PC, either directly or via an external network, using standard Ethernet crossover cabling.

Serial and USB connections have not been evaluated and are outside the scope of the certified usage.

1.2.2 Brief description of the operational environment of the TOE

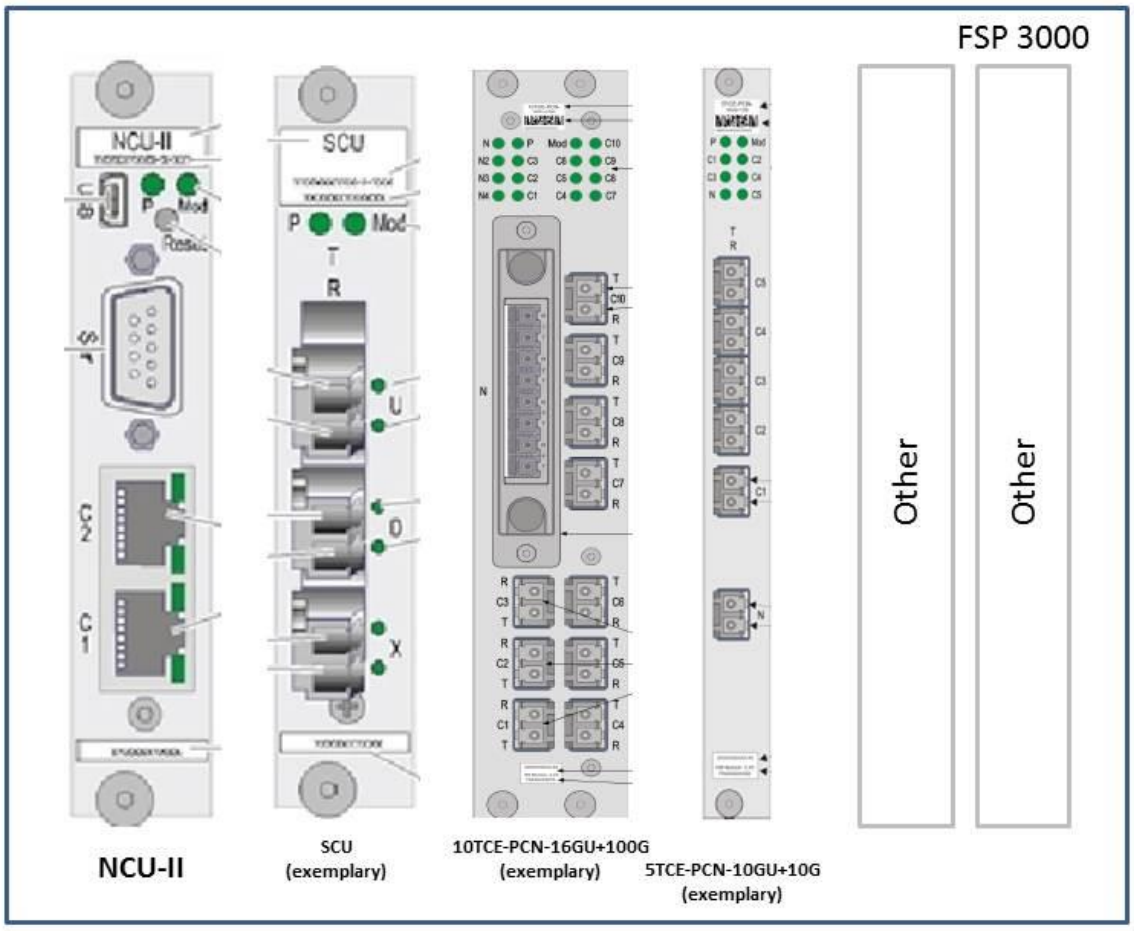
An overview of the TOE and the immediate operational environment is provided in Figure 1.4.

Only one NCU-II is supported per network element. One NCU-II is able to manage a complete network element. The NCU-II must be installed in the master shelf and requires a shelf control unit (SCU, SCU-S, SCU-II) in each (master + any additional) shelf to communicate with the modules.

An NCU communicates with the SCU types in the master shelf using an internal system bus. Exchange of information between the SCU types in the master shelf and the SCU types in the additional shelves takes place over the management fiber ring.

Over the management network an administrative remote connection to the TOE (NCU-II operating system) can be stablished.

Figure 1.4 – NCU-II card in its operational environment



1.3 TOE description

This chapter provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration. The main purpose of this chapter is to bind the TOE in physical and logical terms. The chapter starts with a description of the product type before it introduces the physical scope, the architecture and the logical scope of the TOE.

1.3.1 Product Type

The product Fiber Service Platform (FSP) 3000 is a transport platform for fiber optic applications. Key technologies of the product are Wavelength Division Multiplexing (WDM), optical amplification, wavelength switching, time division multiplexing as well as Ethernet aggregation. The system takes client protocols like Ethernet, SDH, or Fibre Channel and maps them into the ITU-T G.709 transport protocol hierarchy along with an optical conversion from a standard 850nm or 1310nm optical port on the client side of the system to an ITU-T – compliant WDM wavelength on the network side of the system. The system is completely modular. Key elements are:

- 19” – mountable shelf versions
- A central Network Element Controller unit (NCU) which can handle up to 25 shelves via a single IP address
- A shelf controller (SCU)
- Channel Cards for 2.5Gbit/s, 4Gbit/s, 10Gbit/s or 100Gbit/s support all relevant Telco or Datacom protocols.
- Erbium Doped Fiber (EDFA) and Raman amplifiers
- Various types of WDM filters supporting up to 96 different ITU-T compliant wavelengths
- Reconfigurable Optical Add Drop Modules (ROADM)
- Protection switch modules
- Optical supervisory Channel Modules (OSCM)

1.3.2 Physical scope

Figure 1.2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the operational environment of the TOE. The TOE is a software only product and the TOE components are specified in Table 1.3 below:

Table 1.3 – TOE identification and boundary

TOE Component	Description
NCU-II operating system	Part of the NCU-II card is the operating system of the FSP 3000R7 family. The evaluated NCU-II operating system is R7 Rel.17.2.3.

TOE Component	Description
Users' Manual (AGD_OPE)	In addition the following guidance documents are part of the TOE: • FSP3000R7_R17.2_Network_Element_Director_IssA.pdf • FSP3000R7_R17.2_Network_Element_Director_Quick_Start_Guide_IssA.pdf • FSP3000R7_R17.2_Provisioning_and_Operations_Manual_IssA.pdf • FSP3000R7_R17.2_Safety_Guide_IssA.pdf • FSP3000R7_R17.2_System_Description_IssA.pdf • FSP3000R7_R17.2_TL1_Commands_and_Syntax_Guide_IssA.pdf • FSP3000R7_R17.2_TL1_Maintenance_and_Troubleshooting_Manual_IssA.pdf • FSP3000R7_R17.2_TL1_Module_Parameters_Guide_IssA.pdf • FSP 3000R7_R17.2_Network_Hypervisor_User_Guide_IssA.pdf • FSP3000R7_R17.2_Hardware_Description_IssA.pdf • FSP3000R7_R17.2_High-Density_Subshelf_Guide_IssA.pdf • FSP3000R7_R17.2_Installation and Commissioning_Manual_IssA.pdf • FSP3000R7_R17.2_Maintenance_and_Troubleshooting_Manual_IssA.pdf • FSP3000R7_R17.2_Management_Data_Guide_IssA.pdf • FSP3000R7_R17.2_Module_System_Specification_IssA.pdf • FSP 3000R7 R17.2 Secure System Configuration Guide.pdf

The TOE does not have any further hard- or software requirements, since it is provided as a stand-alone solution that does not allow any user modifications except configuration.

1.3.3 Logical scope

The logical boundary of the TOE is divided into the following security classes which are described in detail within the chapters 6 and 7. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Functionality:

- Protected Communication
- System Monitoring
- TOE Administration
- TSF Self Test

1.3.3.1 Protected Communications

To ensure that sensitive data is transmitted to and from the TOE the TOE will provide encryption for these communication paths between themselves and the endpoint. These channels are implemented using following standard protocols:

- HTTPS (TLS), and
- SSH, and
- SNMPv3.

These protocols are specified by RFCs that offer a variety of implementation choices. Requirements have been imposed on some of these choices (particularly those for cryptographic primitives) to provide interoperability and resistance to cryptographic attack.

In addition to providing protection from disclosure (and detection of modification) for the communications, each of the protocols described in this document (SSH, HTTPS and SNMPv3) offer authentication of each endpoint in a cryptographically secure manner, meaning that even if there was a malicious attacker between the two endpoints, any attempt to represent themselves to either endpoint of the communications path as the other communicating party would be detected.

1.3.3.2 System Monitoring

In order to assure that information exists that allows administrators to discover intentional and unintentional issues with the configuration and/or operation of the system, the TOEs have the capability of generating audit data targeted at detecting such activity. Auditing of administrative activities provides information that may hasten corrective action should the system be configured incorrectly. Audit of select system events can provide an indication of failure of critical portions of the TOE (e.g., a cryptographic provider process not running), repeated failures to establish sessions or authenticate to the system) of a suspicious nature.

1.3.3.3 TOE Administration

In order to provide a trusted means for administrators to interact with the TOE, the TOE provides a password-based logon mechanism. The administrator has the capability to compose a strong password. To avoid attacks where an attacker might observe a password being typed by an administrator, passwords must be obscured during logon. Session locking or termination must also be implemented to mitigate the risk of an account being used illegitimately. Passwords must be stored in an obscured form, and there must be no interface provided for specifically reading the password or password file such that the passwords are displayed in plain text.

1.3.3.4 TSF Self Test

In order to detect some number of failures of underlying security mechanisms used by the TSF, the TSF will perform self-tests.

1.4 Conventions

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "_EXT" at the end of the short name.

- Iterations are identified by appending a number in parentheses following the component title. For example, FAU_GEN.1 (1) Audit Data Generation would be the first iteration and FAU_GEN.1 (2) Audit Data Generation would be the second iteration.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. This chapter contains the following sections:

- CC conformance claims
- PP claim
- Package claim
- Conformance rationale

2.1 CC conformance claims

This Security Target claims to be conformant to the Common Criteria 3.1:

- Part 2 extended to [CC]

  In order to provide a complete description of the functional requirements addressed by the TOE, functional components of part 2 of the Common Criteria framework were used. But also additions to the Common Criteria part 2 were defined, to fulfill the requirement of a complete and consistent TOE description.

- Part 3 conformant to [CC]

  For the description of the requirements due to the trustworthiness of the TOE, only security assurance requirements of CC part 3 where used.

2.2 PP claim

This ST does not claim conformance to any PP.

2.3 Package claim

This Security Target claims to be conformant to the Security Assurance Requirements package EAL 2.

2.4 Conformance rationale

This ST does not claim conformance to any PP.

Though the ST does not claim conformance to any PP it borrows several aspects from the [PP-ND] and [CPP-ND].

3 Security Problem Definition

This section describes the security aspects of the operational environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It describes

- the assets that have to be protected by the TOE,
- threats against those assets,
- organizational security policies that TOE shall comply with, and
- assumptions about the operational environment of the TOE.

3.1 Assets

All assets to be protected by the TOE are listed in the table below:

Table 3.1 – Assets

Assets	Description
TOE data	Data for the operation of the TOE upon which the enforcement of the SFR relies. It contains TOE configuration and audit records.
TOE executable code	The TOE firmware.
User data	Data on management plane that is transferred by the TOE (FSP 3000R7 Operating System (CC)) either plain or encrypted.

3.2 Subjects

The following table lists all subjects that interact with the TOE.

Table 3.2 – Subjects

Subject	Description
Attacker / Malicious user	An entity who is attempting to subvert the operation of the TOE. The intention may be to gain unauthorized access to the assets protected by the TOE. They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and has no physical access to the TOE.
(Security) Administrator	An authenticated user who has unrestricted access to the TOE and is able to manage the TOE functionality. Administrators are responsible for the management of all TOE process and have to ensure that the TOE operates in a secure way. Especially only Administrators are allowed to modify the configuration.
IT Entity	An IT entity that sends data to or receives data from the TOE.

3.3 Threats

The table below identifies the threats to the assets against which protection is required by the TOE:

Table 3.3 – Threats

Threat	Description
T.PASSWORD_CRACKING	A malicious user may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_COMPROMISE	A malicious user may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.SECURITY_FUNCTIONALITY_FAILURE	A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	A malicious user may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.UNDETECTED_ACTIVITY	A malicious user may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.UNTRUSTED_COMMUNICATION_CHANNELS	A malicious user may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

Threat	Description
T.WEAK_AUTHENTICATION_ ENDPOINTS	A malicious user may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.

3.4 Organizational security policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE.

Table 3.4 – Organizational security policies

Threat	Description
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

3.5 Assumptions

This section describes the security aspects of the intended operational environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

The assumptions about the TOE's security environment are defined in Table 3.5 below.

Table 3.5 – Assumptions

Assumption	Description
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ST.
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the ST will not include any requirements on physical tamper protection or other physical attack mitigations. The ST will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see chapter 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE‟s operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security objectives for the TOE

TOE security objectives are defined in Table 4.1, below.

Table 4.1 – Security Objectives for the TOE

Objective	Description
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate and store audit data. So compromise credentials and device data enabling continued access to the network device and its critical data, failures during start-up or during operations, unauthorized administrator access to the network device, and access, change, and/or modify the security functionality can be recognized.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE. It ensures that administrators use strong passwords and it also provides protections for logged-in administrators. The TOE will also provide secure protocols to authenticate the endpoints.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

4.2 Security objectives for the operational environment

The security objectives for the TOE operational environment are based on the secure usage assumptions and defined in Table 4.2 below.

Table 4.2 – Security Objectives for the operational environment

Objective	Description
OE.ADMIN_CREDENTIALS_SECURE	The administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

Objective	Description
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.

4.3 Security objectives rationale

Table 4.3 – Security Objectives rationale

Threats and Assumptions vs. Security Objectives	O.DISPLAY_BANNER	O.PROTECTED_COMMUNICATIONS	O.SESSION_LOCK	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	O.TSF_SELF_TEST	OE.ADMIN_CREDENTIALS_SECURE	OE.NO_GENERAL_PURPOSE	OE.NO_THRU_TRAFFIC_PROTECTION	OE.PHYSICAL	OE.TRUSTED_ADMIN
P.ACCESS_BANNER	X										
T.PASSWORD_CRACKING					X						
T.SECURITY_FUNCTIONALITY_COMPROMISE				X	X						
T.SECURITY_FUNCTIONALITY_FAILURE				X		X					
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS			X	X	X						
T.UNDETECTED_ACTIVITY				X							
T.UNTRUSTED_COMMUNICATION_CHANNELS		X									
T.WEAK_AUTHENTICATION_ENDPOINTS					X						
A.ADMIN_CREDENTIALS_SECURE							X				
A.LIMITED_FUNCTIONALITY								X			
A.NO_THRU_TRAFFIC_PROTECTION									X		
A.PHYSICAL_PROTECTION										X	
A.TRUSTED_ADMINISTRATOR											X

P.ACCESS_BANNER is countered by

- **O.DISPLAY_BANNER** since it ensures that the TOE displays an advisory warning before any identification action is performed.

As can be seen above every identified organizational security policy is countered by one or more security objectives as defined in Table 4.1.

T.PASSWORD_CRACKING is countered by

- **O.TOE_ADMINISTRATION** since this TOE security objective provides mechanisms to ensure that administrators do not use weak passwords.

T.SECURITY_FUNCTIONALITY_COMPROMISE is countered by

- **O.TOE_ADMINISTRATION** since this TOE security objective provides mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
- **O.SYSTEM_MONITORING** since it ensures that the TOE provides the capability to generate audit data of administrative actions.

T.SECURITY_FUNCTIONALITY_FAILURE is countered by

- **O.SYSTEM_MONITORING** since it ensures that the TOE provides the capability to generate audit data of TSF failures.
- **O.TSF_SELF_TEST** since it ensures that the TOE provides the capability to test some subset of its security functionality to ensure it is operating properly

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS is countered by

- **O.SESSION_LOCK** since this TOE security objective provides mechanisms that mitigate the risk of unattended sessions being hijacked.
- **O.SYSTEM_MONITORING** since it ensures that the TOE provides the capability to generate audit data of administrative actions like logon trials.
- **O.TOE_ADMINISTRATION** since this TOE security objective provides mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.

T.UNDETECTED_ACTIVITY is countered by

- **O.SYSTEM_MONITORING** since it ensures that the TOE provides the capability to generate audit data of administrative actions.

T.UNTRUSTED_COMMUNICATION_CHANNELS is countered by

- **O.PROTECTED_COMMUNICATIONS** since this TOE security objective provides protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

T.WEAK_AUTHENTICATION_ENDPOINTS is countered by

- **O.TOE_ADMINISTRATION** since this TOE security objective provides mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.

As can be seen above every identified threat is countered by one or more security objectives as defined in Table 4.1.

A.NO_GENERAL_PURPOSE is addressed by

- **OE.NO_GENERAL_PURPOSE**, since it ensures that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

A.PHYSICAL is addressed by

- **OE.PHYSICAL**, since it ensures physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

A.TRUSTED_ADMIN is addressed by

- **OE.TRUSTED_ADMIN**, since it ensures that TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

A.ADMIN_CREDENTIALS_SECURE is addressed by

- **OE.ADMIN_CREDENTIALS_SECURE**, since it ensures that TOE Administrators' credentials (private key) used to access TOE must be protected on any other platform on which they reside.

A.NO_THRU_TRAFFIC_PROTECTION is addressed by

- **OE.NO_THRU_TRAFFIC_PROTECTION**, since it ensures TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

Every assumption is addressed by one objectives for the operational environment. The justification above demonstrates that the defined security objectives for the operational environment uphold all defined assumptions.

5 Extended Components Definition

This chapter defines TOE security functional requirements and assurance requirements which are not part of CC 3.1 part 2 or part 3.

The assurance requirements that have been defined by the Common Criteria v3.1 part 3 are applicable to the extended components.

Because this component is a software component with a well-defined behavior on its external interfaces, the assurance requirements that have been defined in part 3 of Common Criteria are applicable to this functional family.

Through its nature as a software component the assurance classes ADV, AGD, ALC, ATE and AVA are applicable in the evaluation process. It is not required to define a new assurance class or assurance family for a consistent and complete description to cover this SFR. This SFR does not define any behavior that might require an extension of part 3 of the Common Criteria Evaluation Framework.

5.1 Extended TOE Security Functional Components

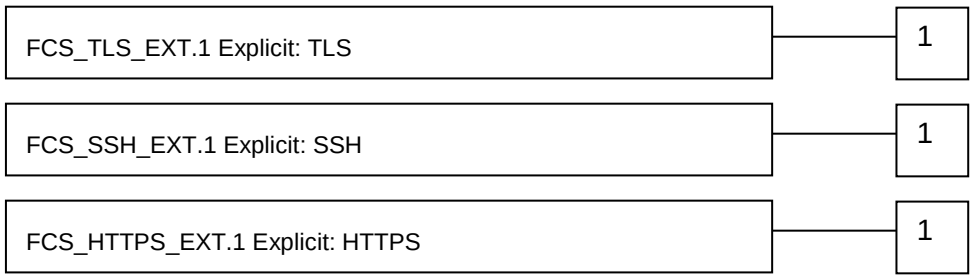
This section specifies the extended SFRs for the TOE.

5.1.1 Class FCS: Cryptographic support

The existing FCS functionality class was extended because part II of [CC] does not contain any SFR, which defines following functionality:

- defining the explicit usage of the TLS protocol,
- defining the explicit usage of the SSH protocol,
- defining the explicit usage of the HTTPS protocol.

Figure 5.1 – Cryptographic support class decomposition

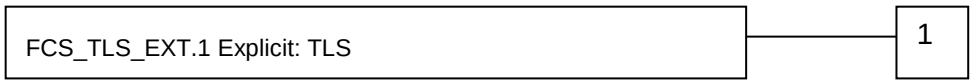


5.1.1.1 Explicit: TLS (FCS_TLS_EXT)

Family Behavior

This family defines the requirements for explicit TLS usage.

Component leveling



FCS_TLS_EXT.1 Explicit: TLS, defines the usage of an explicit TLS protocol.

Management: FCS_TLS_EXT.1

There are no management activities foreseen.

Audit: FCS_TLS_EXT.1

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

a) Minimal: Failure to establish a TLS Session.
b) Minimal: Establishment/Termination of a TLS session.

FCS_TLS_EXT.1 Explicit: TLS

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation,
FCS_CKM.4 Cryptographic key destruction

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA *as defined in RFC 3268*

TLS_RSA_WITH_AES_256_CBC_SHA *as defined in RFC 3268*

Optional Ciphersuites:

[selection:

None

TLS_DHE_RSA_WITH_AES_128_CBC_SHA (TLSv1.2) *as defined in RFC 5246*

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (TLSv1.2) *as defined in RFC 5246*

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (TLSv1.2) *as defined in RFC 5288*

TLS_DHE_RSA_WITH_AES_256_CBC_SHA (TLSv1.2) *as defined in RFC 5246*

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (TLSv1.2) *as defined in RFC 5246*

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (TLSv1.2) *as defined in RFC 5288*

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (TLSv1.2) *as defined in RFC 4492*

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (TLSv1.2) *as defined in RFC 5289*

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (TLSv1.2) *as defined in RFC 5289*
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (TLSv1.2) *as defined in RFC 4492*
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (TLSv1.2) *as defined in RFC 5289*
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (TLSv1.2) *as defined in RFC 5289*
TLS_RSA_WITH_AES_128_GCM_SHA256 (TLSv1.2) *as defined in RFC 5288*
TLS_RSA_WITH_AES_256_CBC_SHA (TLSv1.2) *as defined in RFC 5246*
TLS_RSA_WITH_AES_256_CBC_SHA256 (TLSv1.2) *as defined in RFC 5246*
TLS_RSA_WITH_AES_256_GCM_SHA384 (TLSv1.2) *as defined in RFC 5288*
].

5.1.1.2 Explicit: SSH (FCS_SSH_EXT)

Family Behavior

This family defines the requirements for explicit SSH usage.

Component leveling

FCS_SSH_EXT.1 Explicit: SSH, defines the usage of an explicit SSH protocol.

Management: FCS_SSH_EXT.1

There are no management activities foreseen.

Audit: FCS_SSH_EXT.1

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

a) Minimal: Failure to establish a SSH Session.
b) Minimal: Establishment/Termination of a SSH session.

FCS_SSH_EXT.1 Explicit: SSH

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation,
FCS_CKM.4 Cryptographic key destruction

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254, and [selection: 5656, 6668, no other RFCs].

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [assignment: number of bytes] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4	The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CTR-128, AES-CTR-192, AES-CTR-256, [selection: AEAD_AES_128_GCM, AEAD_AES_256_GCM, no other algorithms].
FCS_SSH_EXT.1.5	The TSF shall ensure that the SSH transport implementation uses [selection: SSH_RSA, ecdsa-sha2-nistp256] and [selection: PGP-SIGN-RSA, PGP-SIGN-DSS, ecdsa-sha2-nistp384, no other public key algorithms,] as its public key algorithm(s)
FCS_SSH_EXT.1.6	The TSF shall ensure that data integrity algorithms used in SSH transport connection is [selection: hmac-sha1, hmac-sha2-256, hmac-sha2-512, hmac-ripmed-160].
FCS_SSH_EXT.1.7	The TSF shall ensure that diffie-hellman-group14-sha1 and [selection: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha1, diffie-hellman-group-exchange-sha256, no other methods] is are the only allowed key exchange methods used for the SSH protocol.

Application Note:

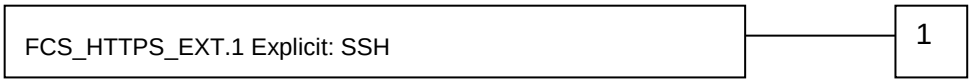
- ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521 (RFC 5656)
- diffie-hellman-group14-sha1 (RFC 4253)
- diffie-hellman-group-exchange-sha1, diffie-hellman-group-exchange-sha256 (RFC 4419)

5.1.1.3 Explicit: HTTPS (FCS_HTTPS_EXT)

Family Behavior

This family defines the requirements for explicit HTTPS usage.

Component leveling



FCS_HTTPS_EXT.1 Explicit: HTTPS, defines the usage of an explicit HTTPS protocol.

Management: FCS_HTTPS_EXT.1

There are no management activities foreseen.

Audit: FCS_HTTPS_EXT.1

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

a) Minimal: Failure to establish a HTTPS Session.
b) Minimal: Establishment/Termination of a HTTPS session.

FCS_HTTPS_EXT.1 Explicit: HTTPS

Hierarchical to: No other components

Dependencies: FCS_TLS_EXT.1 Explicit: TLS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

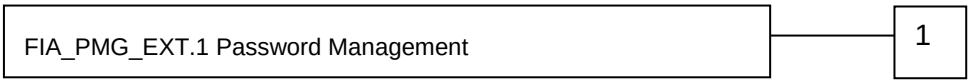
FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

5.1.2 Class FIA: Identification and authentication

The existing FIA functionality class was extended because part II of [CC] does not contain any SFR which defines following functionality:

- defining the complexity of password mechanism.

Figure 5.2 – FIA: Identification and authentication class decomposition

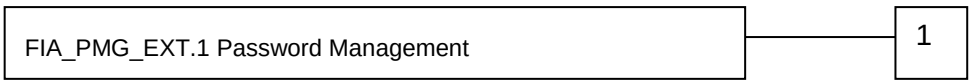


5.1.2.1 Password Management (FIA_PMG_EXT)

Family Behavior

This family defines the requirements for password management.

Component leveling



FIA_PMG_EXT.1 Password Management, defines the password management capabilities for administrative passwords.

Management: FIA_PMG_EXT.1

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

a) Configuration of the password complexity.

Audit: FIA_PMG_EXT.1

There are no auditable events foreseen.

FIA_PMG_EXT.1 Password Management

Hierarchical to: No other components

Dependencies: No dependencies

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

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “(“, “)”, [assignment: other characters]];

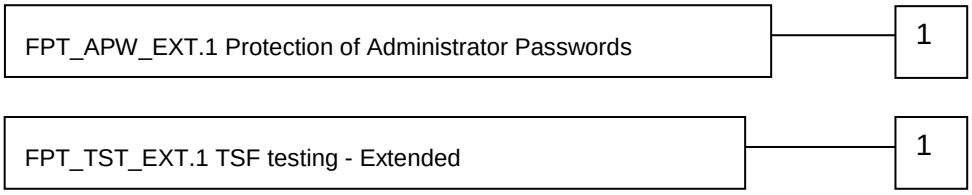
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater.

5.1.3 Class FPT: Protection of the TSF

The existing FPT functionality class was extended because part II of [CC] does not contain any SFR, which defines following functionality:

- protection of administrator passwords,
- testing of TOE security functionality.

Figure 5.3 – FPT: Protection of the TSF class decomposition

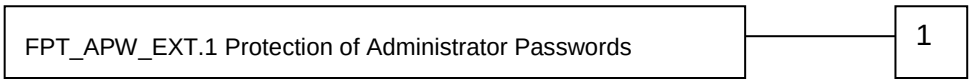


5.1.3.1 Protection of Administrator Passwords (FPT_APW_EXT)

Family Behavior

This family defines the requirements for the protection of administrator passwords.

Component leveling



FPT_APW_EXT.1 Protection of Administrator Passwords, defines how the TSF shall store passwords.

Management: FPT_APW_EXT.1

There are no management activities foreseen.

Audit: FPT_APW_EXT.1

There are no auditable events foreseen.

FPT_APW_EXT.1 Protection of Administrator Passwords

Hierachical to: No other components

Dependencies: No dependencies

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

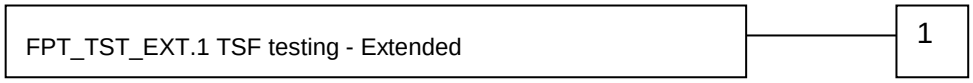
FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

5.1.3.2 TSF testing – Extended (FPT_TST_EXT)

Family Behavior

This family defines the requirements for the testing TOE security functionality.

Component leveling



FPT_TST_EXT.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].

Management: FPT_TST_EXT.1

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

a) management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions;
b) management of the time interval if appropriate.

Audit: FPT_TST_EXT.1

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

a) Basic: Execution of the TSF self tests and the results of the tests.

Application Note:

The TOE does not provide authorized users with the capability to verify the integrity of the TSF data or the TSF itself. Checking the integrity of the firmware (TSF data) is done explained in the guidance manual.

The TOE itself checks essential supporting functionality (File system and Database) that is required for a flawless operation of the TSF on demand of an authorized user via the management software.

5.2 Extended TOE Security Assurance Components

There are no extended TOE Security Assurance Components.

6 Security Requirements

This chapter defines the IT security requirements that shall be satisfied by the TOE or its operational environment:

Common Criteria divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g. configuration management, testing, and vulnerability assessment).

These requirements are discussed separately within the following subchapters.

6.1 Security functional requirements

The specified functional requirements are compliant with Common Criteria v3.1 part 2 and are corresponding with the given functional components.

Table 6.1 – TOE Security Functional Requirements

Name	Description
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User identity association
FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1(1)	Cryptographic Operation (for data encryption/decryption)
FCS_COP.1(2)	Cryptographic Operation (for cryptographic signature)
FCS_COP.1(3)	Cryptographic Operation (for cryptographic hashing)
FCS_COP.1(4)	Cryptographic Operation (for keyed-hash message authentication)
FCS_TLS_EXT.1	Explicit: TLS
FCS_SSH_EXT.1	Explicit: SSH
FCS_HTTPS_EXT.1	Explicit: HTTPS
FIA_PMG_EXT.1	Password Management
FIA_UID.1	Timing of identification
FIA_UAU.2	User authentication before any action
FIA_UAU.7	Protected Authentication Feedback
FMT_MTD.1	Management of TSF Data (for general TSF data)
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Restrictions on Security Roles
FPT_APW_EXT.1	Protection of Administrator Passwords
FPT_STM.1	Reliable Time Stamps

Name	Description
FPT_TST_EXT.1	TSF Testing - Extended
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_TAB.1	Default TOE Access Banners
FTP_TRP.1	Trusted Path

6.1.1 Class FAU – Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shut-down of the audit functions;

b) All auditable events, for the [not specified] level of audit; and

c) [*All administrative actions comprising:*

- *Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).*
- *Security related configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *Resetting passwords (name of related user account shall be logged).*

d) *Specifically defined auditable events listed in Table 6.2].*

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; a

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [*information specified in column three of Table 6.2*].

Application note:

A shutdown information is never logged since the TOE is not intended to be shut down.

Table 6.2 – Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FCS_CKM.1	None.	
FCS_CKM.4	None.	None.
FCS_COP.1(1)	None.	None.
FCS_COP.1(2)	None.	None.
FCS_COP.1(3)	None.	None.
FCS_COP.1(4)	None.	None.
FCS_TLS_EXT.1	Failure to establish a TLS Session.	Reason for failure.
FCS_SSH_EXT.1	Failure to establish a SSH Session.	Reason for failure.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.
FIA_PMG_EXT.1	None.	None.
FIA_UID.1	All use of the user identification mechanism, including the user identity provided.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FMT_MTD.1	None.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TST_EXT.1	None.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.

FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

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.

6.1.2 Class FCS – Cryptographic Support

FCS_CKM.1 Cryptographic Key Generation (for asymmetric keys)

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation,

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic **asymmetric** keys in accordance with a specified cryptographic key generation algorithm [*as defined in Table 6.3*] and specified cryptographic key sizes [*as defined in Table 6.3*] that meet the following: [*standards as defined in Table 6.3*].

Table 6.3 – Cryptographic key generation algorithm

Usage	Cryptographic key generation algorithm	key size	standards
SSH	DH ECDH	key strength of at least 2048 bits	FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1 ECC schemes using “NIST curves” [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4

Usage	Cryptographic key generation algorithm	key size	standards
HTTPS	DH ECDH RSA	key strength of at least 2048 bits	FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1 ECC schemes using “NIST curves” [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4 RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3
TLS	DH ECDH RSA	key strength of at least 2048 bits	FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1 ECC schemes using “NIST curves” [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4 RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroize*] that meets the following: [*none*].

Application Note:

The TSF shall zeroize all plaintext secret and private cryptographic keys when the keys are no longer required.

FCS_COP.1(1) Cryptographic Operation (for data encryption/decryption)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation,

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(1) The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES operating in CBC, GCM, [CTR]*] and cryptographic key sizes [*128 bits, 192 bits, 256 bits*], that meets the following: [*FIPS PUB 197, "Advanced Encryption Standard (AES)", NIST SP 800-38A, NIST SP 800-38D*].

FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation,

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(2) The TSF shall perform [*cryptographic signature services as defined in Table 6.4*] in accordance with a specified cryptographic algorithm [*as defined in Table 6.4*] and cryptographic key sizes [*as defined in Table 6.4*] that meets the following: [*as defined in Table 6.4*].

Table 6.4 – Cryptographic signature services

cryptographic signature	key size	standards
RSA Digital Signature Algorithm	key size (modulus) of 2048 bits or greater	FIPS PUB 186-4, "Digital Signature Standard"

Application Note:

RSA is used for signing the self-signed X.509 certificates used for the web interface. The TOE also uses RSA-based key-exchange algorithms for HTTPS (e.g. DHE-RSA-AES256-SHA). SSH uses the RSA server key for authentication by signing the hash of a public key.

FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation,

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(3) The TSF shall perform [*cryptographic hashing services as defined in Table 6.5*] in accordance with a specified cryptographic algorithm [*as defined in Table 6.5*] and message **hash** sizes [*as defined in Table 6.5*] that meet the following: [*as defined in Table 6.5]*

Table 6.5 – Cryptographic hashing services

operations	hash algorithms	standards
HTTPS	SHA-1, SHA-256, SHA-384	FIPS PUB 180-4
	AES-GCM	supported additionally
SSH	HMAC SHA-1, HMAC SHA-256, HMAC SHA-512	FIPS PUB 180-4
	HMAC RIPMED-160	supported additionally
SNMPv3	HMAC-MD5-96	RFC 1321 (MD5), RFC 2104 (HMAC)

Application Note:

The TOE also supports AES-GCM, HMAC RIPMED-160 and SHA-1-96, which are not part of FIPS PUB 180-3.

FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation,
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(4) The TSF shall perform [*keyed-hash message authentication as defined in Table 6.6*] in accordance with a specified cryptographic algorithm [*as defined in Table 6.6*] and message **hash** sizes [*as defined in Table 6.6*] that meet the following: [*as defined in Table 6.6]*

Table 6.6 – Keyed-hash message authentication

operations	hash algorithms / hash sizes	standards
keyed-hash message authentication	HMAC SHA-1, HMAC SHA-256, HMAC SHA-512	FIPS PUB 180-4
	HMAC RIPMED-160	supported additionally

FCS_TLS_EXT.1 Explicit: TLS

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation,
FCS_CKM.4 Cryptographic key destruction

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA *as defined in RFC 3268*

TLS_RSA_WITH_AES_256_CBC_SHA *as defined in RFC 3268*

Optional Ciphersuites:

[

TLS_DHE_RSA_WITH_AES_128_CBC_SHA (TLSv1.2) *as defined in RFC 5246*
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (TLSv1.2) *as defined in RFC 5246*
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (TLSv1.2) *as defined in RFC 5288*
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (TLSv1.2) *as defined in RFC 5246*
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (TLSv1.2) *as defined in RFC 5246*
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (TLSv1.2) *as defined in RFC 5288*
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (TLSv1.2) *as defined in RFC 4492*
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (TLSv1.2) *as defined in RFC 5289*
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (TLSv1.2) *as defined in RFC 5289*
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (TLSv1.2) *as defined in RFC 4492*
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (TLSv1.2) *as defined in RFC 5289*
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (TLSv1.2) *as defined in RFC 5289*
TLS_RSA_WITH_AES_128_GCM_SHA256 (TLSv1.2) *as defined in RFC 5288*
TLS_RSA_WITH_AES_256_CBC_SHA (TLSv1.2) *as defined in RFC 5246*
TLS_RSA_WITH_AES_256_CBC_SHA256 (TLSv1.2) *as defined in RFC 5246*
TLS_RSA_WITH_AES_256_GCM_SHA384 (TLSv1.2) *as defined in RFC 5288*

].

Application Note:

TLS_RSA_WITH_AES_128_CBC_SHA is required in order to ensure compliance with RFC 5246. These requirements will be revisited as new TLS versions are standardized by the IETF.

FCS_SSH_EXT.1 Explicit: SSH

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation,
FCS_CKM.4 Cryptographic key destruction

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254, and [no other RFCs].

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*32768*] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CTR-128, AES-CTR-192, AES-CTR-256, [no other algorithms].

FCS_SSH_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses [SSH_RSA] and [no other public key algorithms,] as its public key algorithm(s)

FCS_SSH_EXT.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [hmac-sha1, hmac-sha2-256, hmac-sha2-512, hmac-ripmed-160].

FCS_SSH_EXT.1.7 The TSF shall ensure that diffie-hellman-group14-sha1 and [ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha1, diffie-hellman-group-exchange-sha256] are the only allowed key exchange methods used for the SSH protocol.

Application Note:

- ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521 (RFC 5656)
- diffie-hellman-group14-sha1 (RFC 4253)
- diffie-hellman-group-exchange-sha1, diffie-hellman-group-exchange-sha256 (RFC 4419)

FCS_HTTPS_EXT.1 Explicit: HTTPS

Hierarchical to: No other components

Dependencies: FCS_TLS_EXT.1 Explicit: TLS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

6.1.3 Class FIA – Identification and authentication

FIA_PMG_EXT.1 Password Management

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “(“, “)”, [“.”, “[“, “]”, “_”, “-“, “+”, “|”, “~”, “{“, “}”]];

2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater.

Application Note:

"Administrative passwords" refers to passwords used by administrators at the local console, over protocols that support passwords, such as SSH, HTTPS and SNMPv3.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [

- *Display the warning banner in accordance with FTA_TAB.1*

] on behalf of the user to be performed before the user is identified.

FIA_UID_1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note:

The TSF shall display warning banner before the user is identified and then authenticated by FIA_UAU.2.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each **Security Administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **Security Administrator**.

Application Note:

The TSF shall provide a local password-based authentication mechanism to perform administrative user authentication.

FIA_UAU.7 Protected Authentication Feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*obscured feedback*] to the user while the authentication is in progress **at the local console**.

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 Class FMT – Security Management

FMT_MTD.1 Management of TSF Data (for general TSF data)

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to [*manage*] the [*the stored account information*] to [*the Security Administrators*].

Application Note:

The word “manage” includes but is not limited to create, initialize, view, change default, modify, delete, clear, and append. This SFR includes also the resetting of user passwords by the Security Administrator.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies

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

[

to administer the TOE locally and remotely and has the

- *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UID.1 and FIA_UAU.2;*
- *Ability to configure the cryptographic functionality;*

].

FMT_SMR.2 Restrictions on Security Roles

Hierarchical to: FMT_SMR.1 Security roles.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.2.1 The TSF shall maintain the roles: [*Security 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 [

- *Security Administrator role shall be able to administer the TOE locally;*
- *Security Administrator role shall be able to administer the TOE remotely;*

] are satisfied.

Application Note:

The Security Administrator can administer the TOE through the local console and through a remote mechanism (SSH, HTTPS/TLS, SNMPv3).

6.1.5 Class FPT – Protection of the TSF

FPT_APW_EXT.1 Protection of Administrator Passwords

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

Application Note:

The intent of the requirement is that raw password authentication data are not stored in the clear, and that no user or administrator is able to read the plaintext password through “normal” interfaces. An all-powerful administrator of course could directly read memory to capture a password but is trusted not to do so.

FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application Note:

The TSF does not provide reliable information about the current time at the TOE’s location by itself, but depends on external time and date information provided manually by the administrator. The term ‘reliable time stamps’ refers to the strict use of the time and date information, that is provided externally, and the logging of all changes to the time settings including information about the old and new time. With this information the real time for all audit data can be calculated.

FPT_TST_EXT.1 TSF Testing - Extended

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [during normal operation] to demonstrate the correct operation of the TSF: [

- *Testing the file system,*
- *Testing the database*

].

Application Note:

The TOE does not provide authorized users with the capability to verify the integrity of the TSF data or the TSF itself. Checking the integrity of the firmware (TSF data) is done as explained in the guidance manual.

The TOE itself checks essential supporting functionality (File system and Database) that is required for a flawless operation of the TSF on demand of an authorized user via the management software.

6.1.6 Class FTA – TOE Access

FTA_SSL.3 TSF-initiated Termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate **a local or remote** interactive session after a [*Security Administrator-configurable time interval of session inactivity*].

Note, since SNMPv3 administration is session-less, this requirement does not apply to that user type.

FTA_SSL.4 User-initiated Termination

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FTA_TAB.1 Default TOE Access Banners

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAB.1.1 Before establishing **a Security Administrator's** session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

Application Note:

This requirement is intended to apply to interactive sessions between a human user and a TOE. IT entities establishing connections or programmatic connections (e.g., remote procedure calls over a network) are not required to be covered by this requirement.

6.1.7 Class FTP – Trusted Path/Channels

FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1	The TSF shall **be capable of using [*SSH, TLS, HTTPS*] to** provide a communication path between itself and **authorized** [remote] **Security Administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [disclosure, [*and provides detection of modification of the channel data*]].
FTP_TRP.1.2	The TSF shall permit [remote **Security Administrators**] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [initial **Security Administrator** authentication, [*and all remote administration actions*]].

Application Note:

This requirement ensures that authorized remote administrators initiate all communication with the TOE via a trusted path, and that all communication with the TOE by remote administrators is performed over this path. The data passed in this trusted communication channel are encrypted as defined by the protocol chosen in the first selection.

6.2 Security assurance requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2). They are all drawn from Part 3 of the Common Criteria. The assurance components are listed in Table 6.7.

Table 6.7 – EAL Security Assurance Requirements

Assurance component	Name
ADV_ARC.1	Security architecture description
ADV_FSP.2	Security-enforcing functional specification

Assurance component	Name
ADV_TDS.1	Basic design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.2	Use of a CM system
ALC_CMS.2	Parts of the TOE CM coverage
ALC_DEL.1	Delivery procedures
ASE_CCL.1	Conformance claims
ASE_ECD.1	Extended components definition
ASE_INT.1	ST introduction
ASE_OBJ.2	Security objectives
ASE_REQ.2	Derived security requirements
ASE_SPD.1	Security problem definition
ASE_TSS.1	TOE summary specification
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.2	Vulnerability analysis

6.3 Security requirement rationale

6.3.1 Rational for the security functional requirements

Table 6.8 – Fulfillment of Security Objectives

Security Objectives vs. Security Requirements	O.DISPLAY_BANNER	O.PROTECTED_COMMUNICATIONS	O.SESSION_LOCK	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	O.TSF_SELF_TEST
FAU_GEN.1				X		
FAU_GEN.2				X		

Security Objectives vs. Security Requirements	**O.DISPLAY_BANNER**	**O.PROTECTED_COMMUNICATIONS**	**O.SESSION_LOCK**	**O.SYSTEM_MONITORING**	**O.TOE_ADMINISTRATION**	**O.TSF_SELF_TEST**
FCS_CKM.1		X				
FCS_CKM.4		X				
FCS_COP.1(1)		X				
FCS_COP.1(2)		X				
FCS_COP.1(3)		X				
FCS_COP.1(4)		X				
FCS_TLS_EXT.1		X				
FCS_SSH_EXT.1		X				
FCS_HTTPS_EXT.1		X				
FIA_PMG_EXT.1					X	
FIA_UID.1	X				X	
FIA_UAU.2					X	
FIA_UAU.7					X	
FMT_MTD.1					X	
FMT_SMF.1					X	
FMT_SMR.2					X	
FPT_APW_EXT.1					X	
FPT_STM.1				X		
FPT_TST_EXT.1						X
FTA_SSL.3			X			
FTA_SSL.4			X			
FTA_TAB.1	X					
FTP_TRP.1		X				

O.DISPLAY_BANNER covered by following requirements:

- FIA_UID.1
  Display the warning banner in accordance with FTA_TAB.1 before the user is identified.
- FTA_TAB.1
  Displays a Security Administrator-specified advisory notice and consent warning.

O.PROTECTED_COMMUNICATIONS covered by following requirements:

- FCS_CKM.1
  Key generation for protected communications acc. FTP_TRP.1
- FCS_CKM.4
  Key destruction for protected communications acc. FTP_TRP.1
- FCS_COP.1(1)
  Cryptographic Operations for protected communications acc. FTP_TRP.1
- FCS_COP.1(2)
  Cryptographic Operations for protected communications acc. FTP_TRP.1
- FCS_COP.1(3)
  Cryptographic Operations for protected communications acc. FTP_TRP.1
- FCS_COP.1(4) - Cryptographic Operations for protected communications acc. FTP_TRP.1
- FCS_TLS_EXT.1 - for protected communications using TLS.
- FCS_SSH_EXT.1 - for protected communications using SSH.
- FCS_HTTPS_EXT.1 - for protected communications using HTTPS.
- FTP_TRP.1
  Trusted communication path between itself and remote administrators.

O.SESSION_LOCK covered by following requirements:

- FTA_SSL.3
  Ensures that a local or remote interactive session is terminated after a specified period of time.
- FTA_SSL.4
  Ensures that a user can terminate his own session.

O.SYSTEM_MONITORING covered by following requirements:

- FAU_GEN.1
  Generates audit records for certain auditable events.
- FAU_GEN.2
  Audit events resulting from actions of identified users, the TSF associates each auditable event with the identity of the user.

- FPT_STM.1
  The TOE provides reliable time stamps for its own use

O.TOE_ADMINISTRATION covered by following requirements:

- FIA_PMG_EXT.1
  Provides password management capabilities and ensures password complexity.
- FIA_UID.1
  Initiate the identification process and requires each administrative user to be successfully identified.
- FIA_UAU.2
  Provides a local password-based authentication mechanism in order to authenticate an administrator.
- FIA_UAU.7
  Provide only obscured feedback to the administrative user while the authentication is in progress.
- FMT_MTD.1
  Restrict the ability to manage the configuration to the Security Administrators.
- FMT_SMF.1
  Performing certain security management functions.
- FMT_SMR.2
  Maintain the role Authorized Administrator.
- FPT_APW_EXT.1
  Ensures the protection of administrator passwords.

O.TSF_SELF_TEST covered by following requirements:

- FPT_TST_EXT.1
  Ensures that a suite of self-tests is run during normal operation to demonstrate the correct operation of the TSF.

6.3.2 Dependencies of security functional requirements

Table 6.9 – Dependencies of security requirements

Requirement	Dependency	Fulfilled
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FIA_UID.1 FAU_GEN.1	Yes Yes
FCS_CKM.1	FCS_COP.1 FCS_CKM.4	Yes Yes
FCS_CKM.4	FCS_CKM.1	Yes

Requirement	Dependency	Fulfilled
FCS_COP.1(1)	FCS_CKM.1 FCS_CKM.4	Yes Yes
FCS_COP.1(2)	FCS_CKM.1 FCS_CKM.4	Yes Yes
FCS_COP.1(3)	FCS_CKM.1 FCS_CKM.4	Yes Yes
FCS_COP.1(4)	FCS_CKM.1 FCS_CKM.4	Yes Yes
FCS_TLS_EXT.1	FCS_CKM.1 FCS_CKM.4	Yes Yes
FCS_SSH_EXT.1	FCS_CKM.1 FCS_CKM.4	Yes Yes
FCS_HTTPS_EXT.1	FCS_CKM.1 FCS_CKM.4	Yes Yes
FIA_PMG_EXT.1	No dependencies	n/a
FIA_UID.1	No dependencies	n/a
FIA_UAU.2	FIA_UID.1	Yes
FIA_UAU.7	FIA_UAU.1	Yes, by FIA_UAU.2 (hierarchical to FIA_UAU.1)
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Yes Yes, by FMT_SMR.2 (hierarchical to FMT_SMR.1)
FMT_SMF.1	No dependencies	n/a
FMT_SMR.2	FIA_UID.1	Yes
FPT_APW_EXT.1	No dependencies	n/a
FPT_STM.1	No dependencies	n/a
FPT_TST_EXT.1	No dependencies	n/a
FTA_SSL.3	No dependencies	n/a
FTA_SSL.4	No dependencies	n/a
FTA_TAB.1	No dependencies	n/a
FTP_TRP.1	No dependencies	n/a

6.3.3 Rational for the assurance requirements

EAL2 was selected because it is the first time this particular TOE is going to be evaluated. Therefore and in order to keep evaluation efforts reasonable a basic level of independently assured security is required for the TOE.

EAL2 provides assurance by an analysis of the security functions, using a security-enforcing functional specification, guidance documentation, the basic design of the TOE to understand the

security behavior. AVA_VAN.2 provides resistance against attackers with basic attack potential and ensures that the evidence shows that vulnerabilities have been analyzed. The analysis is supported by independent sample testing of the TOE security functions, evidence of developer testing based on the security-enforcing functional specification and basic design, selective independent confirmation of the developer test results, and a vulnerability analysis demonstrating resistance to penetration attackers with a basic attack potential.

7 TOE summary specification

This chapter presents an overview of the security functionality implemented by the TOE.

7.1 Protected Communications

Sensitive data to and from the TOE is transmitted encrypted. The TOE provides encryption for the communication paths between itself and the endpoint using standard protocols:

- HTTPS (with TLS encryption), and **(FCS_HTTPS_EXT.1, FCS_TLS_EXT.1)**
- SSH **(FCS_SSH_EXT.1)**
- SNMPv3 (**FCS_COP.1(1)**).

All protocols (SSH, HTTPS/TLS, SNMPv3) are specified by RFCs. The requirements have been imposed on some specifications for cryptographic primitives to provide interoperability and resistance to cryptographic attack. **(FCS_CKM.1)** This comprises cryptographic operations used for encryption and decryption **(FCS_COP.1(1))**, for cryptographic signatures **(FCS_COP.1(2))**, for hashing **(FCS_COP.1(3))** and for keyed-hash message authentication **(FCS_COP.1(4))**.

Cryptographic keys are destroyed when the keys are no longer required. **(FCS_CKM.4)**

When the administrator uses a remote connection to administrate the TOE, a trusted channel is established. Over this channel the initial administrator authentication and all remote administration actions are transmitted. **(FTP_TRP.1)**

7.2 System Monitoring

The System Monitoring function provides the TOE with the functionality of generating audit records to assure that information exists that allows administrators to discover intentional and unintentional issues with the configuration and/or operation of the system, the TOEs generates audit data targeted at detecting such activity.

All events logged by the audit functions are listed in Table 7.1. **(FAU_GEN.1)**

Table 7.1 – Auditable Events

Auditable Events	Additional Audit Record Contents
Start-up of the audit functions	Reason for failure.
Failure to establish a TLS, SSH and HTTPS session.	Reason for failure.
All use of the user identification mechanism, including the user identity provided.	Provided user identity, origin of the attempt (e.g., IP address).
All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).

Auditable Events	Additional Audit Record Contents
The termination of a remote session by the session locking mechanism.	
The termination of an interactive session.	
Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).	
Security related configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).	
Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).	
Resetting passwords (name of related user account shall be logged).	

The log entries contain date and time of the event **(FPT_STM.1)**, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. When an authenticated user triggers an auditable event, the identity of that user is also logged. **(FAU_GEN.2)**

7.3 TOE Administration

In order to provide a trusted means for administrators to interact with the TOE, the TOE provides a password-based logon mechanism. The TOE supports strong passwords and avoids attacks by observing a password being typed by an administrator. Session termination mitigates the risk of an account being used illegitimately. Passwords are stored unreadable and there must be no interface provided for specifically reading the password or password file such that the passwords are displayed in plain text.

7.3.1 Identification and Authentication

To gain access to the TOE, either by SSH or by Web Session, administrators must log on with a user account and password. When a user connects to the TOE an advisory notice and consent warning message is displayed regarding use of the TOE. A plain text message is displayed when the user connects via SSH or a web page when the user connects via a Web Session. **(FTA_TAB.1)** After that the user can enter his credentials.

The login authentication process on the TOE will verify the entered credentials against account information that is stored locally on the TOE. **(FIA_UID.1, FIA_UAU.2, FIA_UAU.7)**

If the entered credentials match the stored account information **(FMT_MTD.1)**, the user is granted access and assigned administrative privileges associated with their user account. **(FMT_SMR.2)** The authentication mechanism is maintained by the TOE itself.

An administrator (authorized user) can administer the TOE locally and remotely and is able to perform following administrative actions: (**FMT_SMF.1, FMT_SMR.2)**

- Ability to configure a list of services available before an entity is identified and authenticated
- Ability to configure the cryptographic functionality

The system is delivered with a single user account. This user account has administrative privileges and can be used to create other accounts.

7.3.2 Password mechanism

The TOE stores passwords in non-plaintext form and prevents the reading of plaintext passwords. The passwords entered during logon are obscured for SSH (invisible text echo) as well as Web session logons (password field used in web form). **(FPT_APW_EXT.1)**

The TOE password management capabilities for administrative passwords allow passwords to be composed of any combination of upper and lower case letters, numbers, and the following special characters: !, @, #, $, %, ^, ., (,), [,], _, -, +, |, ~, {, }. The minimum password length can be specified by the administrator and support passwords of 15 characters or greater. **(FIA_PMG_EXT.1)**

7.3.3 Session Timeouts

Any uncompleted login attempt or active session will be terminated after a defined period of inactivity. **(FTA_SSL.3, FTA_SSL.4)**. The following table provides an overview of which types of access can be configured and range values available for configuring timeouts.

Table 7.2 – Session and Login Timeouts

Type of Access	Range in seconds	Default
SSH Login	5 - 300 s	30 s
Web Session	30 - 3600 s	900 s

7.4 TSF Self Test

The TOE performs several self tests of following TSF during initial start-up **(FPT_TST_EXT.1)**:

- The consistency of the File system.
- The consistency of the Database.

Self Tests can be started by the user via management.

Self tests or any other action on the module cause alarms to be raised. They become important especially when the self tests result in failure conditions, which require user intervention to recover normal operation. The alarms are logged and can be tracked from there. If everything starts up properly and db checking passes the verification there is no explicit evidence that all the checking and db verifications were performed.

7.5 Rationale on TOE specification

The specification of the TOE security functions refers directly to the TOE security requirements. The following table displays the correlation between security requirements and security functions.

Table 7.3 – Security Requirements vs. Security Functions

Security Requirements vs. Security Functions	Protected Communications	System Monitoring	TOE Administration	TSF Self Test
FAU_GEN.1		X		
FAU_GEN.2		X		
FCS_CKM.1	X			
FCS_CKM.4	X			
FCS_COP.1(1)	X			
FCS_COP.1(2)	X			
FCS_COP.1(3)	X			
FCS_COP.1(4)	X			
FCS_TLS_EXT.1	X			
FCS_SSH_EXT.1	X			
FCS_HTTPS_EXT.1	X			
FIA_PMG_EXT.1			X	
FIA_UID.1			X	
FIA_UAU.2			X	
FIA_UAU.7			X	
FMT_MTD.1			X	
FMT_SMF.1			X	
FMT_SMR.2			X	
FPT_APW_EXT.1			X	
FPT_STM.1		X		
FPT_TST_EXT.1				X

Security Requirements vs. Security Functions	**Protected Communications**	**System Monitoring**	**TOE Administration**	**TSF Self Test**
FTA_SSL.3			X	
FTA_SSL.4			X	
FTA_TAB.1			X	
FTP_TRP.1	X			

8 Appendix

8.1 References

[CC] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Part 1: Introduction and general model, CCMB-2012-09-001,
Part 2: Security functional requirements, CCMB-2012-09-002,
Part 3: Security Assurance Requirements, CCMB-2012-09-003.

[PP-ND] Protection Profile for Network Devices, Version 1.1, 8. June 2012 with Errata #3, 3. November 2014

[CPP-ND] collaborative Protection Profile for Network Devices, Version 1.0, 27. February 2015

8.2 Acronyms

CC	Common Criteria
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
n/a	not applicable
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface