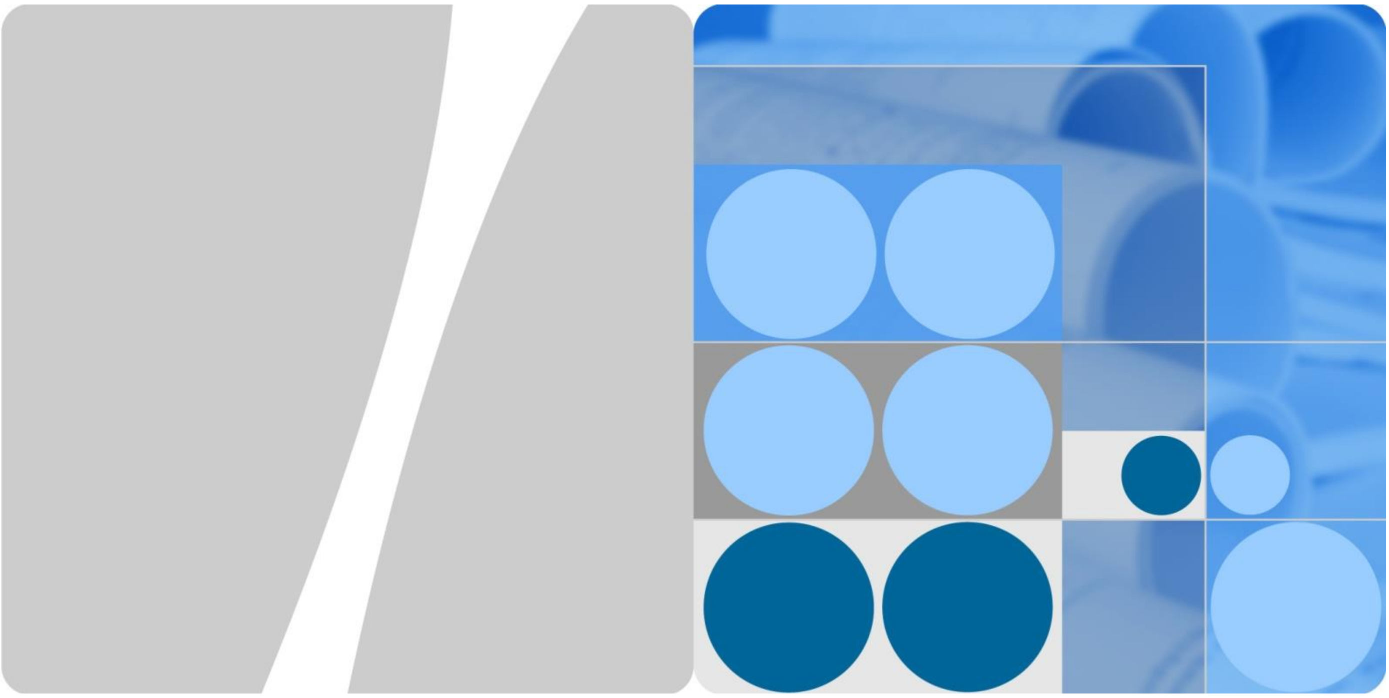


Common Criteria Protection Profile for Network Device Management (NDhPP)

Version 1.0

Date 2021-04-23

HUAWEI TECHNOLOGIES CO., LTD

About This Document

Purpose

This Protection Profile (PP) outlines the requirements for the management of Network Devices. This PP is intended for network devices that manages other network devices (network elements) or are managed by a network device, for example an element management systems.

Contents

1 PP Introduction....................5
1.1 PP Reference....................5
1.2 TOE Overview....................5
1.2.1 Introduction....................5
1.2.2 TOE usage and Major Security Features....................6
1.2.3 Non-TOE Hardware and Software....................6
1.3 Network device management classes....................6
1.3.1 Class A....................7
1.3.2 Class B....................7
2 CC conformance claims....................8
2.1 CC Conformance Claim....................8
2.2 PP Claim....................8
2.3 Package Claim....................8
2.4 Conformance Claim Rationale....................8
2.5 Conformace Statement....................9
3 Security Problem Definition....................10
3.1 Assets....................10
3.2 Threats....................10
3.2.2 Threats Components....................11
3.3 Organisational Security Policies....................12
3.4 Assumptions....................12
4 Security Objectives....................14
4.1 Security Objectives for the TOE....................14
4.2 Security Objectives for the Operational Environment....................15
4.3 Security Objectives Rationale....................16
5 Security Requirements....................18
5.1 General....................18
5.2 Conventions....................19

5.3 Security Functional Requirements 20
5.3.1 Security Audit (FAU) 20
5.3.1.1 FAU_GEN.1 Audit data generation 20
5.3.1.2 FAU_GEN.2 User identity association 21
5.3.1.3 FAU_SAR.1 Audit review 21
5.3.1.4 FAU_SAR.2 Restricted audit review 21
5.3.1.5 FAU_STG.1 Protected audit trail storage 21
5.3.1.6 FAU_STG.3 Action in case of possible audit data loss 21
5.3.2 User Data Protection (FDP) 21
5.3.2.1 FDP_ACC.2 Complete access control 21
5.3.2.2 FDP_ACF.1 Security Attribute based Access Control 22
5.3.2.3 FDP_IFC.1 Subset Information Flow Control 23
5.3.2.4 FDP_IFF.1 Simple Security Attributes 23
5.3.3 Identification and Authentication (FIA) 24
5.3.3.1 FIA_AFL.1 Authentication Failure Management 24
5.3.3.2 FIA_ATD.1 User Attribute Definition 24
5.3.3.3 FIA_UAU.2 User authentication before any action 25
5.3.3.4 FIA_UAU.5 Multiple Authentication Mechanisms 25
5.3.3.5 FIA_UAU.7 Protected authentication feedback 25
5.3.3.6 FIA_UID.2 User identification before any action 25
5.3.4 Security Management (FMT) 25
5.3.4.1 FMT_MOF.1 Management of Security Functions Behavior 25
5.3.4.2 FMT_MSA.1/ACCESS Management of security attributes 26
5.3.4.3 FMT_MSA.1/FILTER Management of security attributes 26
5.3.4.4 FMT_MSA.3/ACCESS Static attribute initialization 26
5.3.4.5 FMT_MSA.3/FILTER Static attribute initialization 26
5.3.4.6 FMT_SMF.1 Specification of Management Functions 27
5.3.4.7 FMT_SMR.1 Security roles 27
5.3.5 TOE Access (FTA) 27
5.3.5.1 FTA_SSL.3 TSF-initiated Termination 27
5.3.5.2 FTA_TSE.1 TOE session establishment 27
5.3.6 Trusted path/channels (FTP) 28
5.3.6.1 FTP_TRP.1 Trusted path 28
5.3.6.2 FTP_ITC.1 Inter-TSF trusted channel 28
5.4 Security Functional Requirements Rationale 29
5.4.1 Coverage 29
5.4.2 Sufficiency 30
5.4.3 Security Requirements Dependency Rationale 31
5.5 Security Assurance Requirements 33

5.6 Security Assurance Requirements Rationale 34

6 Optional Requirements 36

6.1 Optional Security Objective for Class A 36

6.1.2 Cryptographic support (FCS) 36

6.1.2.1 FCS_CKM.1 Cryptographic key generation 36

6.1.2.2 FCS_CKM.4 Cryptographic key destruction 37

6.1.2.3 FCS_COP.1/INFO Cryptographic operation 37

6.2 Optional Security Requirements for O.Authentication 37

6.2.2 Cryptographic support (FCS) 37

6.2.2.1 FCS_COP.1/HASH Cryptographic operation 37

6.2.3 Identification and Authentication (FIA) 38

6.2.3.1 FIA_SOS.1 Verification of secrets 38

6.2.3.2 FIA_UAU.6 Re-authenticating 38

6.2.4 TOE Access (FTA) 38

6.2.4.1 FTA_TAH.1 TOE access history 38

6.3 Optional Security Requirements for O.Audit 38

6.3.2 Security Audit (FAU) 39

6.3.2.1 FAU_SAR.3 Selectable audit review 39

6.4 Optional Security Requirements for O.NEcomm 39

6.4.2 User Data Protection (FDP) 39

6.4.2.1 FDP_UIT.1 Data exchange integrity 39

6.5 Optional Security Requirements Dependency Rationale 40

6.5.1.1 Dependency 40

7 Abbreviations and References 41

7.1 Abbreviations 41

7.2 References 42

1 PP Introduction

1.1 PP Reference

PP Title: Common Criteria Protection Profile for Network Device Management (NDhPP)

PP Version: 1.0

Publication Date: 2021-04-23

1.2 TOE Overview

1.2.1 Introduction

With the rapid development of the Internet industry and the advent of the cloud era, new business models are emerging one after another, and enterprises are moving towards cloudification and digitalization. The telecom industry, as a digital transformation enabler for various industries, faces both challenges and new business opportunities.

Service cloudification results in great flexibility and uncertainty in service applications. However, this requires an intelligent management and control layer, that has a brand-new management, control, and analysis system.

The management and control layer is positioned as the brain of cloud-based networks and integrates functions such as network management, service control, and network analysis. The management and control layer is used to manage service applications and the infrastructure networks.

This Protection Profile (PP) address the network management of cloud-based networks and defines two classes of network device management components (A and B) each of which has slightly different requirements and objectives. This PP describes the security problem definition, security objectives and security requirements for both class A and class B.

1.2.2 TOE usage and Major Security Features

In order to counter the security threats identified in section 3.2 the TOE (both A and B) provides the following security features:

- Identification and authentication of administrative users.
  - Only authenticated users can execute commands of the TOE.
- Authorization.
  - The TOE manages user privileges by access level.
- Auditing.
  - The TOE generates audit records for security-relevant management actions.
- Communication security.
  - The TOE protects data integrity and confidentiality.
- Management traffic flow control (Class B only)
  - The TOE applies an information flow security policy before processing packets received from the management network.
- Security functionality management.
  - Management of user accounts and user attributes, access control management, management of authentication failure policy, enabling/disabling trusted channels, etc.

The ST author should provide sufficient details on the SFs in the TOE Summary Specification of the ST.

1.2.3 Non-TOE Hardware and Software

The environment for TOE includes at minimum the following components.

- The components of the network device that are out of the scope of the TOE e.g. the hardware components where the TOE is installed on.
- Local PCs and remote PCs used by administrators to connect to the TOE.
- The physical infrastructure interconnecting various network elements (e.g. cables, switches, etc.)
- An external entity such as an NTP server for synchronizing time for the TOE.

The list of non-TOE hardware and software components depends on the type of the network device. The ST author should make this list complete by adding additional non-TOE components for the specified TOE (Class A or Class B).

1.3 Network device management classes

The Security Target shall define the class of the network device management components. The difference in the classes is caused by the following:

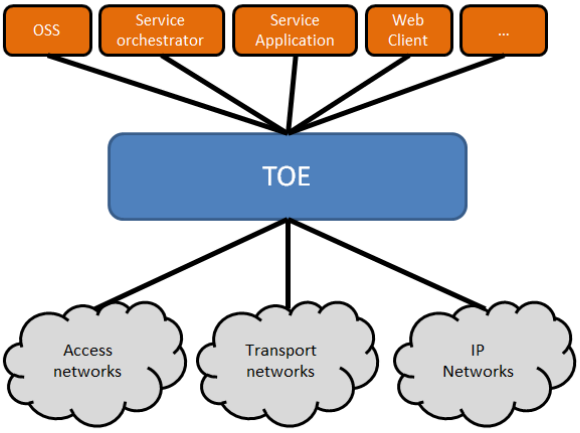
- Class A
  - The software application that is used in the management and control layer of a cloud-based network and is used to manage other infrastructure elements.

- Class B
  - The management software installed on a service application/infrastructure device

1.3.1 Class A

A software application that is located on the management and control layer of the cloud-based network. It can manage and control ubiquitous network devices, including transport, IP, and firewall devices. It provides open interfaces to quickly integrate with upper-layer application systems such as OSSs, service orchestrators and service applications. Various apps can be developed and customized to accelerate service innovation and achieve operations.

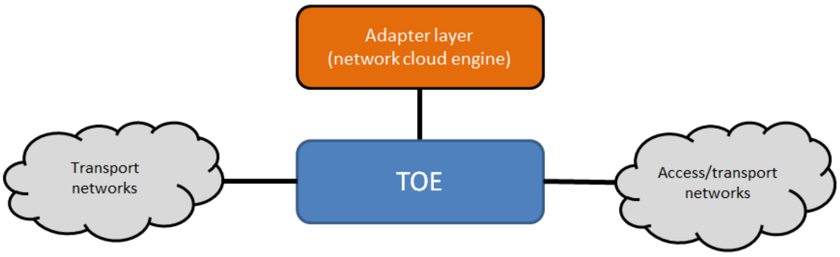
Figure 1-1 Example deployment of a Class A application



1.3.2 Class B

Management software installed on a service application/infrastructure device. Infrastructure devices such as Optical-Line-Terminal (OLT), optoelectronic OTN/WDM products transparently transmit client services from one place to another. In general these devices do not process client services transmitted from other equipment. These devices are generally managed by a EMS (Class A) device

Figure 1-2 Example deployment of a Class B application



2 CC conformance claims

2.1 CC Conformance Claim

This Protection Profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1, 2 and 3, version 3.1 revision 5 [CC]

as follows:

- Part 2 conformant,
- Part 3 conformant.

The following methodology has been taken into account:

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology, version 3.1 revision 5 [CEM31R5].

2.2 PP Claim

This PP does not claim conformance to any another Protection Profiles.

2.3 Package Claim

This PP is conforming to assurance package EAL3 augmented with ALC_FLR.2. However, the ST author may choose to claim additional or hierarchically stronger SFRs and SARs as per section 2.5

2.4 Conformance Claim Rationale

Since this PP is not claiming conformance to any other protection profile, no rationale is necessary here.

2.5 Conformace Statement

This PP requires strict conformance of any ST or PP, which claims conformance to this PP.

As this PP requires strict conformance, the ST shall contain all SFRs and SARs in the PP, but may claim additional or hierarchically stronger SFRs and SARs. This does not violate the conformance claim of the PP.

3 Security Problem Definition

3.1 Assets

The assets to be protected are the information stored, processed or generated by both TOE classes are detailed below:

- Audit data: The data which is provided by the TOE during security audit logging.
- Authentication data: The data which is used by the TOE to identify and authenticate the external entities which interact with the TOE.
- Cryptographic data: All data used by the TOE for cryptographic operations like digital signature handling and encryption or decryption purposes. This includes symmetric and asymmetric cryptographic keys.
- Configuration data for the TOE, which is used for configuration of security features and functions.
- Management Traffic data, which is the management information exchanged between the TOE and the terminal.

3.2 Threats

This section specifies the threats that are addressed by the TOE and the TOE environment. As a result, the following threats for both classes of TOE have been identified in the table below.

Table 3-1 Threats

Threat	Class A	Class B
T.UnwantedManagementTraffic The Unwanted network traffic may originate from an attacker and result in an overload of the management interfaces, which may cause a failure of the TOE to respond to system control and normal management operations.		X

Threat	Class A	Class B
T.UnauthenticatedAccess An unauthenticated person may attempt to bypass the security of the TOE so as to access the TOE.	X	X
T.UnauthorizedAccess An administrator user with restricted action and information access authorization gains access to unauthorized commands or information.	X	X
T.InterceptAdminTraffic A remote attacker is able to intercept, modify and re-use management information assets that are exchanged between the TOE and the entity used by the administrators to administer the TOE.	X	X
T.InterceptConfigTraffic A remote attacker is able to intercept, modify, or re-use information assets that are exchanged between the TOE and NEs, between the TOE client and server, and between the TOE server and OSS/service orchestrator/service application client.	X	

3.2.2 Threats Components

- T.UnwantedManagementTraffic

  Threat agent: Attacker.
  Asset: Audit data, Configuration data.
  Adverse action: Disturbance on TOE operation.

- T.UnauthenticatedAccess

  Threat agent: Unauthenticated person.
  Asset: Authentication data, Audit data, Configuration data, Cryptographic data, Management Traffic data.
  Adverse action: Access to the TOE.

- T.UnauthorizedAccess

  Threat agent: An administrator user with restricted action and information access authorization.
  Asset: Authentication data, Audit data, Configuration data, Cryptographic data, Management Traffic data.
  Adverse action: Access to unauthorized commands or information.

- T.InterceptAdminTraffic

  Threat agent: Remote attacker in the management network.
  Asset: Management traffic data such as Authentication data, Cryptographic data, Configuration data.
  Adverse action: Intercept, modify and re-use management information assets that are exchanged

between the TOE and the entity used by the administrators to administer the TOE.

- T.InterceptConfigTraffic

  Threat agent: Remote attacker in the management network.
  Asset: Authentication data, Cryptographic data, Configuration data.
  Adverse action: intercept, modify, or re-use information assets that are exchanged between the TOE and NEs, between the TOE client and server, and between the TOE server and OSS/service orchestrator/service application client.

3.3 Organisational Security Policies

No OSPs have been defined in this PP.

3.4 Assumptions

The following table provides defines the assumptions made for both classes of TOE.

Table 3-2 Assumptions

Assumptions	Class A	Class B
A.PhysicalProtection The hardware that the TOE is running on is operated in a physically secure and in a well-managed environment.	X	X
A.ManagementElements It is assumed that the operational environment provides reliable timestamps via NTP server and if required remote authentication mechanism (RADIUS). These servers are located within the trusted, internal network.	X	X
A.NetworkSegregation It is assumed that the operational environment provides segregation of networks by deploying the management interface in TOE into an independent network.	X	X
A.Firewall Communications with the TOE server are performed through a firewall	X	
A.NoEvil It is assumed that personnel working as authorized administrators and non-TOE administrators (administrators that have physical access to the TOE but do not operate the TOE) shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These administrative users will be competent, and not careless or wilfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.	X	X

Assumptions	**Class A**	**Class B**
A.NetworkElements It is assumed that the managed network elements are trusted and can support the TLS/SNMPv3/SSHv2/SFTP connection with the TOE. The operational environment provides securely and correctly working network devices as resources that the TOE needs to cooperate with.	X	X
A.TrustedPlatform It is assumed that the underlying hardware of the network device, which is outside the scope of the TOE operates as intended. This also applies to any non-TOE software component installed on the underlying hardware.	X	X

4 Security Objectives

4.1 Security Objectives for the TOE

The following table provides defines the security objectives for the TOE for both classes of the TOE.

Table 4-1 Security Objectives for the TOE

Security Objectives for TOE	Class A	Class B
O.Communication The TOE implements logical protection measures for network communication between the TOE and management device/workstation.	X	X
O.NEcomm The TOE implements logical protection measures for the network communication between the TOE and class A network devices (applications/services).	X	
O.Authorization The TOE shall implement different authorization roles that can be assigned to users in order to restrict the functionality that is available to them.	X	X
O.Authentication The TOE authenticates users before access to data and security functions is granted. The TOE provides configurable system policies to restrict user session establishment.	X	X
O.Audit The TOE shall provide functionality to generate audit records for security-relevant administrator actions.	X	X
O.SecurityManagement The TOE shall provide functionality to manage security functions provided by the TOE.	X	X

Security Objectives for TOE	Class A	Class B
O.DataFilter The TOE shall ensure that only allowed management traffic goes through the TOE.		X

4.2 Security Objectives for the Operational Environment

The following table provides defines the security objectives for the operational environment for both classes of the TOE.

Table 4-2 Security Objectives for the Operational Environment

Security Objectives for Operational Environment	Class A	Class B
OE.PhysicalProtection The TOE and its operational environment (i.e. the complete system including attached peripherals) shall be protected against unauthorized physical access. Only administrators and non-TOE administrators (administrators that have physical access to the TOE but do not operate the TOE) with explicit approval by the administrator(s) shall be authorized to physically access the TOE and its operational environment.	X	X
OE.ManagementElements The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. The behaviour of such network devices provided by the operational environment shall be secure and correct and be protected against unauthorized physical access. This applies e.g. to devices used for TOE management, time management (NTP server) and if required remote authentication mechanism (RADIUS).	X	X
OE.NetworkSegregation The operational environment protects the network where the TOE hosts are installed by separating it from the application (or public) network.	X	X
OE.Firewall A firewall is installed between the TOE server and untrusted domain to filter unused communication ports.	X	
OE.NoEvil Personnel working as authorized administrators and non-TOE administrators (administrators that have physical access to the TOE but do not operate the TOE) shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These administrative users shall be competent, and not careless or willfully negligent or hostile, and shall follow and abide by the instructions provided by the TOE documentation.	X	X

Security Objectives for Operational Environment	Class A	Class B
OE.NetworkElements The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. The behaviour of such network devices provided by the operational environment shall be secure and correct.	X	X
OE.TrustedPlatform It is assumed that the underlying hardware of the network device, which is outside the scope of the TOE operates as intended. This also applies to any non-TOE software component installed on the underlying hardware.	X	X

4.3 Security Objectives Rationale

The following table provides a mapping of TOE objectives to threats, showing that each objective is at least covered by one threat

Table 4-3 Security objectives coverage

Threat/Assumption	Security Objectives	Rationale for Security Objective
T.UnwantedManagementTraffic (Class B type of TOE)	O.DataFilter	Requires the TOE to filter unwanted management traffic.
	O.SecurityManagement	Requires the TOE to allow the configuration of filter rules by an authorized users with sufficient user level.
	OE.NetworkSegregation	Requires the operational environment to provide a separate network that is used to access/manage the TOE.
T.UnauthenticatedAccess	O.Authentication	Requires the TOE to implement an authentication mechanism for its users.
	O.Audit	Requires the TOE to generate and store login attempts. This allows detection of login attempts and possible tracing of the offender.
	O.SecurityManagement	Requires the TOE to allow configuration of the authentication mechanisms by users with sufficient user level.

Threat/Assumption	Security Objectives	Rationale for Security Objective
T.UnauthorizedAccess	O.Authorization	Requires the TOE to implement an access control mechanism.
	O.Audit	Requires the TOE to generate and store actions. This allows detection of unauthorized action attempts and possible tracing of the offender.
	O.SecurityManagement:	Requires the TOE to allow configuration of the authentication mechanisms by users with sufficient user level.
T.InterceptAdminTraffic	O.Communication:	Requires the TOE to implement a secure communication channel to be used for management of the TOE.
	O.SecurityManagement	Requires the TOE to allow configuration of the secure communication channel.
T.InterceptConfigTraffic (Class A TOE type)	O.NEcomm	Requires the TOE to implement logical protection measures for the network communication between the TOE and the OSS/service orchestrator/service application.
	O.SecurityManagement	Requires the TOE to implement the management of the logical protection measure.
	OE.NetworkElements	Requires the operational environment provides securely and correctly working network devices.
A.PhysicalProtection	OE.PhysicalProtection	The objectives for the environment are mirrored by the assumptions. Therefore, the mapping is trivial.
A.NetworkSegregation	OE.NetworkSegregation	
A.Firewall	OE.Firewall	
A.NoEvil	OE.NoEvil	
A.NetworkElements	OE.NetworkElements	
A.TrustedPlatform	OE.TrustedPlatform	
A.ManagementElements	OE.ManagementElements	

5 Security Requirements

5.1 General

As defined in section 1.2 1.2 two classes of network device management, which differ from each other in various aspects. This chapter describes a number of security requirements, but not all security requirements are valid for all classes. This is indicated in Table 5-1.

Table 5-1 Security functional requirements for the network device management TOEs

Security Functional Requirement		Class A	Class B
FAU_GEN.1	Audit event records generation	X	X
FAU_GEN.2	User identity association	X	X
FAU_SAR.1	Audit review	X	X
FAU_SAR.2	Restricted audit review	X	X
FAU_STG.1	Protected audit trail storage	X	X
FAU_STG.3	Action in case of possible audit data loss	X	X
FDP_ACC.2	Complete access control	X	X
FDP_ACF.1	Security attribute based access control	X	X
FDP_IFC.1	Subset information flow control		X
FDP_IFF.1	Simple security attributes		X
FIA_AFL.1	Authentication failure handling	X	X
FIA_ATD.1	User attribute definition	X	X
FIA_UAU.2	User authentication before any action	X	X
FIA_UAU.5	Multiple authentication mechanisms	X	X

Security Functional Requirement		Class A	Class B
FIA_UAU.7	Protected authentication feedback	X	X
FIA_UID.2	User identification before any action	X	X
FMT_MOF.1	Management of security functions behaviour	X	X
FMT_MSA.1/ACCESS	Management of security attributes	X	X
FMT_MSA.1/FILTER	Management of security attributes		X
FMT_MSA.3/ACCESS	Static attribute initialisation	X	X
FMT_MSA.3/FILTER	Static attribute initialisation		X
FMT_SMF.1	Specification of Management Functions	X	X
FMT_SMR.1	Security roles	X	X
FTA_SSL.3	TSF-initiated termination	X	X
FTA_TSE.1	TOE session establishment	X	X
FTP_TRP.1	Trusted path	X	X
FTP_ITC.1	Inter-TSF trusted channel	X	

5.2 Conventions

In order to define the Security Functional Requirements Part 2 of the Common Criteria was used. However, some Security Functional Requirements require operations to be made to the requirement to allow the developer to tailor the security requirements. The operations allowed are:

- Refinement operations are used to alter the requirement. Note the refinement is made to restricts the requirement
- Selection operation are used to select one or more options provided by the CC in stating a requirement
- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password.
- The iteration operation is used when a component is repeated with varying operations.

Therefore, the following convention is used:

- Refinements
  - Added words are in ***bold italics*** text and removed words are ~~strikethrough~~.
- Selections
  - Selections made by this PP are denoted with **bold** text.
  - Selections to be made by the ST author appear in square brackets[] with an indication that a

selection is to be made [selection:] and the selection to be made are in *underlined italics*.

- Assignments:
  - Assignments made by this PP are denoted with underlined text.
  - Assignments to be made by the ST author appear in square brackets[] with an indication that an assignment is to be made [assignment:] and details on the assignment are in *italics*.
- Iterations:
  - Iterations are denoted by showing a forward slash/, and the iteration indicator after the component identifier.

5.3 Security Functional Requirements

5.3.1 Security Audit (FAU)

5.3.1.1 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:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the ***not specified***[1] level of audit; and

c) The following auditable events:

i. user activity

1) login, logout events

ii. user management

1) add, delete, modify users
2) user password change

iii. [assignment: *other specifically defined auditable events*][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; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

Application Note: The other audit relevant information may include e.g. user name, IP address.

[1] [selection: choose one of: *minimum*, *basic*, *detailed*, *not specified*]

[2] [assignment: *other specifically defined auditable events*]

5.3.1.2 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.

5.3.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [assignment: *authorized users*] with the capability to read all information[3] from the audit records.

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

5.3.1.4 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.

5.3.1.5 FAU_STG.1 Protected audit trail storage

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

FAU_STG.1.2 The TSF shall be able to **prevent**[4] unauthorized modifications to the stored audit records in the audit trail.

5.3.1.6 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *pre-defined limit*].

5.3.2 User Data Protection (FDP)

5.3.2.1 FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the Access Control SFP[5] on

Subject: users;

Objects: commands provided by TOE[6]

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

[3] [assignment: *list of audit information*]

[4] [selection, choose one of: *prevent, detect*]

[5] [assignment: *access control SFP*]

[6] [assignment: *list of subjects and objects*]

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.

5.3.2.2 FDP_ACF.1 Security Attribute based Access Control

FDP_ACF.1.1 The TSF shall enforce the Access Control SFP[7] to objects based on the following:

Subject security attributes:

Users and their following security attributes:

- user identity
- user level

Objects security attributes:

Commands and their security attributes:

- command level[8].

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

1) Only authorized users are permitted access to commands.
2) Users can be configured with different user levels to control the device access permission.
3) There are [assignment: *number of user access levels*] user access levels and command levels.
4) A user can access a command if the command's access level is lower or equal to the user's access level.
5) The command level is stored by the TOE and [selection, choose one of: *can*, *cannot*] be modified by [assignment: *user role*][9].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[10].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[11].

[7] [assignment: *access control SFP*]

[8] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

[9] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[10] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]

[11] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

5.3.2.3 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the Management Network Filtering SFP[12] on

Subjects:

- Device management interface

Information:

- IP packets

Operations:

- Device management interface will accept or deny IP packets based on the settings of the device management interface and the IP packets content (i.e. based on subject attributes and information security attributes as defined in Section 5.3.2.4)[13].

5.3.2.4 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the Management Network Filtering SFP[14] based on the following types of subject and information security attributes

Subject:

- Device management interface

Subject attributes:

- IP address setting of the device management interface
- Port number

Information security attributes:

- Source IP address
- Destination IP address
- IP Protocol number
- Source port number
- Destination port number[15].

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

[12] [assignment: *information flow control SFP*]

[13] [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]

[14] [assignment: *information flow control SFP*]

[15] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

1) The TOE uses the Access Control List (ACL) to match the IP packets received from the device management interface. If the IP packet match an ACL rule, the TOE discards or accepts the packets based on the action specified in the ACL rule.

2) An ACL rule contains one or more of the following attributes: source IP address, destination IP address, IP protocol number, source port number, and destination port number[16].

FDP_IFF.1.3 The TSF shall enforce the no additional information flow control SFP rules[17].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: none[18].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: none[19].

5.3.3 Identification and Authentication (FIA)

5.3.3.1 FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: *positive integer number*], *an administrator configurable positive integer within* [assignment: *range of acceptable values*]]: unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*]

5.3.3.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

1) User ID

2) User level

3) User password

4) The inactivity time after which an account is automatically logged out.

5) Status of the account (locked/unlocked)

6) Number of failed authentication attempts within a certain period of time and timestamp of last successful login

7) [assignment: *other security attributes*][20]

[16] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attribute*]

[17] [assignment: *additional information flow control SFP rules*]

[18] [assignment: *rules, based on security attributes, that explicitly authorize information flows*]

[19] [assignment: *rules, based on security attributes, that explicitly deny information flows*]

[20] [assignment: *list of security attributes*]

5.3.3.3 FIA_UAU.2 User authentication before any action

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

Application Note: The authentication mechanism for NBIs and NEs to connect to Class A device is also implemented by FIA_UAU.2.

5.3.3.4 FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide the following authentication mechanisms:

1) Remote authentication by [assignment: *authentication mechanism for remote authentication*]
2) Local Authentication by [assignment: *authentication mechanism for local authentication*][21]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules:

1) For remote authentication, [assignment: *rules describing how the authentication mechanism provides authentication*]
2) For local authentication, [assignment: *rules describing how the authentication mechanism provides authentication*][22].

5.3.3.5 FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.

5.3.3.6 FIA_UID.2 User identification before any action

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

5.3.4 Security Management (FMT)

5.3.4.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to **determine the behaviour of**[23] the functions identified in FMT_SMF.1[24] to [assignment: *the authorised identified roles defined in FMT_SMR.1*].

[21] [assignment: *list of multiple authentication mechanisms*]

[22] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

[23] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[24] [assignment: *list of functions*]

5.3.4.2 FMT_MSA.1/ACCESS Management of security attributes

FMT_MSA.1.1/ACCESS The TSF shall enforce the Access Control SFP[25] to restrict the ability to **query, modify**[26] the security attributes identified in FDP_ACF.1 and FIA_ATD.1 and [assignment: *additional security attributes*][27] to [assignment: *the authorised identified roles defined in FMT_SMR.1*].

5.3.4.3 FMT_MSA.1/FILTER Management of security attributes

FMT_MSA.1.1/FILTER The TSF shall enforce the Management Network Filtering SFP[28] to restrict the ability to **query, modify**[29] the security attributes identified in FDP_ACF.1 and FIA_ATD.1 and [assignment: *additional security attributes*][30] to users with administrator or super administrator user level as defined in FMT_SMR.1[31].

5.3.4.4 FMT_MSA.3/ACCESS Static attribute initialization

FMT_MSA.3.1/ACCESS The TSF shall enforce the Access Control SFP[32] to provide **permissive**[33] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/ACCESS The TSF shall allow users with administrator or super administrator user level as defined in FMT_SMR.1[34] to specify alternative initial values to override the default values when an object or information is created.

5.3.4.5 FMT_MSA.3/FILTER Static attribute initialization

FMT_MSA.3.1/FILTER The TSF shall enforce the Management Network Filtering SFP[35] to provide **permissive**[36] default values for security attributes that are used to enforce the SFP.

[25] [assignment: *access control SFP(s), information flow control SFP(s)*]

[26] [selection: *change default, query, modify, delete, [assignment: other operations]*]

[27] [assignment: *list of security attributes*]

[28] [assignment: *access control SFP(s), information flow control SFP(s)*]

[29] [selection: *change default, query, modify, delete, [assignment: other operations]*]

[30] [assignment: *list of security attributes*]

[31] [assignment: *the authorized identified roles*]

[32] [assignment: *access control SFP(s), information flow control SFP(s)*]

[33] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

[34] [assignment: *the authorized identified roles*]

[35] [assignment: *access control SFP(s), information flow control SFP(s)*]

[36] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

FMT_MSA.3.2/FILTER The TSF shall allow users with administrator or super administrator or operator user level as defined in FMT_SMR.1[37] to specify alternative initial values to override the default values when an object or information is created.

5.3.4.6 FMT_SMF.1 Specification of Management Functions

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

1) Management of user accounts and user attributes, including user credentials
2) Management of authentication failure policy
3) Configuration of network addresses for services used by the TOE
4) Enabling/disabling trusted channels for remote access to the TOE's management interfaces
5) Management of the TOE's time
6) [selection: *Management of ACLs and ACL parameters like IP addresses or address ranges*, [assignment: *other functions*]].[38]

Application Note: the services used by the TOE are NTP and remote authentication mechanisms defined in FIA_UAU.5 e.g. RADIUS.

5.3.4.7 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *multiple administrator roles*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.3.5 TOE Access (FTA)

5.3.5.1 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].

5.3.5.2 FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on

1) User authentication failure
2) [Selection, for class B TOE: *Source IP address,* assignment: *other attributes*].[39]

[37] [assignment: *the authorized identified roles*]

[38] [assignment: *list of management functions to be provided by the TSF*]

[39] [assignment: *attributes*]

5.3.6 Trusted path/channels (FTP)

5.3.6.1 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and **remote**[40] 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**[41].

FTP_TRP.1.2 The TSF shall permit **the TSF *and* remote users**[42] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **initial user authentication and remote management**[43].

Application Note: The ST author needs to iterate this requirement for each protocol that shall be used to establish a trusted path for secure communication management. Examples of such protocols are SSH, TLS, and SFTP protocols.

5.3.6.2 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product 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 The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for authentication, dumping audit logs, backing up NE Data and restoring NE data[44].

[40] [selection*: remote, local*]

[41] [selection: *modification, disclosure, [assignment: other type of integrity or confidentiality violation]*]

[42] [selection: *the TSF, local users, remote users*]

[43] [selection: *initial user authentication, [assignment: other services for which trusted path is required]*]

[44] [assignment: *list of functions for which a trusted channel is required*]

5.4 Security Functional Requirements Rationale

5.4.1 Coverage

The development and the evaluation of the TOE shall be done in accordance to the following security assurance requirements:

Table 5-2 Mapping SFRs to objectives

Security Functional Requirements	O.Communication	O.NEcomm	O.Authorization	O.Authentication	O.Audit	O.SecurityManagement	O.SensitiveInformation	O.DataFilter
FAU_GEN.1					X			
FAU_GEN.2					X			
FAU_SAR.1					X			
FAU_SAR.2					X			
FAU_STG.1					X			
FAU_STG.3					X			
FDP_ACC.2			X					
FDP_ACF.1			X					
FDP_IFC.1								X
FDP_IFF.1								X
FIA_AFL.1				X				
FIA_ATD.1			X					
FIA_UAU.2				X				
FIA_UAU.5				X				
FIA_UAU.7				X				
FIA_UID.2			X					
FMT_MOF.1						X		
FMT_MSA.1/ACCESS						X		

Security Functional Requirements	**O.Communication**	**O.NEcomm**	**O.Authorization**	**O.Authentication**	**O.Audit**	**O.SecurityManagement**	**O.SensitiveInformation**	**O.DataFilter**
FMT_MSA.1/FILTER								X
FMT_MSA.3/ACCESS						X		
FMT_MSA.3/FILTER								X
FMT_SMF.1						X		
FMT_SMR.1			X			X		X
FTA_SSL.3	X			X				
FTA_TSE.1	X							X
FTP_TRP.1	X							
FTP_ITC.1		X						

5.4.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Table 5-3 SFR sufficiency analysis

Security objective	**Rationale**
O.Communication	Communication security is implemented by the establishment of a trusted path in FTP_TRP.1. Termination of inactive secure sessions is covered by FTA_SSL.3. FTA_TSE.1 addresses that session establishment is denied if an ACL exists that specifies a deny rule for the attempted connection.
O.NEcomm	Communication security is implemented by the establishment of a trusted channel in FTP_ITC.1 between the TOE and network elements.
O.DataFilter	The requirement of ACL is defined in FDP_IFF.1 and FDP_IFC.1 and the impact on session establishment is covered in FTA_TSE.1. The requirements on management functionality for the definition of ACL are provided in FMT_MSA.1/FILTER, FMT_MSA.3/FILTER and FMT_SMF.1. Rejection of connections are also addressed by FTA_TSE.1.

O.Audit	The generation of audit records is implemented by FAU_GEN.1. Audit records are supposed to include timestamp as provided by an external entity (e.g. an external NTP server) and user identities as defined in FAU_GEN.2. The protection of unauthorized deletion and modification of the audit trail storage is implemented in FAU_STG.1. FAU_STG.3 ensure that possible audit data loss is prevented when the audit tail is exceeded. Requirements on reading audit records are defined in FAU_SAR.1 and FAU_SAR.2
O.Authentication	User authentication is implemented by FIA_UAU.2, and FIA_UAU.5. Authentication feedback information is protected by FIA_UAU.7. Interactive management sessions are terminated by FTA_SSL.3. The authentication mechanism supports authentication failure handling as addressed in FIA_AFL.1.
O.Authorization	User identification is addressed in FIA_UID.2. The requirement for access control is detailed in FDP_ACC.2, and the access control policies are modelled in FDP_ACF.1. User-related attributes are detailed in FIA_ATD.1. Access control is based on the definition of roles as subject and functions as object as defined in FMT_SMR.1.
O.Security Management	The management functionality for the security functions of the TOE are defined in FMT_SMF.1, FMT_MOF.1, FMT_MSA.1/ACCESS, FMT_MSA.1/FILTER, FMT_MSA.3/ACCESS and FMT_MSA.3/FILTER and the security user roles are defined in FMT_SMR.1.

5.4.3 Security Requirements Dependency Rationale

The following table demonstrates the dependencies of SFRs modelled in CC Part 2 and how the SFRs for the TOE resolve those dependencies.

Table 5-4 TOE security functional requirements dependencies rationale

Security Functional Requirement	Dependencies	Rationale
FAU_GEN.1	FPT_STM.1	This TOE relies on an external entity (e.g. an external NTP server) to provide the timestamp and it does not provide the reliable timer.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Met by: FAU_GEN.1 FIA_UID.1

Security Functional Requirement	Dependencies	Rationale
FAU_SAR.1	FAU_GEN.1	Met by: FAU_GEN.1
FAU_STG.1	FAU_GEN.1	Met by: FAU_GEN.1
FAU_STG.3	FAU_STG.1	Met by: FAU_STG.1
FDP_ACC.2	FDP_ACF.1	Met by: FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Met by: FDP_ACC.1 FMT_MSA.3/ACCESS
FDP_IFC.1	FDP_IFF.1	Met by: FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Met by: FDP_IFC.1 FMT_MSA.3/FILTER
FIA_AFL.1	FIA_UAU.1	Met by: FIA_UAU.2
FIA_ATD.1	No dependencies	N/A
FIA_UAU.2	FIA_UID.1	Met by: FIA_UID.2
FIA_UAU.5	No dependencies	N/A
FIA_UID.1	No dependencies	N/A
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	Met by: FMT_SMF.1 FMT_SMR.1
FMT_MSA.1/ACCESS	[FDP_ACC.1, or FDP_ICF.1] FMT_SMR.1 FMT_SMF.1	Met by: FDP_ACC.1 FMT_SMR.1 FMT_SMF.1

Security Functional Requirement	Dependencies	Rationale
FMT_MSA.1/FILTER	[FDP_ACC.1, or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Met by: FDP_IFC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3/ACESS	FMT_MSA.1 FMT_SMR.1	Met by: FMT_MSA.1/ACCESS FMT_SMR.1
FMT_MSA.3/FILTER	FMT_MSA.1 FMT_SMR.1	Met by: FMT_MSA.1/IFF FMT_SMR.1
FMT_SMF.1	No Dependencies	N/A
FMT_SMR.1	FIA_UID.1	Met by: FIA_UID.2
FTA_SSL.3	No Dependencies	N/A
FTA_TSE.1	No Dependencies	N/A
FTP_TRP.1	No Dependencies	N/A

5.5 Security Assurance Requirements

The security assurance requirements for the TOE are Evaluation Assurance Level 3 augmented with ALC_FLR.2, as specified in [CC] Part 3. No operations are applied to the assurance components.

Table 5-5 Security Assurance Requirements

Assurance Class	Assurance component	Component Description
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.3	Authorisation controls

Assurance Class	**Assurance component**	**Component Description**
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_FLR.2	Flaw reporting procedures
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
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

5.6 Security Assurance Requirements Rationale

The Evaluation Assurance Level 3 augmented with ALC_FLR.2 has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

Dependencies within the EAL3 package have been considered by the authors of CC Part 3 and are therefore not analysed here. Requirement ALC_FLR.2 has no dependencies.

A discerning developer may can choose to claim a high assurance package. The PP recommends the ST author use the hierarchically stronger SARs required for EAL4. For situations where the developer requires further assurance. The PP allows the ST author the possibility as this PP requires strict conformance.

If EAL 4 is chosen the ST author is to use the following hierarchically stronger and additional SARs packages:

- Hierarchically stronger:
  - ADV_FSP.4: Functional specification with complete summary
  - ADV_TDS.3: Basic modular design
  - ALC_CMC.4: Production support, acceptance procedures and automation
  - ALC_CMS.4: Problem tracking CM coverage
  - AVA_VAN.3: Focused vulnerability analysis
- Additional SARs:
  - ADV_IMP.1: Implementation representation of the TSF
  - ALC_TAT.1: Well-defined development tools

6 Optional Requirements

6.1 Optional Security Objective for Class A

Class A device may store sensitive information that can assist threat T.UnauthorizedAccess. Therefore, an additional security objective for the TOE can be selected by the ST author to mitigate the threat T.UnauthorizedAccess.

Table 6-1 Additional Security Objectives for the TOE

Additional Security Objectives for TOE
O.SensitiveInformation The TOE shall provide the ability to encrypt sensitive information such as users' mobile numbers and email addresses.

The ST author can select this security objective for the TOE and along with the following additional security functional requirements.

Table 6-2 Additional security functional requirements for O.SensitiveInformation

Additional Security Functional Requirement	
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1/INFO	Cryptographic operation

The SFRs shown in the table above covers O.SensitiveInformation by requiring the TOE to implement a symmetric encryption algorithm to encrypt the sensitive information detailed in the objective. The optional SFRs are listed below. The dependency rationale is given in section 6.5 . The ST author is to follow the conventions listed in 5.2

6.1.2 Cryptographic support (FCS)

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 [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [*assignment: list of standards*].

6.1.2.2 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 [*assignment: cryptographic key destruction method*] that meets the following: [*assignment: list of standards*].

6.1.2.3 FCS_COP.1/INFO Cryptographic operation

FCS_COP.1.1/INFO The TSF shall perform symmetric de- and encryption[45] in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [*assignment: list of standards*].

6.2 Optional Security Requirements for O.Authentication

Additional security requirements are be selected by the ST author to further strengthen the security objective O.Authentication. This objective requires the TOE to authenticate users before accessing the TOE. The following optional functional security requirements provide further requirements on user management and TOE access. The ST author is able to select these requirements for both Class A and Class B devices.

Table 6-3 Optional security functional requirements for O.Authentication

Additional Security Functional Requirement	
FCS_COP.1/HASH	Cryptographic operation
FIA_SOS.1	Verification of secrets
FIA_UAU.6	Re-authenticating
FTA_TAH.1	TOE access history

The optional SFRs are listed below. The dependency rationale is given in section 6.5 . The ST author is to follow the conventions listed in 5.2

6.2.2 Cryptographic support (FCS)

6.2.2.1 FCS_COP.1/HASH Cryptographic operation

FCS_COP.1.1/HASH The TSF shall perform password hashing[46] in accordance with a specified cryptographic algorithm [*assignment: hash algorithm*] ~~and cryptographic key sizes [*assignment: cryptographic key sizes*]~~ that meet the following: [*assignment: list of standards*].

[45] [assignment: list of cryptographic operations]

[46] [assignment: list of cryptographic operations]

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

6.2.3.2 FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [assignment: *list of conditions under which re-authentication is required*].

6.2.4 TOE Access (FTA)

6.2.4.1 FTA_TAH.1 TOE access history

FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the [selection: *date, time, method, location*] of the last successful session establishment to the user.

FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the [selection: *date, time, method, location*] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

6.3 Optional Security Requirements for O.Audit

Additional security requirements are be selected by the ST author to further strengthen the security objective O.Audit. This objective requires the TOE to generate audit records. The following optional functional security requirement adds selectable audit review as the TOE may generate a large amount of audit records and therefore the need for selectable review is required. The ST author is able to select these requirements for both Class A and Class B devices.

Table 6-4 Optional security functional requirements for O.Audit

Additional Security Functional Requirement	
FAU_SAR.3	Selectable audit review

The optional SFRs are listed below. The dependency rationale is given in section 6.5 . The ST author is to follow the conventions listed in 5.2

6.3.2 Security Audit (FAU)

6.3.2.1 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [assignment: *methods of selection and/or ordering*] of audit data based on [assignment: *criteria with logical relations*].

6.4 Optional Security Requirements for O.NEcomm

Additional security requirements are be selected by the ST author to further strengthen the security objective O.NEcomm. This objective requires the TOE implement logical protection measures for the network communication between the TOE and network elements. Some network elements require the use of a CA server to apply certificates (apply for a certificate, update the certificate, and publish the CRL certificate revocation list (CRL) file). Therefore, the following optional functional security requirement adds integrity requirement to the certificate exchange.The ST author is able to select these requirements for Class A device only.

Table 6-5 Optional security functional requirements for O.NEcomm

Additional Security Functional Requirement	
FDP_UIT.1	Data exchange integrity

The optional SFRs are listed below. The dependency rationale is given in section 6.5 . The ST author is to follow the conventions listed in 5.2

6.4.2 User Data Protection (FDP)

6.4.2.1 FDP_UIT.1 Data exchange integrity

FDP_UIT.1.2 The TSF shall ~~enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to~~ **transmit and receive**[47] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [selection: *modification, deletion, insertion, replay*] has occurred.

[47] [selection: transmit, receive]

6.5 Optional Security Requirements Dependency Rationale

6.5.1.1 Dependency

Table 6-6 Optional TOE security functional requirements dependencies rationale

Security Functional Requirement	Dependencies	Rationale
FCS_CKM.1	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	Met by: FCS_COP.1 FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	Met by: FCS_CKM.1
FCS_COP.1/INFO	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Met by: FCS_CKM.1 FCS_CKM.4
FCS_COP.1/HASH	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	The SFR has been refined to a hashing operation. Therefore key management is not required.
FIA_SOS.1	No dependency	N/A
FIA_UAU.6	No dependency	N/A
FTA_TAH.1	No dependency	N/A
FAU_SAR.3	FAU_STG.1	Met by: FAU_STG.1
FDP_UIT.1	[FDP_ACC.1, or FDP_IFC.1], [FTP_ITC.1, or FTP_TRP.1]	FDP_ACC.1 and FDP_IFC.1 are not applicable because there is no access control or information flow control enforced. FTP_ITC.1 and FTP_TRP.1 are not applicable because there is no confidentiality issue and no trusted path.

7 Abbreviations and References

7.1 Abbreviations

Table 7-1 Abbreviations

Name	Explanation
ACL	Access Control List
CC	Common Criteria
EAL	Evaluation Assurance Level
IP	Internet Protocol
LMT	Local Maintenance Terminal
NTP	Network Time Protocol
PP	Protection Profile
RMT	Remote Maintenance Terminal
SFP	Security Function Policies
SFR	Security Functional Requirement
SSH	Secure Shell
TLS	Transport Layer Security
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

7.2 References

Table 7-2 References

Name	Description
[CC]	Common Criteria for Information Technology Security Evaluation. Part 1-3, April 2017, Version 3.1 Revision 5, CCMB-2017-04-001, -002, -003
[CEM31R5]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 5, CCMB-2017-04-004