Security Target for Ericsson Smart Service Router SSR 8020, SSR 8010 running IPOS Software

DESIGN SPECIFICATION

Headquarters:

Ericsson AB,
Torshamnsgatan 23,
Zip Code 164 83,
Stockholm, Sweden.

R&D India Center:

4-5th floor building,
Ferns Icon, Doddanekundi Main Rd,
Doddanekundi,
Bengaluru, Karnataka 560037

Rev PA12

Revision	Author(s)	Date	Approver	Description
PA1	Ravi Ashvin Divecha	12-March-2015	Ravi Ashvin Divecha	Checked in version in Ericsson repository : Eridoc. All comments implemented from observation reports received from ERTL
PA2	Raghuraman M	24-June-2015	Ravi Ashvin Divecha	Updated based on observation report OR_ASE_260515
PA3	Raghuraman M	11-Jan-2016	Ravi Ashvin Divecha	Updated based on observation report OR_ASE_260515 again.
PA4	Raghuraman M	11-Jan-2016	Ravi Ashvin Divecha	Updated based on observation report OR_ASE_260515 again.
PA5	Raghuraman M	18-May-216	Ravi Ashvin Divecha	Updated based on email received on 29-Feb-2016.
PA6	Raghuraman M	10-June-2016	Ravi Ashvin Divecha	Updated based on meeting with Malbika on 10th June.
PA7	Raghuraman M	10-June-2016	Ravi Ashvin Divecha	Updated based on meeting with Malbika on 10th June.
PA8	Raghuraman M	10-June-2016	Ravi Ashvin Divecha	Updated based on meeting with Malbika on 10th June.
PA9	Ravi Ashvin Divecha	21-Sept-2016	Ravi Ashvin Divecha	Updated based on comments from ERTL for DSA key
PA10	Ravi Ashvin Divecha	29-Sept-2016	Ravi Ashvin Divecha	Updated based on comments from ERTL team
PA11	Ravi Ashvin Divecha	30-Sept-2016	Ravi Ashvin Divecha	Updated based on comments from ERTL team
PA12	Ravi Ashvin Divecha	3-Nov-2016	Ravi Ashvin Divecha	Updated the version number

© Ericsson AB 2016
Ericsson Internal

Contents

© Ericsson AB 2016
Ericsson Internal

Contents – Tables and Figures

-

1 ST Introduction

1.1 ST and TOE Reference Identification

TOE Reference: IPOS*, running on* Ericsson Smart Service Routers, SSR 8020, SSR 8010

IPOS Build number: IPOS-15.2.129.1.108-Release

IPOS Build Date: 15-July-2015

ST Reference: Security Target for Ericsson Smart Service Router SSR 8020, SSR 8010 running IPOS Software.

ST Version: Revision PA12

Assurance Level: Evaluation Assurance Level (EAL) 3

ST Author: Ericsson

Keywords: Router, IP, Service Manager

1.2 TOE Overview

1.2.1 TOE Type

The TOE is the SSR Operating System – IPOS, running on the Ericsson Smart Services Routers, as listed in section 1.1. It provides routing services in a communication network.

1.2.2 Required non - TOE hardware/software/firmware

The TOE requires physical network interfaces to be installed to communicate with external network entities. These interfaces include the line-cards, XFP's & optical connectivity devices & drivers. However, these interfaces would be outside the TOE boundary.

© Ericsson AB 2016
Ericsson Internal

1.2.3 Usage and major features of the TOE

The TOE is Ericsson IPOS, running on Smart Service Routers, as listed in section 1.1 of this document.

The TOE routes IP traffic over any type of network, with increasing scalability of the traffic volume with each TOE model. All packets on the monitored network are scanned and then compared against a set of rules that define the routing of the IP traffic.

The hardware on which the TOE runs on Ericsson Smart Service Router SSR 8020, SSR 8010 which have same functionality as far as security features are concerned. These hardware models vary in the type of physical interfaces, traffic processing capacity, memory and power consumption requirement but other functionalities, the configurations are the same.

1.2.4 Major security features of the TOE

The TOE supports the following security features:

1.2.4.1 Information Flow Function

The TOE is designed primarily to route IP network traffic. Network traffic represents information flows between source and destination network entities based on the routing configuration subject to the flow control rules.

1.2.4.2 Authentication Function

The TOE requires users to provide unique identification and authentication data (username, password) before any access to the system is granted.

The IPOS software supports four methods of user authentication:

1. local password authentication (authentication against locally stored user name & user password)

2. key based authentication (only RSA),

3. Authentication based on Remote Authentication Dial - In User Service (RADIUS)

4. Authentication based on Terminal Access Controller Access Control System plus (TACACS) which is recommended always.

© Ericsson AB 2016
Ericsson Internal

1.2.4.3 Security Management Function

The TOE restricts the ability to administer the router’s configuration entries to Restricted-admin and Administrators. The CLI provides a text based interface from which the router configuration can be managed and maintained. The following are examples of tasks that can be performed by the users from the CLI:

- Administer user attributes – create, modify or delete user accounts
- View or Manage audit logs
- Configure date/time settings
- Create, delete or modify the rules that control the presumed address from which management sessions can be established.

1.2.4.4 Audit Function

The TOE supports audit data generation for various events like successful user logins, logout, failed login attempts, configuration changes etc.

User identity association: Each audit record is associated with the identity of the user causing the event to ensure tracing the audit records against the user.

Only Restricted-operator, Operator, Restricted-admin and Administrators have the ability to review audit data from the CLI. Audit trail storage is also secured from modification by any user below Administrators.

1.2.4.5 TOE Access function

The TOE can be configured by Restricted-admin or Administrator through use of packet filters such that users can only gain access from specific management networks/stations at specific IP addresses.

All access attempts to the TOE require to pass through an authentication mechanism.

1.2.4.6 Clock Function

The clock function of the TOE provides a source of date and time information for the appliance, used in audit timestamps.

1.2.4.7 TOE Self-Test

The TOE performs a series of self-tests on startup, which checks the health of the TOE.

1.2.4.8 Trusted Recovery

The TOE high availability and process restorability are used for trusted recovery across processes and version upgrades.

1.2.4.9 Domain Separation

The TOE offers clear separation of data and control/management plane at its architecture ensuring TOE protection.

1.2.5 Operation environment of the TOE

The TOE is IPOS running in any of the Ericsson routers SSR 8020 and SSR 8010. Each SSR comes with a preloaded software version present on the RPSW card. A minimum of 1 RPSW and 1 ALSW card also termed as controller cards are required with 2 power modules and 2 fan trays to bring the TOE online. The preloaded software is the software which when upgraded brings the TOE online as mentioned in the preparatory documents of the TOE.

The major differences across the hardware models are summarized as:

Table 1 Capability comparison of the SSR models

	SSR 8010	SSR 8020
I/O Slots	10	20
Forwarding Capacity	400x1G, 100x10G, 20x40G, 10x 100G	800x1G, 200x10G, 40x40G, 20x 100G
Backplane Simplex Capacity	8 Tbps	16 Tbps
Initial Simplex Capacity	2 Tbps	4 Tbps
Full Duplex Slot Capacity*	400/100 Gbps	400/100 Gbps#

The operation environment is the conditions favorable for the TOE to be able to provide all of its security functionality, with few assumptions on physical, personnel & operational aspects of the conditions surrounding the TOE.

1.3 References

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1 Revision 4 September 2012, CCMB-2012-09-001

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1 Revision 4 September 2012, CCMB-2012-09-002

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1 Revision 4 September 2012, CCMB-2012-09-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4 September 2012, CCMB-2012-09-004

1.4 TOE Description

The TOE platforms are designed to provide an efficient and effective IP router/switch solution that can be managed centrally.

1.4.1 Smart Service Routers

IPOS running on an Ericsson SSR series routing platform is a complete routing system that supports Ethernet interfaces for medium/large networks and network applications. Ericsson routers share common IPOS software, features, and technology for compatibility across platforms.

The Smart Service Router is a carrier-class product that supports high availability and the ability to have multiple virtual routers through the configuration of “contexts”, known as a Multi-Service Edge Router (MSER), with an architecture that supports packetized traffic. This router is considered "smart" as it combines different kinds of network traffic such as mobile, video, and so on and manages them in one single router. The 3 main system components are the chassis, controller cards, and traffic cards also known as Ethernet line cards.

The Ethernet line card, along side the controller cards like the RPSW and ALSW, form a key component of a Smart Service Router. The main function of the line card is to route IP/Ethernet traffic to its destination port, which can be a different port on the same card or a different port on a different card in the same chassis. The routing task is done by the Platform Specific Packet Forwarding (NP4) hardware, and the software that controls the card runs on the RPSW card.

© Ericsson AB 2016
Ericsson Internal

The RPSW card runs the software that controls (TOE) the system and is responsible for the packet routing protocols and the IPOS command-line interface (CLI).

The architecture is a carrier-class or ISP-class product (depending on customer needs), targeted towards edge network markets. Its architecture supports packet-based IP traffic.

The router architecture of each platform cleanly separates routing and control functions from packet forwarding operations, thereby eliminating bottlenecks and permitting the router to maintain a high level of performance.

1.4.2 External IT Environment Components

The TOE can optionally use the service of external servers, for example, RADIUS and TACACS for authentication, NTP for time synchronization, Syslog for event logging. However the TOE is able to function even in the absence of these components as mentioned in the Guidance Documents. (AGD_OPE and AGD_PRE)

1.5 TOE Boundaries

The physical and logical boundaries of the TOE are described as follows.

1.5.1 Physical Boundary

The TOE is a IPOS which is a software operating within the physical boundary of the appliance.

The Ethernet Line Cards and other appliance hardware components along with their firmwares are outside the TOE boundary though they constitute the environment in which the TOE runs.

© Ericsson AB 2016
Ericsson Internal

The interfaces to the TOE are twofold: the routing interfaces and the management interfaces. The management interfaces include the TOE console interface through which the appliance can be managed locally.

The TOE ensures clear separation between control plane and data / forwarding plane. Control plane (also known as Forwarding Abstraction Layer- FABL), contains processes that implement the protocols needed for the basic functionality of system, i.e., routing protocols, BRAS protocols, AAA, configuration management, NMS and so on.

1.5.2 Logical Boundaries

The logical boundaries of the TOE are defined by the functions that can be carried out by the TOE external interfaces. These functions include network information flow control, identification and authentication for the administrative functions, access control for administrative functions, and management of the security configurations, audit and protection of the TOE itself.

Information Flow Control

The TOE is designed to forward network packets (i.e., information flows) from source network entities to destination network entities based on available routing information. This information is either provided directly by TOE users or dynamically gets generated through routing protocols.

Authentication

The TOE requires users to provide unique authentication information before any access to the system is granted. TOE provides five levels of authority to the users (in increasing level of privilege) – Non-privileged user, Restricted-Operator, Operator, Restricted-Admin, and Administrator providing administrative flexibility.

The appliances also require that applications exchanging information with them successfully authenticate prior to any exchange.

Authentication services can be handled either internally (user selected passwords) or through a RADIUS or TACACS authentication server in the IT environment (the external authentication server is considered outside the scope of the TOE). For SSH, Public Key Authentication or password can be used for the validation of the user credentials, but the user's identity and privileges are still handled internally.

Security Management

© Ericsson AB 2016
Ericsson Internal

The appliance is managed, including user management and the configuration of the router functions, through a Command Line Interface (CLI) protected by SSH. The CLI interface is accessible through SSH session, or via a local terminal console.

Audit

IPOS auditable events are stored locally in the syslog folder and although they can be sent to an external log server, the requirements for auditing are met by local storage. Audit events cover authentication activity and configuration changes. Audit logs include the date and time, event category, event type & username. An accurate time is gained by the appliance ntp daemon, acting as a client, from an NTP server in the IT environment. This external time source allows synchronization of the TOE audit logs with external audit log servers in the environment.

Protection of Security Functions

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate before any administrative operations can be performed on the system, whether those functions are related to the management of user accounts or the configuration of routes. Another protection mechanism is that all routing functions of the TOE are confined to the appliance itself.

The TOE is completely self - contained, and maintains its own execution domain as follows:

- Each sub - component of the appliance software operates in an isolated execution environment, protected from accidental or deliberate interference by others.

- The entire software environment is protected from accidental or deliberate corruption.

1.5.3 Summary of items out of the TOE boundary

There are no security functionality claims relating to the following items:

- All hardware, including that associated with forwarding interfaces & Line Cards.
- External servers (audit, NTP, authentication, FTP servers)

© Ericsson AB 2016
Ericsson Internal

2 CC Conformance

CC Identification:

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1 Revision 4 September 2012, CCMB-2012-09-001

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1 Revision 4 September 2012, CCMB-2012-09-002

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1 Revision 4 September 2012, CCMB-2012-09-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4 September 2012, CCMB-2012-09-004

This ST does not claim conformance to any PPs.

Ericsson attempts to get the IPOS certified at EAL 3. This ST has been prepared to address the EAL3 certification requirements.

© Ericsson AB 2016
Ericsson Internal

3 Security Problem Definition `

The security problem definition (SPD) specifies threats, organizational security policies and assumptions concerning the TOE. The statement of TOE security environment defines the following:

Threats to be countered by the TOE, its operational environment, or a combination of the two;

Assumptions made on the operational environment in order to be able to provide security functionality;

Organizational security policies with which the TOE, its operational environment, or a combination are to be enforced.

3.1 Threats

A threat consists of a threat agent, an asset and an adverse action of that threat agent on that asset.

- Threat agents are entities that can adversely act on assets.
- Assets are entities that someone places value upon.
- Adverse actions are actions performed by a threat agent on an asset

Table 2 Threats, Assets and Threat Definition Table

Threat Agent	Threat	Asset	Threat Definition	Adverse Effect
Unauthorized User	T.ROUTE	Routing Tables	Network packets may be routed inappropriately due to accidental or deliberate mis-configuration.	Clearing of route table entries and redirection of traffic
	T.PRIVIL	TSF Configuration Data	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data, inappropriately changing the configuration data for TOE security functions.	Unauthorized changes to router configuration causing service failure Loss of TOE users configured in management configuration
	T.INTERCEPT	TSF Configuration Data	Unauthorized change to the management traffic to/from the TOE may be made through interception of traffic on a network.	Unauthorized changes to router configuration causing service failure Loss of TOE users configured in management configuration
	T.CONFLOSS	TSF TSF Configuration Data	Failure of network components may result in loss of configuration data that cannot quickly be restored.	Unauthorized changes to router configuration causing service failure Loss of TOE users configured in management configuration Change in clock resulting in incorrect timestamps for audit logs
	T.NOAUDIT	TSF Configuration Data Audit Logs	Unauthorized changes to the TOE configurations and other management information may not be detected.	Unauthorized changes to router configuration causing service failure Loss of TOE users configured in management configuration Loss of audit logs by clearing or deleting log files Change in clock resulting in incorrect timestamps for audit logs

© Ericsson AB 2016
Ericsson Internal

3.2 Organizational Security Policies

There are no organizational security policies that the TOE must meet.

3.3 Assumptions

The following usage assumptions are made about the intended environment of the TOE.

3.3.1 Physical Assumptions

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.3.2 Personnel Assumptions

A.NOEVIL The authorized users will be competent, and not careless or willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.3.3 IT Environment Assumptions

A.EAUTH External authentication services will be available through either a RADIUS server or a TACACS server, or both.

A.TIME External NTP services will be available.

4 Security Objectives

4.1 Security Objectives for the TOE

The following security objectives are intended to be satisfied by the TOE.

Table 3 Objectives Table

O.FLOW	The TOE must ensure that network packets flow from source to destination according to defined routing information.
O.ACCESS	The TOE must only allow authorized users and processes (applications) to access protected TOE functions and data.

© Ericsson AB 2016
Ericsson Internal

O.ROLBAK	The TOE must enable rollback of router configurations to a previously stored known state.
O.AUDIT	Users must be accountable for their actions in administering the TOE.
O.ENCRYPT	Encryption of management data in a remote management session

4.2 Security Objectives for the Environment

The following security objectives for the environment of the TOE must be satisfied in order to fulfill its own security objectives.

OE.EAUTH: A RADIUS server, a TACACS server, or both must be available for external authentication services.

OE.TIME: NTP server(s) must be available to provide accurate/synchronized time services to the router.

OE.PHYSICAL: Those responsible for the TOE must ensure that the TOE is protected from any physical attack.

OE.ADMIN: Authorized users must follow all administrator guidance.

© Ericsson AB 2016
Ericsson Internal

5 Extended Component Definition

This section describes the extended components defined for the TOE.

5.1 FPT_TST_EXT

5.1.1 Requirement for the Extended Component

In order to detect integrity failures of underlying security functionalities used by the TSF, the TOE will perform self-tests.

The component described in FPT_TST family does not address the self-test feature present in the TOE. Hence the new extended component has been defined.

5.1.2 Definition

The TOE consists of a set of processes, corresponding to different functions such as – AAA, routing protocols etc. These processes are invoked by the process manager (PM). The PM checks the process binaries, before starting the processes.

Family Behavior

This family addresses the need for self test by the TOE

Component leveling

This family consists of only one component.

FPT_TST_EXT: Perform self-test
1

5.1.3 Management: FPT_TST_EXT.1

None

5.1.4 Audit: FPT_TST_EXT.1

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

Basic: Results of the tests.

5.1.5 Dependency

This extended component has no dependency and is not hierarchical to any other component.

5.1.6 FPT_TST_EXT.1.1

The TOE shall perform the POST to start the processes.

5.1.7 Testability and Traceability

This extended component can be tested, verified and could be traced through the test cases that ensures the TOE checks the binaries.

© Ericsson AB 2016
Ericsson Internal

6 IT Security Requirements

6.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, refinement and iteration.
- The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.
- The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by [*italicized text within square brackets*].
- The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment value].
- The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration sequence [letter or numeric] following the component identifier.

6.2 Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE, organized by CC class. Table 4 below identifies all SFRs implemented by the TOE. In the following table the components are listed, showing completed operations.

Table 4 Security Functional Components

Security Functional Class	Security Functional Components
Audit (FAU)	Security alarms (FAU_ARP.1)

© Ericsson AB 2016
Ericsson Internal

	Audit review (FAU_SAR.1)
	Audit data generation (FAU_GEN.1)
	User identity association (FAU_GEN.2)
	Potential violation analysis (FAU_SAA.1)
	Protected audit trail storage (FAU_STG.1)
User data protection (FDP)	Subset information flow control (FDP_IFC.1)
	Simple security attributes (FDP_IFF.1)
Identification and authentication (FIA)	User attribute definition (FIA_ATD.1)
	Authentication failure (FIA_AFL.1)
	Verification of secrets (FIA_SOS.1)
	User authentication before any action (FIA_UAU.2)
	Multiple authentication mechanisms (FIA_UAU.5)
	User identification before any action (FIA_UID.2)
Security management (FMT)	Static attribute initialization (FMT_MSA.3)
	Management of TSF data (Router/Switch configuration) (FMT_MTD.1a)
	Management of TSF data (User attributes) (FMT_MTD.1b)
	Management of TSF data (Audit logs) (FMT_MTD.1c)
	Management of TSF data (Date/time) (FMT_MTD.1d)
	Management of TSF data (Sessions) (FMT_MTD.1e)
	Specification of Management Functions (FMT_SMF.1)
	Security roles (FMT_SMR.1)
Protection of the TSF (FPT)	Time stamps (FPT_STM.1)
	Self Test (FPT_TST_EXT.1)
	Trusted recovery (FPT_RCV.2)

© Ericsson AB 2016
Ericsson Internal

	Recovery from failure (FPT_FLS.1)
	TOE session establishment (FTA_TSE.1)
TOE access (FTA)	Limit multiple concurrent sessions (FTA_MCS.1)
	Session Termination on Inactivity (FTA_SSL.3)
	Cryptographic key generation (FCS_CKM.1)
Cryptographic support (FCS)	Cryptographic key destruction (FCS_CKM.4)
	Cryptographic operation (FCS_COP.1)

6.2.1 Audit (FAU)

6.2.1.1 Security alarms (FAU_ARP.1)

FAU_ARP.1.1

The TSF shall take [create a log entry and drop connection] upon detection of a potential security violation **such as incorrect login to the router.**

6.2.1.2 Audit data generation (FAU_GEN.1)

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 **refer table 5** for the [*not specified*] level of audit; and
c) [User login/ logout;
 Login failures;
 Committing the TOE configuration;
 Changing the TOE configuration]

Table 5 ‘Auditable Event’

SFR Family	**Description**	**Audit Event ****
FAU_ARP.1	Security audit	

© Ericsson AB 2016
Ericsson Internal

	automatic response	Actions taken due to potential security violations
FAU_GEN.1	Security audit data generation	None
FAU_SAA.1	Security Audit Analysis	1) Enabling of the security profile 2) Automated responses performed by the tool.
FAU_STG.1	Security Audit event Storage	None
FDP_IFC.1	Information Flow Control policy	None
FIA_ATD.1	User Attribute definition	None
FIA_AFL.1	User Attribute definition	1) Account lock out after Consecutive 6 unsuccessful use of the authentication mechanism for the same user 2) Re-enabling of a locked account by Administrator
FIA_SOS.1	Specification of Secrets	Rejection by the TSF of any tested secret
FIA_UAU.2	User Authentication	Unsuccessful use of the authentication mechanism
FIA_UAU.5	Authentication mechanism	Authentication with external servers and local authentication within the node
FIA_UID.2	User Identification	Unsuccessful use of the user identification mechanism, including the user identity provided
FMT_MSA.3	Management of Security attributes	1) Modifications of the default setting of permissive or restrictive

		rules. 2) All modifications of the initial values of security attribute
FMT_MTD.1a FMT_MTD.1b FMT_MTD.1c FMT_MTD.1d FMT_MTD.1e	Management of TSF data	1) All modifications to the router configuration 2) User attribute modification 3) Change of time configuration
FMT_SMR.1	Security Management Roles	modifications to the group of users that are part of a role;
FMT_SMF.1	Specification of Management functions	Use of the management functions.
FPT_STM.1	Time stamps	changes to the time;
FPT_TST_EXT.1	Extended component	None
FPT_RCV.2	Trusted recovery	1) The fact that a failure or service discontinuity occurred; 2) resumption of the regular operation;
FPT_FLS.1	Fail Secure	Failure of the TSF
FTA_MCS.1	TOE session establishment	Denial of a session establishment due to maximum number of concurrent sessions is reached
FTA_SSL.3	Session termination on inactivity	Termination of an interactive session by the session locking mechanism

** - Whatever is the configuration change made to the TOE, the event type will indicate only "configuration change" and will not indicate the exact changes made to the TOE.

FAU_GEN.1.2

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

Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST [no additional information].

6.2.1.2 User identity association (FAU_GEN.2)

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.

6.2.1.3 Potential violation analysis (FAU_SAA.1)

FAU_SAA.1.1

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [failed authentication attempt events] known to indicate a potential security violation;

b) [No other events].

6.2.1.4 Audit review (FAU_SAR.1)

FAU_SAR.1.1

The TSF shall provide [Restricted-operator, Operator, Restricted-admin, Administrator] with the capability to read [all information] 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.

6.2.1.5 Protected audit trail storage (FAU_STG.1)

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*] unauthorized modifications to the stored audit records in the audit trail.

6.2.2 User data protection (FDP)

6.2.2.1 Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1

The TSF shall enforce the [UNAUTHENTICATED SFP] on

a [subjects:
  - Unauthenticated external IT entities that send and receive packets through the TOE to one another;

b information (packets):
  - Network packets sent through the TOE from one subject to another;

c operation:
  - Route packets].

6.2.2.2 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1

The TSF shall enforce the [UNAUTHENTICATED SFP] based on the following types of subject and information security attributes: [

a subject security attributes:
  - Presumed address

b information security attributes:
  - Presumed address of source subject

© Ericsson AB 2016
Ericsson Internal

- Presumed address of destination subject
- Network layer protocol (OSPF, BGP, RIP, LDP)
- TOE interface on which packet arrives and departs

]

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:

a [subjects on a network can cause packets to flow through the TOE to another connected network if:

all the packet security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the packet security attributes, created by the authorized user;

The presumed address of the source subject, in the packet, is consistent with the network interface it arrives on;

The presumed address of the destination subject, in the packet, can be mapped to a configured nexthop].

FDP_IFF.1.3

The TSF shall enforce the [no additional UNAUTHENTICATED SFP rules].

FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules: [no additional rules that explicitly authorize information flows].

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [no additional rules that explicitly deny information flows].

6.2.3 Identification and authentication (FIA)

6.2.3.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [

a User identity;

b Authentication data;

c Privileges].

6.2.3.2 Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [password – Alpha-numeric-special character string of length minimum 8 characters excluding control characters].

6.2.3.3 User authentication before any action (FIA_UAU.2)

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.

6.2.3.4 User identification before any action (FIA_UID.2)

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.

6.2.3.5 Authentication failure (FIA_AFL.1)

FIA_AFL.1.1

The TSF shall detect when [*6*]consecutive unsuccessful authentication events occur related to [login of any level of user].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [*met*] the TSF shall [lock the user account].

© Ericsson AB 2016
Ericsson Internal

6.2.3.6 Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1

The TSF shall provide [internal password mechanism, SSH public key and external server (RADIUS or TACACS) mechanism] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [authentication mechanism specified by Administrator].

6.2.4 Security management (FMT)

6.2.4.1 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1

The TSF shall enforce the [UNAUTHENTICATED SFP] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [Restricted-admin and Administrator] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.2 Management of TSF data (Router/Switch configuration) (FMT_MTD.1a)

FMT_MTD.1.1a

The TSF shall restrict the ability to [*modify*] the [router configuration data] to [Restricted-admin, Administrators].

6.2.4.3 Management of TSF data (User attributes) (FMT_MTD.1b)

FMT_MTD.1.1b

The TSF shall restrict the ability to [*modify*] the [user account attributes] to [Administrators].

© Ericsson AB 2016
Ericsson Internal

6.2.4.4 Management of TSF data (Audit logs) (FMT_MTD.1c)

FMT_MTD.1.1c

The TSF shall restrict the ability to [*delete*] the [audit logs] to [Administrators].

6.2.4.5 Management of TSF data (Date/time) (FMT_MTD.1d)

FMT_MTD.1.1d

The TSF shall restrict the ability to [*modify*] the [NTP Server address] to [Restricted-admin, Administrator].

6.2.4.6 Management of TSF data (Sessions) (FMT_MTD.1e)

FMT_MTD.1.1e

The TSF shall restrict the ability to [*modify*] the [rules that restrict the ability to establish management sessions] to [Restricted-admin and Administrator].

6.2.4.7 Security roles (FMT_SMR.1)

FMT_SMR.1.1

The TSF shall maintain the privilege levels to differentiate [Non-privileged user, Restricted-operator, Operator, Restricted-admin and Administrator [Non-privilege user, restricted operator, Operator, Restricted Admin, Administrator as defined in Table 6]

The TSF supports 5 types of user levels as described below:

Table 6 User Levels

User role[1]	Privilege Level	Operations
Non-privileged user	0 - 2	• Escalate own privilege by "enable" command if permitted
Restricted-Operator	3 - 6	• Show commands
Operator	7 - 9	All actions as Restricted-Operator + • Enter Exec mode (though can not perform

		anything in that mode
Restricted-Admin	10 - 14	All actions as operator + • Change configuration • Rename files
Administrator	15	All actions of Restricted-Admin + • Change User Attributes • Create Another Administrator • Copy/edit/delete Files

[1] User roles are classified logically – as per their functions / privilege and do not reflect in the configuration file

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.4.8 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions:

[

- Configuring Management Access
- Configuring IP ACL Filters
- Configuring Login control (authentication method to use: local/radius, ssh server attributes etc.)
- Configuring RADIUS/TACACS
- Configuring SNMP/ Syslog
- Configuring NTP
- Session limit per administrative user

All the above functions can be carried out by Restricted-Admin or Administrator

- Configuring Administrators in local and non-local context;
- Configuring user account attributes like privilege levels;
- Copying and Overwriting Administrators and user attributes;

The above functions can be performed only by Administrator].

© Ericsson AB 2016
Ericsson Internal

6.2.5 Protection of the TOE security functions (FPT)

6.2.5.1 Time stamps (FPT_STM.1)

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

6.2.5.2 Self Test (FPT_TST_EXT.1)

FPT_TST_EXT.1.1

The TSF shall run a suite of self tests [*during initial start-up*] to demonstrate the correct operation of [parts of the TSF as below]

- The POST shall run a list of process during the startup.

6.2.5.3 Fail Secure (FPT_RCV.2)

FPT_RCV.2.1

When automated recovery from [TOE failure] is not possible, the TSF shall enter a maintenance mode [like under].

- Manual maintenance of reloading the TOE

FPT_RCV.2.2

For [service discontinuities] the TSF shall ensure the return of the TOE to a secure state using automated procedures [like under]

- Switchover (High availability feature)
- Process restart

6.2.5.4 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1

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

- Controller card failure

© Ericsson AB 2016
Ericsson Internal

- Process termination]

6.2.6 TOE access (FTA)

6.2.6.1 Basic limitation on multiple concurrent sessions (FTA_MCS.1)

FTA_MCS.1.1

The TSF shall restrict the maximum number of concurrent sessions.

FTA_MCS.1.2

The TSF shall enforce by default session limit per user [10 total maximum numbers, which is configurable up to 32] sessions irrespective of the user accounts.

6.2.6.2 Session termination on Inactivity (FTA_SSL.3)

FTA_SSL.3.1

The TSF shall terminate an interactive session after a [3 minutes of user inactivity].

6.2.6.3 TOE session establishment (FTA_TSE.1)

FTA_TSE.1 1

The TSF shall be able to deny session establishment based on originating address

6.2.7 [Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation - DSA (Digital Signature Algorithm), DH (Diffie-Hellman exchange)

FCS_CKM.1.1(1) SH Symmetric Key Derivation

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Diffie-Hellman group 1, Diffie-Hellman group 14] and specified cryptographic key sizes [1024, 2048] that meet the following: [SSHv2 Standards:RFC4251, RF 4252, RFC 4253].

© Ericsson AB 2016
Ericsson Internal

FCS_CKM.1.1 (2): SSH DSA Asymmetric Key pair

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithms [DSA and RSA] and specified cryptographic key sizes [1024] that meet the following: [FIPS 186-2: US National Institute of Standards and Technology [Digital Signature Standard (DSS)].

FCS_CKM.4 Cryptographic key Destruction

FCS_CKM.4.1 (1): Symmetric key destruction

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

FCS_CKM.4.1 (2): Asymmetric key destruction

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

6.2.7 FCS_COP.1.1 (1): Cryptographic Operation (for data encryption/decryption)

The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [AES operating in [**ECB, CBC mode**], 3DES-cbc] and cryptographic key sizes 128-bits, 192bits or 256-bits, and [***168 bits***] that meet the following:

- FIPS PUB 197, 'Advanced Encryption Standard (AES)'
- FIPS 46-3 with Keying Option 1

6.2.8 FCS_COP.1.1 (2): Cryptographic Operation (for cryptographic signature)

The TSF shall perform cryptographic signature services in accordance with a [**DSA Digital Signature Algorithm with key length 1024 bit**] that meets the following: [**FIPS PUB 186-3, 'Digital Signature Standard'**]

© Ericsson AB 2016
Ericsson Internal

6.2.9 FCS_COP.1.1 (3): Cryptographic Operation (for keyed-hash message authentication)

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-[***SHA-1***], key size [**160 bits**], and message digest sizes [***160***] bits that meet the following: FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code', and FIPS Pub 180-3, 'Secure Hash Standard.'

6.3 Security Assurance Requirements

The following table describes the TOE security assurance requirements drawn from Part 3 of the CC.

Table 7 Security Assurance Requirements

Assurance Class	Assurance Components
Security Target (ASE)	*ST introduction (ASE_INT.1)*
	Conformance claims (ASE_CCL.1)
	Security problem definition (ASE_SPD.1)
	Security objectives (ASE_OBJ.2)
	Extended components definition (ASE_ECD.1)
	Derived security requirements (ASE_REQ.2)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	*Security architecture description (ADV_ARC.1)*
	Functional specification with complete summary (ADV_FSP.3)
	Architectural design (ADV_TDS.2)
Guidance documents (AGD)	*Operational user guidance (AGD_OPE.1)*
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	*Authorization controls (ALC_CMC.3)*
	Implementation representation CM coverage (ALC_CMS.3)
	Delivery procedures (ALC_DEL.1)
	Identification of security measures (ALC_DVS.1)

	Developer defined life-cycle model (ALC_LCD.1)
Tests (ATE)	*Analysis of coverage (ATE_COV.2)*
	Testing: basic design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment (AVA)	*Vulnerability analysis (AVA_VAN.2)*

7 TOE Summary Specification

7.1 TOE Security Functions

7.1.1 Information Flow Function

FDP_IFC.1 Subset information flow control and FDP_IFF.1 Simple security attributes

The TOE is designed primarily to route unauthenticated network traffic. Network traffic represents information flows between source and destination network entities. The specific routing of traffic is based on the routing configuration data that has been created by the TOE users or has been collected (e.g., OSPF, RIP, LDP, BGP) from network peers as defined by the TOE users. The routing decision is based on the presumed source and destination IP address of the packet, the network layer protocol, service and the interface on which the packet arrives and is to depart on.

7.1.2 Identification and Authentication Function

FIA_ATD.1 User Attribute Definition

User accounts in the TOE have the following attributes: user name, authentication data (password, public key) and privilege (user class). The Administrator can delegate the authentication process to a RADIUS or TACACS server or Local to the router.

If the user account is authenticated locally via ssh then, either public key or password has to be successful to gain access to the TOE. For Local authentication via console, password authentication is required to gain the access to the TOE

If a user is authenticated remotely then, the packets with the relevant user credentials are sent by the TOE towards the external authentication server (Radius or TACACS+). When the authentication server successfully authenticates the user they pass the unique username to the TOE. The user name that was authenticated is used when generating audit records regarding activity by that user.

FIA_SOS.1 Verification of secrets

Locally stored authentication data for password authentication is a case−sensitive, alphanumeric value. The password is an alphanumeric string excluding control characters having a minimum length of 8 characters. This password is digested in the configuration repository. SSH keys are stored in the local flash on RPSW card.

Remotely stored authentication data i.e. on Radius or TACACS is subject to the password requirements of those machines as described in the preparatory documents for TOE.

FIA_UAU.2 User authentication before any action, FIA_UAU.5 Multiple authentication mechanisms and **FIA_UID.2 User identification before any action**

The TOE requires users to provide unique identification and authentication data (password or SSH public key) before any administrative access to the system is granted.

The IPOS software supports four methods of user authentication: local password authentication, key based authentication (only RSA), Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS).

With local authentication, a password or public key is configured for each user allowed to log into the router. RADIUS and TACACS are authentication methods for validating users who attempt to access the router

If the identity specified is defined locally, the TOE can successfully authenticate that identity if the authentication data provided matches that stored in conjunction with the provided identity. Alternately, if the TOE is configured to work with a RADIUS or TACACS server, the identity and authentication data is provided to the server and the TOE enforces the result returned from the server. Regardless, no administrative actions are allowed until successful authentication as an authorized administrator.

It should be noted that when RADIUS and/or TACACS are used for authentication and the TOE can verify the remote authentication server with the correct IP address configured in the TOE.

The TOE can be configured to allow users to be authenticated via RADIUS and/or TACACS. The order in which authentication mechanisms are attempted is applied to all users. The configuration can also specify that local passwords and keys stored in the TOE can be used when external authentication servers are unavailable, or as a general fallback. For local ssh based authentication user authentication to the TOE, public key based authentication will be the attempted first and if unsuccessful, then the password based authentication will be attempted.

Local authentication using the SSH application utilizes the user’s public key stored on the appliance to both establish the SSH session and to authenticate the user to the CLI.

Irrespective of what access method is used for management sessions, successful authentication is required prior to giving a user access to the system. These mechanisms are used for administration of the routing functions as well as the administration of the user accounts used for management.

Authentication data can be stored either locally or on a separate server. The separate server must support either the RADIUS or TACACS protocols to be supported by the TOE.

7.1.3 FIA_AFL.1 Authentication failure

TOE has the capability to detect 6 unsuccessful SSH authentication events in the node. Unsuccessful login attempt to a TOE can be due to the mismatch in keys, or password or username. Upon such instances the user account gets locked.

The locked user account can be unlocked by any administrative user. The Locked user account can also be unlocked automatically after 5 minutes of time.

7.1.4 Security Management Function

The TOE is designed in such a way where every user account having association with the privilege level and every action of the user could be authorized by sending authorization request to local or external AAA servers & obtaining the authorization information for the user. Only after successful authorization of the privilege level associated with the user, execution of enabling or disabling or to modify any configurations (these configuration could even be the controlling of how authentication or authorization and auditing itself is done by the TOE), towards managing security functions.

© Ericsson AB 2016
Ericsson Internal

The TOE restricts to Administrator the ability to add or delete users, modify their access permissions or manage authentication attributes.

The management functions are as follows:

- Configuring Management Access;
- Configuring IP ACL Filters;
- Configuring Administrators;
- Configuring user attributes;
- Copying and Overwriting Administrators and user attributes;
- Configuring Login control;
- Configuring RADIUS/TACACS;
- Configuring SNMP/Syslog;
- Configuring NTP;

FMT_MSA.3 Static attribute initialization

TOE allows by default packet flow between any ingress port and egress port of the node on the basis of source IP address, destination IP address, network layer control packets etc.

The default behavior can be changed or modify by configuring security policies within the TOE to allow and restrict certain types of packets as per the requirement.

FMT_MTD.1a Management of TSF Data (Router/Switch Information)

The TOE restricts the ability to administer the router configuration data. The CLI provides a text - based interface from which the router configuration can be managed and maintained. From this interface all TOE functions, such as BGP, RIP and MPLS protocols can be managed, as well as TCP/IP configurations and date/time. The TOE automatically routes traffic based on available routing information, much of which is automatically collected from the TOE environment.

FMT_MTD.1b Management of TSF Data (User Data)

© Ericsson AB 2016
Ericsson Internal

The TOE restricts the ability to administer user data to only Administrators. The CLI provides admin - users with a text - based interface from which all user data can be managed. From this interface new accounts can be created, and existing accounts can be modified or deleted. User accounts created with administrative privilege in a non-local context cannot modify the user attributes of another user account as Administrator in another non-local context. The user account created as an Administrator in context local however has the ability to change attributes of all user accounts in all contexts. This interface also provides the Administrator with the ability to configure an external authentication server, such as a RADIUS or TACACS server. When this is assigned, a user can be authenticated to the external server instead of directly to the TOE. If authentication - order includes RADIUS and/or TACACS, then these will be consulted in the configured order for all users. Typically, local password is only used as a fallback in such cases.

FMT_MTD.1c Management of TSF Data (Audit logs)

The user account (administrator) logged into TOE can delete logs manually.

FMT_MTD.1d Management of TSF Data (Date/time)

The TOE will allow only a Restricted-admin or Administrator to modify the date/time setting on the appliance.

FMT_MTD.1e Management of TSF Data (Sessions)

The TOE will allow only a Restricted-admin or Administrator to create, delete or modify the rules that control the presumed address from which management sessions can be established.

FMT_SMF.1 Management of Security Functions

The TOE provides the ability to manage the following security functions:

User authentication (authentication data, roles);

TOE information related to software;

Audit management and review;

Modify the time;

Session establishment restrictions.

FMT_SMR.1 Security Roles

The TOE has privilege levels defined per user. When a new user account is created, it must be assigned one of the privilege levels.

- Administrator (privilege level 15): User with this privilege level
    - Can perform all management functions on the TOE.
    - Can manage user accounts (create, delete, modify), view and modify the TOE configuration information.
- Restricted-admin (privilege level 10 to 14): User with this privilege level
    - Can read some configuration data
    - Can modify existing configuration of the TOE other than that of other user accounts.
    - Can view audit records.
- Operator (privilege level 7 to 9): User with this privilege level
    - Can read some configuration data
    - Can view audit records
    - Can enter exec mode
- Restricted-operator (privilege level 3 to 6): User with this privilege level
    - Can read some configuration data
    - Can view audit records.
- Non-privileged user (privilege level 0 to 2): User with this privilege level
    - Cannot view configuration or audit records

7.1.5 Audit Function

FAU_GEN.1 Audit data generation

IPOS creates and stores audit records for the following events:

- User login/logout;
- Login failures;
- Configuration is committed;
- Configuration is changed.

Startup and shutdown of auditing function is not supported on the TOE. Auditing is enabled by default and cannot be disabled.

© Ericsson AB 2016
Ericsson Internal

FAU_GEN.2 User identity association

IPOS will record within each audit record the following information:

Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and Identity of the user causing the event.

FAU_SAR.1 Audit review

IPOS provides Restricted-operator, Operator, Restricted-admin, Administrator users with the ability to display audit data from the CLI. Commands are available to list entire files, or to select records that match or do not match a pattern. Records can also be saved to files for further analysis offline

FAU_STG.1 Protected audit trail storage

Audit records are stored in files. Both the files and that directory are only modifiable by the Administrators.

FAU_ARP.1 Security alarms

The daemons that authenticate the users if notices 3 successive login failures will generate an audit log message and close the session.

FAU_SAA.1 Potential violation analysis

The daemons authenticating users to IPOS perform analysis of the failed authentication attempts to identify activity indicating a potential violation. The following patterns of activity are defined to represent a potential violation and the action specified is triggered:

After 6 successive login failures the user account is locked.

The TOE can also be configured to display selected audit events as they occur.

7.1.6 TOE Access Function

FTA_TSE.1 TOE session establishment

The TOE can be configured by a Restricted-admin or Administrator through use of packet filters (Access Control List) such that users can only gain access from specific management networks/stations at specific IP addresses.

FTA_MCS.1 Maximum number of concurrent sessions

© Ericsson AB 2016
Ericsson Internal

The TOE allows a maximum of 10 concurrent sessions for every user account by default, which is configurable up to 32 sessions. The TOE also will ensure that a total of 32 active sessions are allowed at any point of time for all the user accounts.

FTA_SSL.3 Session termination on user inactivity

As part of The TOE feature, any idle SSH session will get terminated after 3 minutes of inactivity.

7.1.7 Clock function

FPT_STM.1 Time stamps

The clock function of the TOE provides a source of date and time information for the appliance, used in audit timestamps. The clock function is reliant on the system clock provided by the underlying hardware.

For better accuracy of timestamp and synchronization of time across devices in the IT environment, an external NTP server can be deployed. In such deployments the audit timestamps will be synchronized with external syslog servers, if configured

7.1.8 Trusted Recovery

FPT_RCV.2 Trusted Recovery

The TOE high availability (switchover) and process restorability are used for trusted recovery across processes and version upgrades.

- When there is a failure on the RPSW and ALSW card that is detected by the TOE there is an automatic recovery by switchover
- Whenever a process malfunction, PM kills the process and restarts the same along with a crash dump generation of the process
- When there is a router reload the system is automatically restored to the previous system state based on the boot configuration
- For cases where automatic recovery is not possible such as hardware failure of controller and line cards, manual intervention is needed to rel-load the TOE

7.1.9 Self-Test

FPT_TST_EXT.1

TOE performs a self-test after initial loading to detect the integrity failure of processes. Each process in the TOE corresponds to one specific independent function like AAA, routing protocols etc. All the processes available in the TOE are being invoked by the Process Manager. All the processes are different daemon and are independently compiled within the binaries. Failure of any process would result in malfunction in certain functionalities within the TOE. Hence during self-Test the functioning of each process is verified to maintain the integrity of the ToE.

7.1.10 Fail Secure

FPT_FLS.1 Failure with preservation of secure state

When there are switchovers such as RPSW switchover, the TOE recovers the current running state. There are a many hardware and software features that promote high availability and redundancy:

- Redundant Hot standby RPSW controller card with hitless fail over and no interruption to traffic forwarding and subscriber sessions

- When one of the processes get killed, the system automatically detects the condition and restarts the process

7.1.11 Protection of the TSF

The TOE implements secure shell (SSH) as a remote access mechanism using DSA key generation and 168 bit 3DES or 128, 192 or 256 bits AES encryption. This protects all the exchanges between the TOE and the remote management client from reading or modification by any other entity in the network. Remote management via SSH provides access to the management CLI. When new cryptographic keys are generated, the old ones are overwritten.

FCS_CKM.1

The TOE is having the capability to generate SSH Symmetric key derivation and SSH DSA Asymmetric Key pair. TOE can generate SSH Symmetric cryptographic keys in accordance to the Key generation algorithm of Diffie-Hellman group 1,Diffie-Hellman group 14.The cryptographic key sizes [1024, 2048] meet the following: [SSHv2 Standards:RFC4251, RF 4252, RFC 4253].

Also for DSA Asymmetric algorithm the TOE can generate keys with a specified cryptographic key generation algorithm [DSA] and specified cryptographic key sizes [1024] that meet the following: [FIPS 186-2: US National Institute of Standards and Technology "“ Digital Signature Standard".

FCS_CKM .4

The TOE destroys the cryptographic keys by overwriting the old existing key with the newly generated key.

FCS_COP.1

The TOE performs cryptographic signature services in accordance with a DSA [Digital Signature Algorithm] with key of 1024 bit. The TOE also support keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-[***SHA-1***], key size [**160 bits]**

8 Rationale

This section provides the rationale for completeness and consistency of the security target. The rationale addresses the following areas:

- Security objectives
- Security functional requirements
- Security assurance requirements
- Dependencies

8.1 Rationale for Security Objectives

This section shows that all assumptions and threats are countered by security objectives, and that each security objective addresses at least one assumption or threat.

8.1.1 Rationale for Security Objectives for the TOE

This section provides a mapping of TOE security objectives to those threats that the TOE is intended to counter, and to those assumptions that must be met.

Table 8 TOE Security Objectives Rationale

	T.ROUTE	T.PRIVIL	T.INTERCEPT	T.CONFLOSS	T.NOAUDIT
O.FLOW	✓				
O.ACCESS		✓			
O.ENCRYPT			✓		
O.ROLBAK				✓	
O.AUDIT					✓

O.FLOW: This objective helps to counters the threat T.ROUTE through the use of routing tables to correctly route information.

O.ACCESS: This objective addresses the need to protect the TOE’s operations and data against unauthorized access (T.PRIVIL)

O.ENCRYPT: This objective address the need to prevent the interception of the remote management data by encrypting the remote management data (T.INTERCEPT)

O.ROLBAK: The objective to restore previous configurations helps recover from loss of configuration data (T.CONFLOSS)

O.AUDIT: This objective serves to discourage and detect inappropriate use of the TOE (T.NOAUDIT)

O-PROTECT: This objective is to prevent unauthorized users from gaining accessing to the TOE’s configuration data (T.PROTECT)

8.1.2 Rationale for Security Objectives for the Environment

This section provides a mapping of environment security objectives to those threats that the environment is expected to counter, and to those assumptions that must be met.

© Ericsson AB 2016
Ericsson Internal

Table 9 Environment Security Objectives Rationale

	A.LOCATE	A.NOEVIL	A.TIME	A.EAUTH
OE.PHYSICAL	✓			
OE.ADMIN		✓		
OE.TIME			✓	
OE.EAUTH				✓

OE.EAUTH: The objective to have a AAA server (RADIUS / TACACS) in the TOE environment for external Authentication, Authorization and Accounting (A.EAUTH).

OE.TIME: The objective to have an NTP server in the TOE environment supports the assumption (A.TIME) that time services are available to provide the appliance with accurate/synchronized time information.

OE.PHYSICAL: The objective to provide full physical protection for the TOE supports the assumption that the TOE will prevent unauthorized physical access (A.LOCATE).

OE.ADMIN: The objective that users should follow administrator guidance supports the assumption that they will not be careless, willfully negligent or hostile (A.NOEVIL).

© Ericsson AB 2016
Ericsson Internal

8.2 Rationale for Security Requirements

8.2.1 Rationale for TOE Security Functional Requirements

This section demonstrates that all security objectives for the TOE are met by security functional requirements for the TOE, and that each security functional requirement for the TOE addresses at least one security objective for the TOE. The functional requirements are mutually supportive, and their combination meets the security objectives. Table 8 and Table 9 demonstrate the relationship between the threats and assumptions and the security objectives. Table 10 illustrates the mapping between security functional requirements and security objectives for the TOE. Together these tables demonstrate the completeness and sufficiency of the requirements.

Table 10 Security Functional Requirements Rationale

	O.FLOW	O.ACCESS	O.ROLBAK	O.AUDIT	O.ENCRYPT
FAU_ARP.1				✓	
FAU_GEN.1				✓	
FAU_GEN.2				✓	
FAU_SAA.1				✓	
FAU_SAR.1				✓	
FAU_STG.1				✓	
FDP_IFC.1	✓				
FDP_IFF.1	✓				
FIA_ATD.1		✓		✓	
FIA_SOS.1		✓			
FIA_AFL.1		✓			
FIA_UAU.2		✓			
FIA_UAU.5		✓			
FIA_UID.2		✓			
FMT_MSA.3		✓			
FMT_MTD.1a	✓				
FMT_MTD.1b		✓			
FMT_MTD.1c				✓	
FMT_MTD.1d				✓	

© Ericsson AB 2016
Ericsson Internal

FMT_MTD.1e		✓			
FMT_SMF.1		✓		✓	
FMT_SMR.1		✓		✓	
FPT_STM.1				✓	
FTA_TSE.1		✓			
FTA_MCS.1		✓			
FTA_SSL.3		✓			
FPT_RCV.2			✓		
FPT_FLS.1			✓		
FCS_CKM.1					✓
FCS_CKM.4					✓
FCS_COP.1					✓
FPT_TST_EXT.1			✓		

FAU_ARP.1 This component takes action following detection of potential security violations, and therefore contributes to meeting O.AUDIT.

FAU_GEN.1 This component outlines what events must be audited, and aids in meeting O.AUDIT.

FAU_GEN.2 This component required that each audit event be associated with a user, and aids in meeting O.AUDIT.

FAU_SAA.1 This component helps to detect potential security violations, and aids in meeting O.AUDIT.

FAU_SAR.1 This component requires that the audit trail can be read, and aids in meeting O.AUDIT.

FAU_STG.1 This component requires that unauthorized deletion of audit records does not occur, and thus helps to maintain accountability for actions, as required by O.AUDIT.

© Ericsson AB 2016
Ericsson Internal

FDP_IFC.1 this component identifies the entities involved in the UNAUTHENTICATED information flow SFP (i.e. external IT entities sending packets), and aids in meeting O.FLOW.

FDP_IFF.1 This component identifies the conditions under which information is permitted to flow between entities (the UNAUTHENTICATED SFP), and aids in meeting O.FLOW.

FIA_ATD.1 This component specifies that individual user attributes to be maintained and aids in meeting O.ACCESS and O.AUDIT.

FIA_AFL.1 This component protects against repeated unauthorized access attempts and hence helps meeting O.ACCESS.

FIA_SOS.1 This component specifies metrics for authentication, and aids in meeting objectives to restrict access O.ACCESS

FIA_UAU.2 This component ensures that users are authenticated to the TOE. As such it aids in meeting objectives to restrict access and aids in meeting O.ACCESS

FIA_UAU.5 This component was selected to ensure that appropriate authentication mechanisms can be selected. As such it aids in meeting objectives to restrict access O.ACCESS.

FIA_UID.2 This component ensures that users are identified to the TOE. As such it aids in meeting objectives to restrict access O.ACCESS.

FMT_MSA.3 This component ensures that there is a default deny policy for the information flow control security rules. As such it aids in meeting O.ACCESS.

FMT_MTD.1a This component restricts the ability to modify routing configuration details, and as such aids in meeting O.FLOW.

FMT_MTD.1b This component restricts the ability to modify identification and authentication data, and as such aids in meeting O.ACCESS.

FMT_MTD.1c This component restricts the ability to delete audit logs, and as such contributes to meeting O.AUDIT.

FMT_MTD.1d This component restricts the ability to modify the date and time, and as such contributes to meeting O.AUDIT.

FMT_MTD.1e This component restricts the ability to modify the data relating to TOE access locations, and as such contributes to meeting O.ACCESS.

FMT_SMF.1 This component lists the security management functions that must be controlled. As such it aids in meeting O.ACCESS and O.AUDIT.

© Ericsson AB 2016
Ericsson Internal

FMT_SMR.1 Each of the components in the FMT class listed above relies on this component (apart from FMT_MSA.3). It defines the roles on which access decisions are based. As such it aids in meeting, O.ACCESS and O.AUDIT.

FPT_STM.1 This component ensures that reliable time stamps are provided for audit records and aids in meeting O.AUDIT.

FPT_RCV.2 This component ensures that reliable recovery mechanism is performed in meeting O.ROLBAK

FPT_FLS.1 This component ensures that reliable recovery is performed under certain hardware and software failures and helps meeting O.ROLBAK. It also helps in rolling back to a previously saved configuration thus helping meet the O.ROLBACK objective.

FTA_TSE.1 This component limits the range of locations from which a user session can be established, and hence reduces the chance of unauthorized access. It aids in meeting O.ACCESS.

FTA_MCS.1 This component limits the number of sessions a user can establish, and hence reduces the chance of unauthorized access. It aids in meeting O.ACCESS.

FTA_SSL.3 This self-terminates idle sessions after a timeout, and hence reduces the chances of unauthorized access via unattended sessions. This helps meeting O.ACCESS.

FCS_CKM.1 & FCS_CKM.4 Defines cryptographic key management functions, namely the generation and destruction of keys. These key management secures the cryptographic operations and hence meets objective O.ENCRYPT

FCS_COP.1 is the actual cryptographic operation that secures the communication between the TOE and users, meeting the objective O.ENCRYPT

FPT_TST_EXT.1 This component ensures that reliable self test are performed and aids in meeting O.ROLBAK

8.3 Rationale for Security Assurance Requirements (SAR)

The TOE meets the independent security assurance requirements EAL3 of CC3 part3 version 3.1 revision 4

© Ericsson AB 2016
Ericsson Internal

Table 11 Describes the relationship between the evaluation assurance levels and the assurance classes, families and components.

Assurance class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level 3**
Development	ADV_ARC	1
	ADV_FSP	3
	ADV_TDS	2
Guidance documents	AGD_OPE	1
	AGD_PRE	1
Life-cycle support	ALC_CMC	3
	ALC_CMS	3
	ALC_DEL	1
	ALC_DVS	1
	ALC_LCD	1
Security Target evaluation	ASE_CCL	1
	ASE_ECD	1
	ASE_INT	1
	ASE_OBJ	2
	ASE_REQ	2
	ASE_SPD	1
	ASE_TSS	1
Tests	ATE_COV	2
	ATE_DPT	1
	ATE_FUN	1
	ATE_IND	2
Vulnerability assessment	AVA_VAN	2

© Ericsson AB 2016
Ericsson Internal

8.3.1 Dependencies Rationale

All functional and assurance requirements dependencies indicated in [CC2] and [CC3] have been satisfied, with the exception of the dependency of FMT_MSA.3 on FMT_MSA.1. The requirement for FMT_MSA.3 is included as a dependency from FDP_IFF.1, to specify how the security attributes associated with the information flow rules are initialized. The subsequent dependency from FMT_MSA.3 on FMT_MSA.1 allows for the specification of the management of the security attributes. However, for this TOE the management of the information flow security attributes is specified using FMT_MTD.1a. Therefore, there is no need to include FMT_MSA.1 as FMT_MTD.1a has satisfied the intent of the dependency.

No additional dependencies have been identified. Dependencies on FIA_UAU.1 and FIA_UID.1 have been satisfied through inclusion of the hierarchical components FIA_UAU.2 and FIA_UID.2, respectively.

FAU_GEN.2 is dependent on FIA_UID.1, which is satisfied through inclusion of the hierarchical component FIA_UID.2

© Ericsson AB 2016
Ericsson Internal

9 Acronyms

Table 11 Acronyms

AAA	Authentication Authorization Auditing
ACL	Access Control List
ACM	Access Control Management
AGD	Administrator Guidance Document
ALD	Adaptation Layer
ALSW	Alarm Switch
API	Application Programming Interface
BGP	Border Gateway Protocol
CC	Common Criteria
CLI	Command Line Interface
CM	Control Management
DAC	Discretionary Access Control
DPC	Dense Port Concentrators
EAL	Evaluation Assurance Level
FABL	Forward Abstraction Layer
FALD	Forward Adaptation Layer
FTP	File Transfer Protocol
I/O	Input/Output
IPOS	Internet Protocol Operating System
IS-IS	Intermediate System to Intermediate System
LDP	Label Distribution Protocol
NP4	Network Processor 4
NTP	Networking Timing Protocol
OSPF	Open Shortest Path First
PFE	Packet Forwarding Engine
PIM	Protocol Independent Multicast
PP	Protection Profile
PPA4	Packet Processing ASIC
RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol
RIP	Route Information Protocol
RPSW	Route Processor Switch
SF	Security Functions
SFR	Security Functional Requirements
SNMP	Simple Network Management Protocol
SPD	Security Problem Definitioin
SSH	Secure Shell
SSR	Smart Service Router
ST	Security Target

© Ericsson AB 2016
Ericsson Internal

TACACS	Terminal Access Controller Access Control System Plus
TDM	Time Division Multiplex
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
XFP	Optical Transceiver

© Ericsson AB 2016
Ericsson Internal