Security Target

Nokia
9500 Microwave Packet Radio (MPR) R8.0.1
V1.07

Ref :3DB19413ACAADTZZA

Table of Contents

List of Tables

List of Figures

1. Security Target Introduction

This document is the Security Target for the Common Criteria evaluation of the Nokia 9500 Microwave Packet Radio (MPR).
The 9500 MPR product has been initially certified by ANSSI reference ANSSI-CC-2017/57 the 5th of October 2017.
This new Security Target insert the possibility to manage the restart function in case the Network Management is reaching the Neighboring equipment using the radio link as per described in System Overview/system architecture alternative.1.4.2.

The 9500 MPR is based on two systems:

a) MSS (Microwave Service Switch), which acts as a traffic aggregator equipment capable of aggregating any kind of incoming traffic into an Ethernet fabric, to be transported on any kind of microwave uplink (TDM/Ethernet or fully integrated MPT);
b) MPT (Microwave Packet Transport) which is a radio based on packet

Layer 1 encryption provides end-to-end protection against loss of confidentiality along the radio. Encryption at this layer also allows independence in the selection of protocols or applications used at higher layers, as well as lower encryption latency.
The MSS (Multi Service Switch) can support up to 24 radios transceivers (MPTs) pointing in same or different directions.
The MPT is a packet radio able to transport up to 500 Mb/s over the air. The maximum throughput depends on the Channel Spacing. The MPT provides Advanced Encryption Standard (AES) 256 encryption

1.1 Security Target Identification

Name:	Security Target Nokia 9500 Microwave Packet Radio (MPR)
Version:	1.07
Publication Date:	11 June 2020
Author:	Nokia Wireless Transmission Division

1.2 TOE Identification (*)

Name:	9500 Microwave Packet Radio (MPR)
Version:	R8.0.1 (Software package – V08.00.1W and EC = V35.41.20
Sponsor:	Nokia
Developer:	Nokia
Keywords:	Microwave, radio, switch, multi-service, encryption

(*): The TOE is identified by a commercial release number (here R8.0.1) make by a software package V08.00.1W
containing the Equipment Controller (EC)V35.41.20. Software package version and EC version can be read on the equipment.

The key management tool is the SMS (Security Management Server).

1.3 Abbreviations, Terminology and References

1.3.1 Abbreviations

The following abbreviations are used in this document.

Term	Description
AES	Advanced Encryption Standard
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CBC	Cipher-Block Chaining
CC	Common Criteria
CIT	Craft Interface Terminal
CTR	Counter Mode
DoS	Denial of Service
EAL	Evaluation Assurance Level
EC	Equipment Controller
EMS	Equipment Management System
FPGA	Field Programmable Gate Array
GE	Gigabit Ethernet
HMAC	Keyed-Hash Message Authentication Code
IPsec	Internet Protocol security
KGF	Key Generation Functionality
KMF	Key Management Functionality
KMT	Key Management Tool
MPT	Microwave Packet Transport
MSS	Microwave Service Switch
NE	Network Element
NMS	Network Management System
NTP	Network Time Protocol
OSP	Organizational Security Policy
ODU	Out Door Unit
RBAC	Role Based Access Control
SAM	Service Aware Manager
SFP	Security Function Policy
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SHS	Secure Hash Standard
SMS	Security Management Server
SSH	Secure Shell
SSL	Secure Socket Layer
SNMP	Secure Network Management Protocol
SW	Software
SWP	Software Package
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
Web-CT	Web Craft Terminal

WKAT	Well Known Answer Test

Table 1.1: Abbreviation

1.3.2 Terminology

Terms defined in the [CC] are not reiterated here, unless stated otherwise.

1.3.3 References

Abbreviation	Document
[CC]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012, CCMB-2012-09-(001 to 003)
[CCP1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, July 2012
[CCP2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
[CCP3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012
[CEM]	Common Methodology for Information Technology Security Evaluation; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

Table 1.2: References

1.4 Target of Evaluation (TOE) Overview

1.4.1 General Overview

Nokia 9500 MPR Microwave Packet Radio (9500 MPR) is a solution for smooth transformation of backhaul networks from TDM to IP. It is a microwave digital radio that supports PDH, SDH and packet data (Ethernet). The 9500 MPR provides a generic, modular IP platform for multiple network applications (including 2G/3G/HSDPA/WiMAX backhauling to Metro Ethernet areas) to accommodate broadband services. The 9500 MPR radio family supports low, medium, and high capacity applications using ANSI and ETSI data rates, frequencies, channel plans, and tributary interfaces.

- TDM/PDH/SDH Data Rates:
  - ETSI market: E1, E3, STM-1
  - ANSI market: DS1, DS3 and OC-3
- Ethernet Data Speed: 10, 100, 1000 Mb/s
- RF Frequency Range: 4 to 80 GHz

The 9500 MPR provides:

- Multiservice aggregation layer: the capacity to use Ethernet as a common transmission layer to transport several kind of traffic, independently by the type of interface.
- Service awareness: traffic handling and quality management, queuing traffic according to the type of service assigned, independently by the type of interface
- Packet node: no service aggregation limits with all traffic aggregated in packets, in term of: capacity, type of service requirements and type of interface.

- Service-driven adaptive modulation: fully exploit the air bandwidth in its entirety by changing modulation scheme according to the propagation availability and allocate transport capacity, discriminating traffic by different services, only possible in a packet-based environment.
- Air traffic communication encryption: the capacity to encrypt traffic between 9500 MPR.

Nokia9500 MPR encryption functionality is based on an encryption board installed in the radio mechanic and connected to the MSS shelf thanks to a Gb Ethernet cable. The MSS own the Equipment Controller (EC), called CorEvo. The CorEvo card can be redounded inside the MSS.

Figure 1 – CorEvo board and Microwave Service Switch (MSS)

Depending on the desired network configuration, the MSS can be integrated whether in a Short Haul configuration, or in a Long Haul configuration.

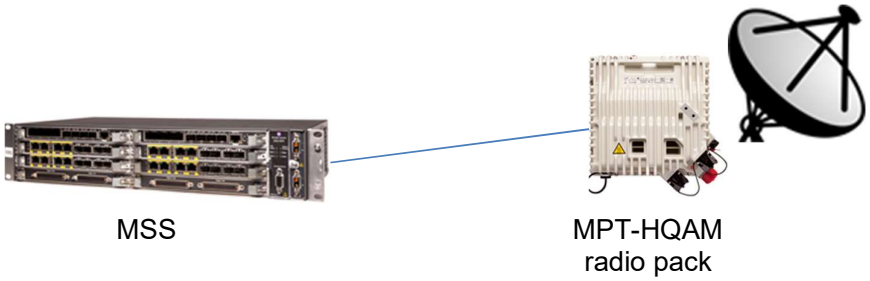


Figure 2 – 9500 Microwave Packet Radio (MPR) in Short Haul architecture

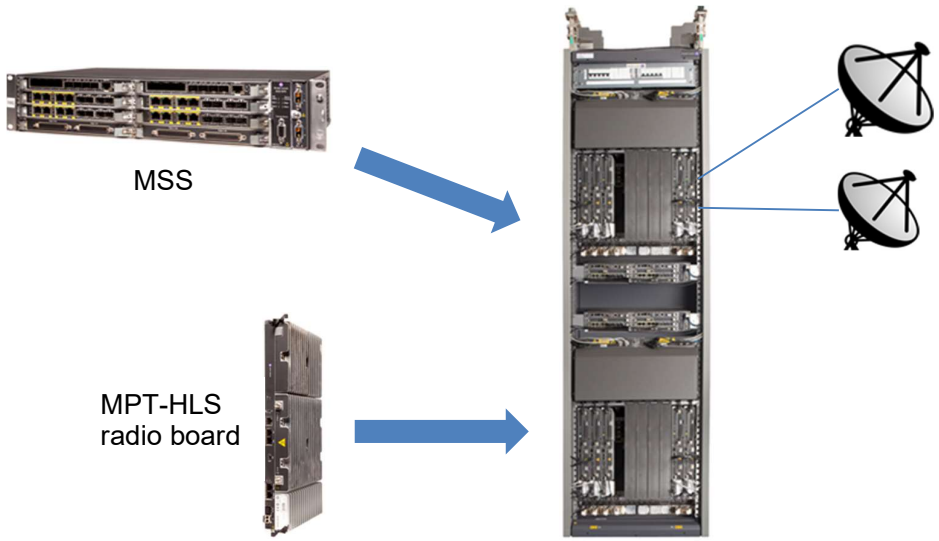


Figure 3 – 9500 Microwave Packet Radio (MPR) in Long Haul architecture

The interfaces covered by the TOE are:

a) The data client interfaces to connect external client equipment or to connect client boards (see next section for more details);

b) The MPT radio interface to connect the TOE to similar remote equipment. The radio carrier between the equipment extends through an untrusted or public network; and

c) The Management Interfaces to configure and manage the TOE

The main security features covered by the TOE are:

a) Layer 1 transport protocol encryption;

b) Secure Management;

c) User Authentication, Authorization and Audit Logs;

d) Redundancy.

For this evaluation, the only allowed KMT is the SMS (Security Management Server).

1.4.2 System Overview

The TOE is integrated into a subsystem composed of Neighboring Equipment (NE), which is a remote 9500 MPR, and a management system. The following drawing gives a general overview of the system architecture and interconnections.

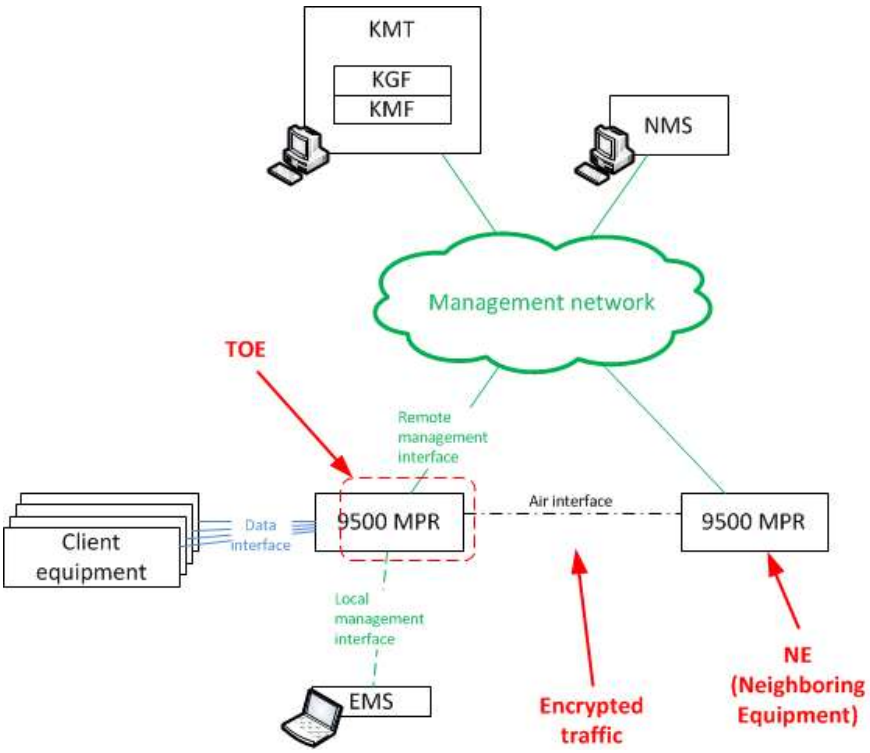


Figure 4 – System overview

The TOE (9500 MPR) is connected to a NE through radio carrier link. They communicate using an Nokia private air frame, with an encrypted payload.
The KMT (Key Management Tool), composed of a KGF (Key Generation Functionality) and a KMF (Key Management Functionality), generates and distributes traffic session keys used by the TOE and its NEs to encrypt the payload of radio communications. The KMT is based on a Bull/ATOS HSM (Hardware Security Module) Proteccio appliance.
The NMS (Network Management System) offers a remote network management capabilities (provioning of links between 9500 MPR, …) and users management. It is either WebCTRem which is dedicated to 9500 MPR equipement, or the product called 5620 SAM (Service Aware Manager) which is used to managed many different network products from Nokia.
The EMS (Equipment Management System) allows to perform initial configuration and provisioning of the TOE and other local management activities.

Alternative system architecture :

The TOE can also be used according to the following scheme :

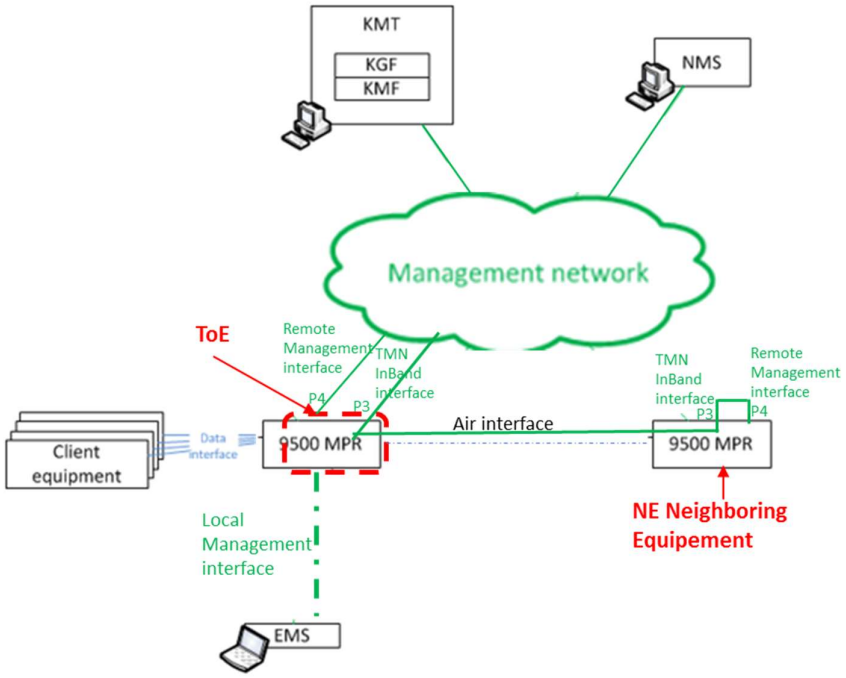


Figure 5 - System architecture alternative

The Main difference are the following :

- The management reach the NE neighboring equipment using the air interface
- The initial security (before link is encrypted) is done by the IPSEC VPN.
- During initial link encryption setup, only management IPSEC VPN is flying over the radio
- IPSEC VPN to the NE neighboring equipment is entering in the NE by a dedicated port (TMN-In Band port 3), going out from the NE neighboring equipment on a dedicated port (TMN-In Band port 3), reintering in the equipment on the “normal remote management port 4” in SNMP format. (IPSEC tunnels are closed outside the equipment as for the other architecture.

This System shall be able to automatically come back in operational mode in any restart condition (Power Down, Reset, …).

The typical operational environment of the TOE may consist of the following external hardware and software in the customer’s Operational Environment.

Environment	Purpose	Applicable Standards
Neighboring Equipment	As Neighboring Equipment, it is defined as a second 9500 MPR connected via the radio carrier link to the TOE in a remote site as shown in Figure 2.	Proprietary air frame and Advanced Encryption Standard AES-256 in CTR mode
Equipment Management System (EMS)	The EMS is an external system or equipment that can be used to administer and operate the TOE via the Local Management Interface. EMS communicates with the TOE through a web interface over HTTPS (called Web-CT component).	
EMS Browser	An Internet browser with TLS/SSL (TLS v1.2) support is used on the EMS for configuration of the TOE and troubleshooting via the Management Interface and the Web-CT component. The HTTPS Client is also used from the EMS to upload and install software updates and to backup and restore Database backups.	TLS/SSL IETF RFC 4346
Network Management System (NMS)	The NMS is an external system that can be used to administer and operate the TOE via the Remote Management Interface. NMS communicates with the TOE through SNMPv3, SFTP (over SSH v2) and NTP. SFTP allows collecting SNMP and auditing logs. SFTP allows also uploading software, performing Databade backups from the NMS. Web-CT can also be cross-launched from the NMS via a web browser (WebCTRem).	SNMP IETF RFC 3411, 3412, 3413, 3414 and 3826 SSH IETF RFC 4251

Environment	Purpose	Applicable Standards
Key Management Tool (KMT)	The KMT is an external system that can be used to manage the cryptographic functions (in particular to generate and distribute cryptographic keys for user data communication protection) of the TOE via the Remote Management Interface. KMT communicates with the TOE through SNMPv3. For this evaluation, the only allowed KMT is the SMS (Security Management Server).	SNMP IETF RFC 3411, 3412, 3413, 3414 and 3826
SFTP client	A SFTP client can be enabled to upload software from NMS and to collect SNMP and audit logs.	SSH IETF RFC 4251

Table 1.3: Non-TOE Components

1.5 TOE Description

1.5.1 Scope of Evaluation

This section defines the scope of the TOE to be evaluated.

1.5.2 TOE Physical Scope

The physical scope of the TOE is made of:

- A 9500 MPR platform composed of a shelf, power supply, fans, card fillers, a front panel, a Core Card (COREVO) and radio interface boards
- A MPT radio composed of a modem board embedding the encryption module, and RF analog board

Client interface boards are outside the scope of the evaluation. In terms of security, they are considered as pure passive interface which only aim is to convert client protocol and physical interface to Gigabit Ethernet.

Two different mechanical arrangement are available for the MPT part :

- MPT-HQAM for Short haul configuration;
- MPT-HLS fir Long haul configuration.

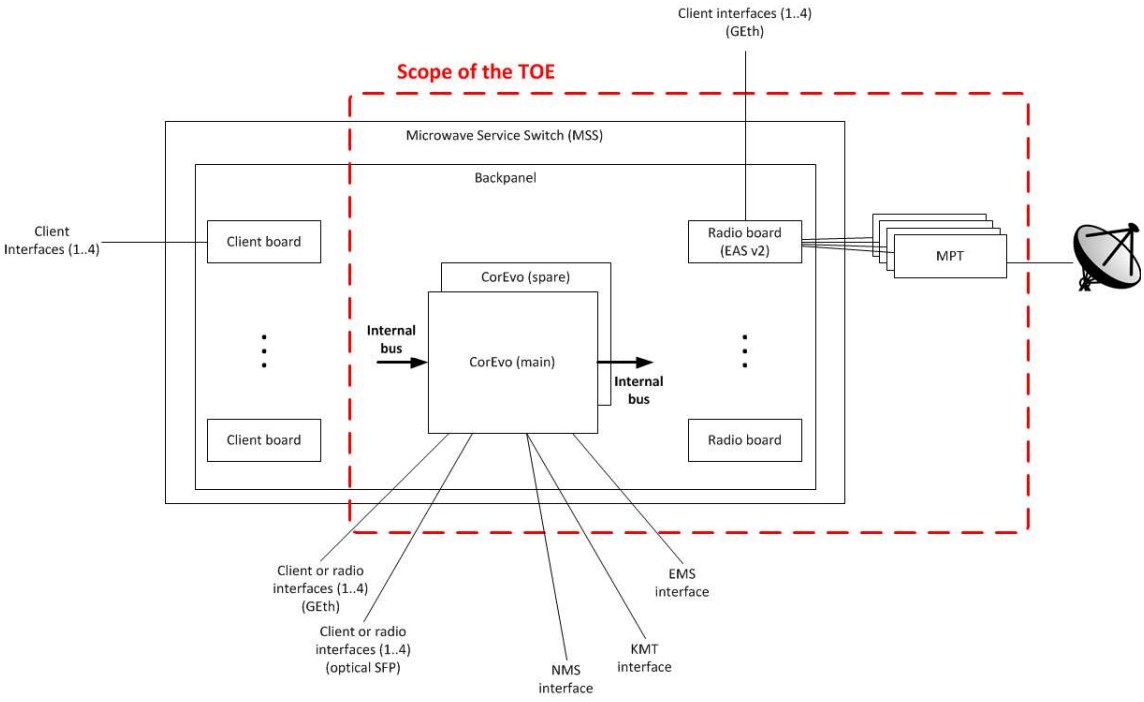


Figure 6 - Physical Scope

After manufacturing and delivery to customer premises, the TOE is verified, initialized and customized in conformance with Nokia guidance. It is assumed that the TOE is located in a controlled and secured zone in order to prevent unauthorized logical and physical access for manipulation.

1.5.3 TOE Logical Scope

The TOE provides cryptographic algorithms at radio rate speeds (Layer 1)

The 9500 MPR also allows the aggregation of client traffic. Different radio configuration (redundancy, combiner) provide different way to protect the datapath.

The logical scope of the evaluation comprises the whole 9500 MPR capabilities except client interface boards, with its radio encryption capability, except following features that are excluded from the evaluation scope but can be used in accordance with environmental security measures:

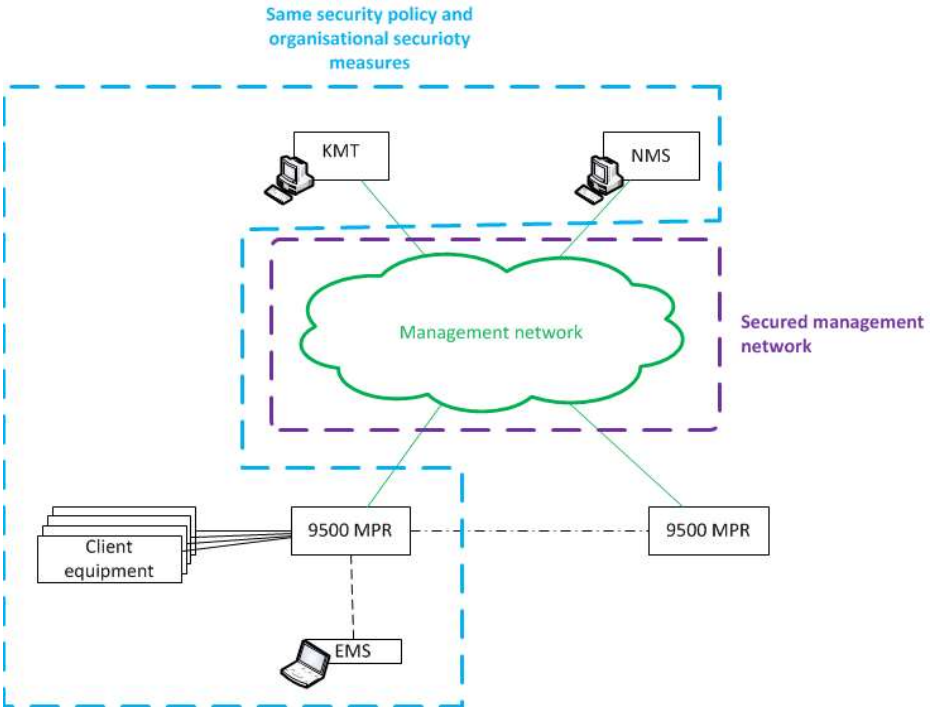
- SSH cryptographic support (for SFTP);
- SSL/TLS cryptographic support (including HTTPS);
- SNMP cryptographic support; and
- NTP server support.

For SSH, SSL/TLS and SNMP protocols, they are activated and they can be used to manage the TOE, but their cryptography services are outside the scope of the evaluation.

The following features are disabled on the evaluated software release of 9500 MPR:

- Telnet support;
- TACACS+ authentication protocol capability(If available); and

Since features outside the TOE scope concerns local and remote management, a secured management network has to be used within the system architecture as shown on the following drawing, and the environment shall protect the EMS and the local management interface.



As the management network (which is part of the TOE environment) transports session keys, it has to be protected in a manner commensurate with the value of the TOE and the user data that the TOE protects. At minimum, the secured management network will provide cryptographic support (encryption) or physically secured support. It can also provide integrity, authentication and non-replay security services.
For example, if the network aims to be compliant with the ANSSI “Qualification Standard” [QSTD] requirements, the management network has to be protected in confidentiality, integrity, authentication and non-replay using encryption devices (e.g. VPN IPSec appliances) which are certified and approved by ANSSI.

1.5.4 External TOE Physical Interfaces

The TOE provides following physical interfaces available on the COREVO, the radio interface board and the MPT.

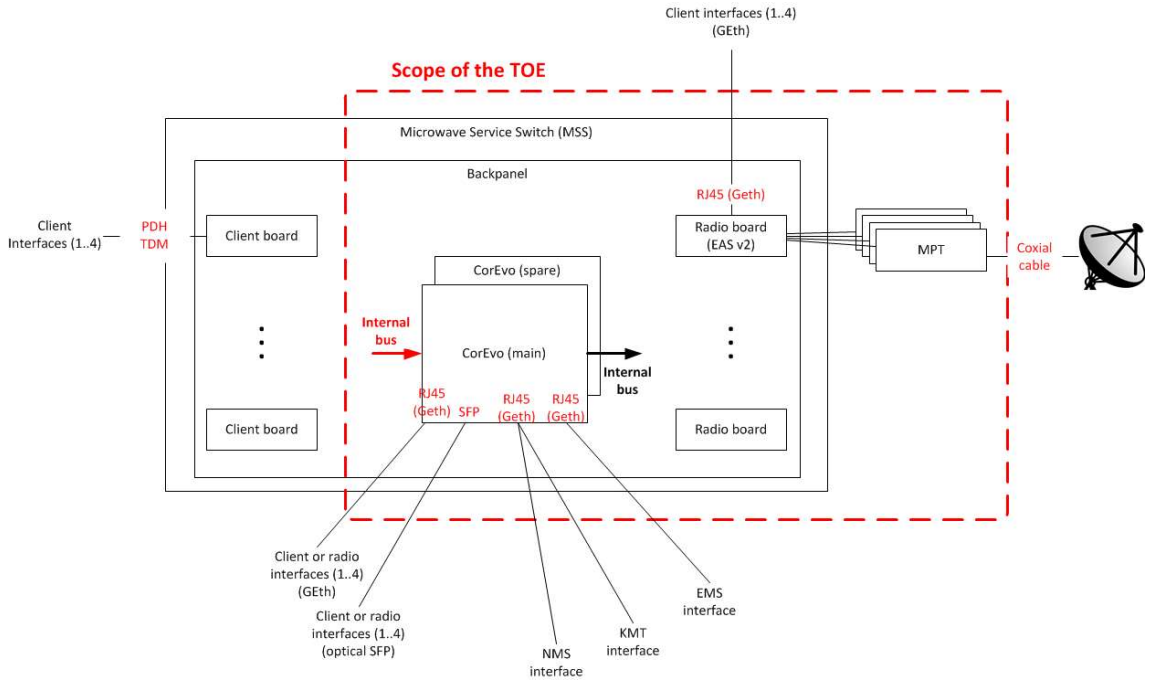


Figure 7 – TOE physical interfaces

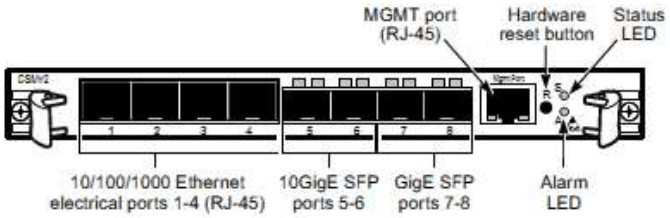


Figure 8 – CoreEvo front panel details

The physical interfaces of the TOE are:

- For the COREVO :
  - 4 Base 10/100/1000BaseT electrical Ethernet interfaces with client equipments;
  - 4 SFP optical Ethernet interfaces with client equipments;
  - 1 electrical Ethernet interface for local management via an EMS;
  - 1 electrical Ethernet interface for remote management via NMS and KMT;
  - 2 LED to show to an external user nearby the TOE the status of the equipment;
  - And also backplane electrical Ethernet interfaces to communicates with client and radio interface boards.
- For each radio interface board (EASv2 card):
  - 4 Ethernet interfaces (either optical SFP or electrical RJ 45 ones) with MPTs;
  - 4 electrical interfaces with client equipments;
- For the MPT : the number and type of interface depends on the type of MPT module
  - 1 Ethernet interface with radio interface board;
  - 1 Ethernet interface with another MPT for redundancy purpose (see below);

- 1 radio interface with the antenna.

1.5.5 External TOE Logical Interfaces

The logical interfaces of the TOE are:

- All the interface available for Client equipments, provided by the CorEvo board and the radio interface boards:
  - By CoreEvo:
    - 8 Gigabit Ethernet interfaces (4 electrical + 4 optical);
    - Gigabit Ethernet interfaces with client boards through the backplane;
  - By radio boards:
    - 8 Gigabit Ethernet interfaces (electrical);
- The interface with the antenna to connect the TOE to a similar neighboring equipment
- Management interface providing TOE management through HTTP over TLS (that is HTTPS);
  - The web interface is able in local (EMS directly connected to the TOE);
  - It is also available in remote (cross-launched from the NMS);
- Remote management interface that provides KMT with:
  - TOE management through SNMPv3
- Remote management interface that provides NMS with:
  - TACACS+ authentication protocol capability (if available)
  - Time management though NTP
  - SFTP (FTP over SSH) for software update and for log retrieval capabilities

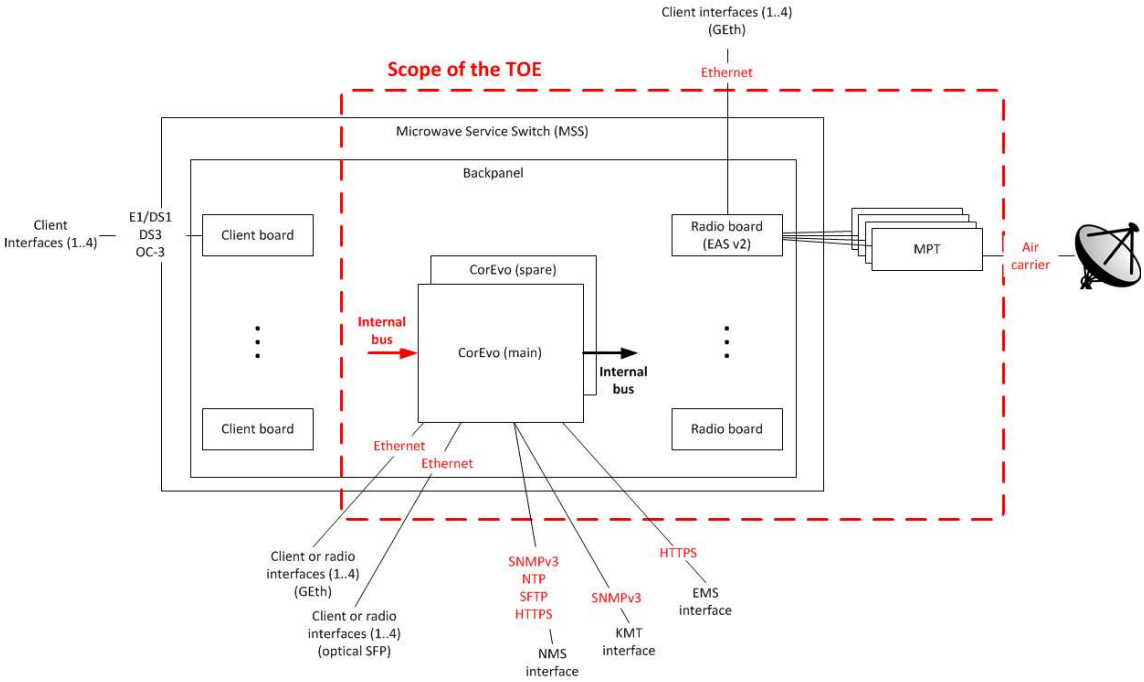


Figure 9 – TOE communication protocols

1.5.6 Summary of Security Features

The TOE comprises the following security features:

- Layer 1 transport protocol encryption
- Secure management
- User identification and authentication
- Redundancy

1.5.6.1 Layer 1 transport protocol encryption

The TOE provides protection against loss of confidentiality along the radio through layer 1 encryption. It protects radio line using AES-CTR with 256 bit-keys by means of the MPT.

Note: encryption at layer 1 allows independence in the selection of protocols or applications used at higher layers, as well as lower encryption latency than that possible with higher level protocols of the TCP/IP and OSI stacks.

1.5.6.2 Secure Management

The TOE is managed through its Equipment Controller (EC) board. It can be either locally or remotely managed.

For local management, the TOE provides an Ethernet interface and a configuration capability through HTTPS (the tool is called Web-CT).

For remote management, the TOE provides encrypted interfaces for SNMPv3 management functions accessed via an Ethernet interface for KMT and NMS.
The NMS and/or KMT system in the operational environment provides a user friendly interface for the SNMP interface to the TOE. The user can view audit records as they are received by the NMS or KMT system. Web-CT can also be cross-launched from the NMS.

For management through Web-CT, the user shall logon using an individual account. For remote management, authentication is performed through SNMPv3.

Web-CT supports different user roles (Role Based Access Control, RBAC). Roles can be assigned to users during system commissioning and are consistently applied for access via Web-CT. The TOE supports following roles:

- Administrator
- Crypto officer

For remote management, the TOE supports NMS and KMT “roles”. The two equipment are distinguished through their IP address and the cryptographic keys used to protect SNMPv3 protocol. The keys (AuthKey and PrivKey) are configured during system commissioning. The initial configuration of the keys for the Management Interface is done using pre-shared keys. SNMPv3 is configured both as server (for commands) and client (for notifications) in AuthPriv mode.

In band management interface and radio control plane function can be used only if they are following the ANSSI “Qualification Standard” [QSTD] requirements. For example, VPN IPSEC, is kept and radio interface used as part of the secured management network.

The figure here after illustrate the view:

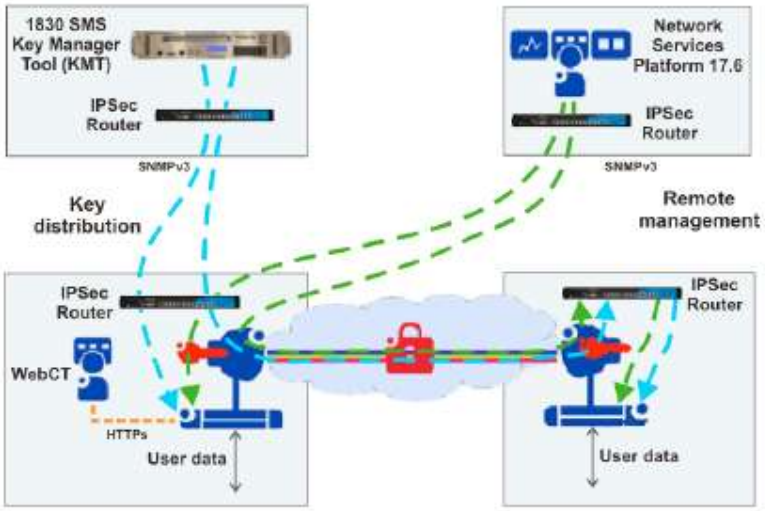


Figure 10 -Illustration of Management over radio interface

Role	Privileges
Administrator	This role is the administrator of the TOE. It provides all services that are necessary for initial installation and further management of the module. This role can configure the system and perform provisioning and testing of all IO cards, ports, interfaces, and circuits. It can also create, delete, and modify user accounts. A summary of what this role can do is: - provision the TOE; - configure IO cards, ports, interfaces and circuits; - SNMP configuration; - management of KMT server connection information; - run test; - initiate transfer of non-security related files to RFS, e.g. PM log - TOE software update; - supervise and manage Security Auditing Alarms; - retrieve audit logs; - set system-wide user security attributes; - retrieve system-wide user security attributes; - inhibit and allow all users, including Service user; - manage and retrieve security information about users (not password) such as authentication failure lockout, session inactivity timeout, minimum password length.
Crypto Officer	This role is the administrator for the cryptographic keys. It can manage cryptographic functions and parameters. A summary of what this user can do is: - establish a session with the TOE (logon); - set encryption state and encryption keys; - manage cryptographic parameters and functions.

Role	Privileges
NMS[1]	This role is equivalent to the “Administrator” role. It has access to the same functionalities as the latter except management of users: NMS role can only retrieve information about users, but it can neither create nor modify users and user attributes.
KMT	This role is equivalent to the “Crypto Officer” role. It has access to the same functionalities as the latter (but more elaborated and user-friendly).

Table 1.*4: User Roles*

Date and time are configured by the “Administrator” or the “NMS” role, or they can be also synchronized via NTP protocol.

1.5.6.3 User Authentication, Authorization and Audit Logs

The access to management functions is only possible after successful user authentication and authorization. The TOE supports identity-based authentication. Users are identified and authenticated against the local database in the evaluated configuration.

After users are successfully authenticated to the TOE and authorized according to their assigned role, they may change the system or network configuration.

The following table summarizes authentication mechanism for each role or entity:

Role or entity	Authentication mechanism
Administrator	Password
Crypto Officer	Password
NMS[2]	Authentication symmetric key of the AuthPriv mode of SNMPv3 Note : the key is different from the KMT one.
KMT	Authentication symmetric key of the AuthPriv mode of SNMPv3 Note : the key is different from the NMS one.

Security-related auditable events are recorded in:

- the SNMP log;
- or in the security event log;
- or the User Activities Log (UAL).

These logs can be retrieved using the SFTP protocol for further manipulation and investigation. SNMP is used to automatically configure the transfer these logs to the NMS or KMT system in the operational environment for storage and review.
The TOE will transmit audit records sent to the SNMP log and security event log to an external IT entity using SNMP v3 or SFTP. The audit records are usually sent to an NMS or external log server.

[T]In the remainder of the ST, the “Administrator” role has the same privileges / permissions as the “NMS” role (except about user attributes creation and modification). When the “Administrator” role is mentioned, it is also referring to the “NMS” role.

[T]In the remainder of the ST, the “Administrator” role has the same privileges / permissions as the “NMS” role (except about user attributes creation and modification). When the “Administrator” role is mentioned, it is also referring to the “NMS” role.

1.5.6.3.1 SNMP log

Activities performed via SNMP are collected and stored locally in a user-readable format, along with the time and date of the action, the source IP address, user name and the action itself. One entry is captured for each user action through SNMP. The purpose of this log is to provide accountability.

1.5.6.3.2 Security Event Log

The security event log is used to record all important events of the TOE. These events include managing user accounts, modifying settings, exporting audit logs, and user login.

1.5.6.3.3 User Activities Log (UAL)

All user activities done from HTTPS are recorded in the User Activity Log (UAL), which is in a user-readable format. Each entry in the UAL contains the time and date of the action, the source IP address, the user name and the action itself. One entry is captured for each user action through HTTPS.

1.5.6.4 Redundancies

The TOE provides redundancies capabilities :

- CoreEvo board redundancy;
- MPT redundancy (also called 1+1 configuration).

The CorEvo can be redunded within the MSS shelf. In that case, one board is declared “main” board, the other one “spare” board.
All parameters configured in the 9500 MPR is automatically replicated from the main CorEvo to the spare one : this operation is called alignment.
Switching from main to spare board is performed when a default is detected on the main board. Switching can also be controlled by a Administrator (it is called manual switching) for example, for maintenance reason.

Concerning MPTs, they can be redunded through 2 configurations:

- 1+1HSB, for reception redundancy
- 1+1FD , for emission and reception redundancy

The two following drawings illustrate those configurations.

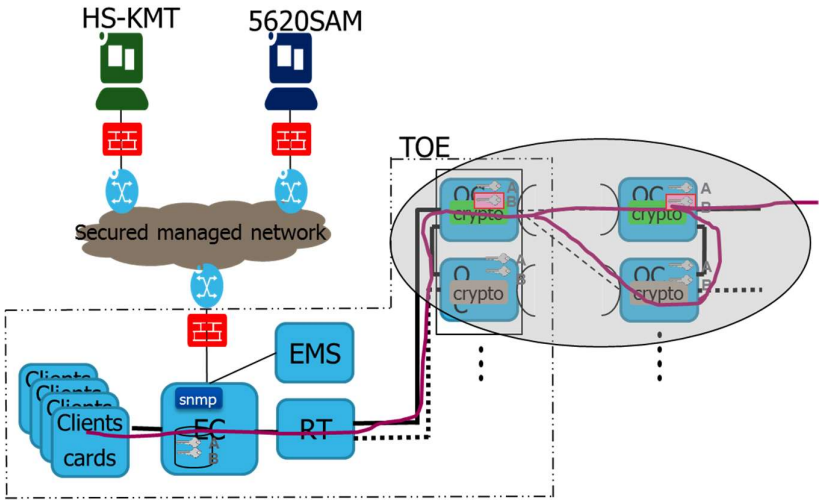


Figure 11 – 1+1 HSB redundancy configuration

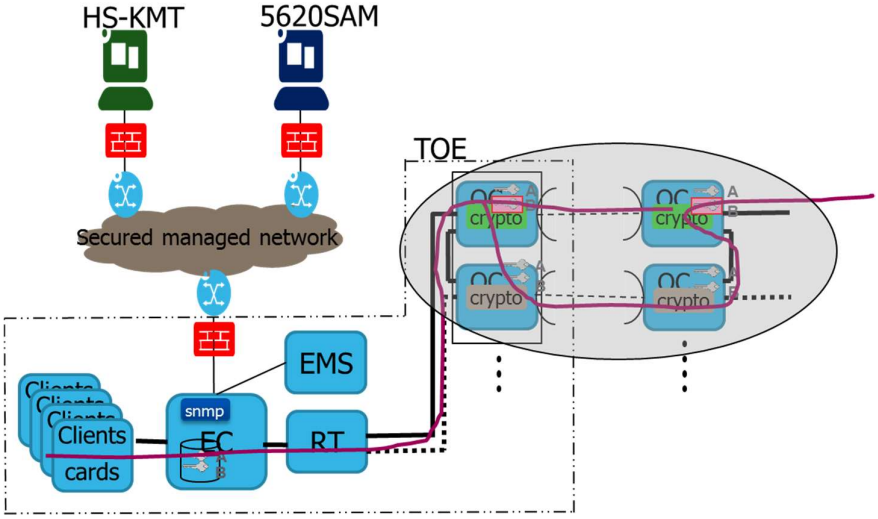


Figure 12 – 1+1 FD redundancy configuration

1.5.7 Evaluation test platform

The following platform is used to test the TOE.

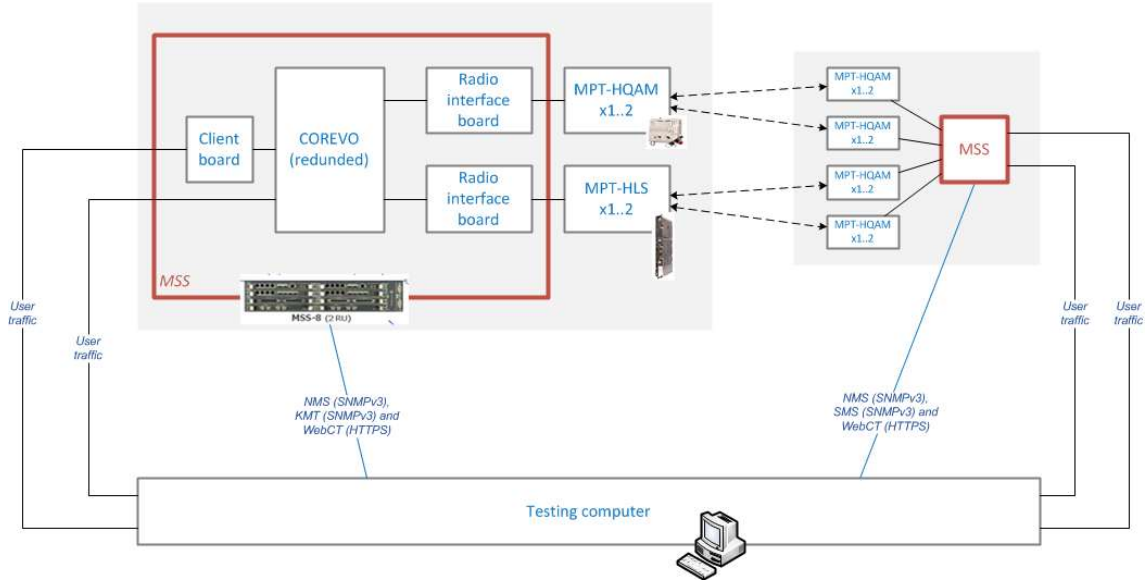


Figure 13 – Evaluation testing platform

2. CC Conformance Claim

2.1 CC Conformance Claim

This Security Target claims to be conformant to version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 [CCP1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 [CCP2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 [CCP3]

as follows:

- CC Part 2 extended,
- CC Part 3 conformant.

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 [CEM] has to be taken into account.

2.2 Protection Profile Claim

This Security Target does not claim conformance to a validated Protection Profile.

2.3 Assurance Package Claim

This Security Target claims conformance to Evaluation Assurance Level (EAL) 3 augmented with ALC_FLR.3 and AVA_VAN.3.

3. TOE Security Problem Definition

3.1 Assets

This section lists sensitive assets. For each of them, it associates a "security needs" attribute indicating what protection the asset needs.
A security need specified as optional means that the risk analysis of the system using the TOE shall determine if this security need is required or not for the purposes of the system. If it is, the user will have to configure the TOE such as it provides the appropriate security protection.

3.1.1 Assets protected by the TOE (User Data)

The primary asset that will be protected by the TOE:

Asset	Definition
D_DATA	User (i.e. client equipment) data in radio carrier between the TOE and the Neighbouring Equipment. These data may be temporarily stored in the TOE to be able to process them (i.e., enforce security services) before sending them on to the Neighboring Equipment. ***Security needs:*** *Confidentiality* ***Note:*** *Integrity, Authentication and Non-Replay capabilities are provided at higher level protocols when necessary (by or before the client equipment).*

Table 3.1: TOE Primary Asset

3.1.2 Assets belonging to the TOE (TSF Data)

The TOE uses secondary assets in order to achieve its security functionalities. They also have to be protected by the TOE in order to support the protection of the primary asset:

Asset	Definition
D_CRYPTO_KEYS	Symmetric keys used by the encryption and decryption of D_DATA. ***Security needs:*** *Confidentiality, Integrity, Authentication, Replay*
D_CONFIG_KEYS	Symmetric and asymmetric keys used for encryption and decryption of D_CONFIG_MANAGEMENT and D_MONITORING_DATA through SNMPv3, SSH, etc. ***Security needs:*** *Confidentiality, Integrity, Authentication, Replay*
D_CONFIG_MANAGEMENT	Configuration parameters of the TOE via the management interfaces. This asset groups all TOE configuration parameters that are not confidential ***Security needs:*** *Confidentiality, Integrity Authentication, Replay*

Asset	Definition
D_AUDIT	This asset represents audit record generated by the TOE: security auditing alarms, SNMP logs, and security event logs generated by the TOE. ***Security needs:*** *Integrity, Authentication, Non replay*
D_TIME_BASE	This asset represents the reliable time base kept within the TOE and used by the TOE. ***Security needs:*** *Integrity*
D_MONITORING_DATA	Monitoring data in the out-of-band channel between the TOE and a non-TOE components. Monitoring data are: - Alarms - Radio analog measurement - Adaptive Modulation Performance Monitoring - Radio Power Levels Performance Monitoring ***Security needs:*** *Integrity, Authentication, Non replay*
D_SOFTWARE_UPDATE	Software update of the TOE. The update is uploaded to the TOE and then installed on the TOE. ***Security needs:*** *Integrity, Authentication*
D_DB_BACKUP	TOE Database backup. It contains TOE network and radio configuration (radio parameters, input interfaces, cross connections, …) ***Security needs:*** *Integrity, Authentication*

Table 3.2: TOE Secondary Assets

3.2 Users

This security target considers the following subjects and descriptions:

Subject	Description
User: Crypto Officer	The Crypto Officer is a user or process authorized to perform self tests, provision and configure the well known answer test (WKAT) and facility information associated with the MPT, and provision the Encryption Key. The Crypto Officer is a privileged user with Crypto Officer rights defined in Table *1*.4.
User: Administrator	The Administrator is a user or process authorized to perform configuration and advanced equipment and service management functions. The Administrator is a privileged user with Administrative rights, which include user management as defined in Table *1*.4.
IT Product: NMS	This role is equivalent to the “Administrator” role. It has access to the same functionalities as the latter.

Subject	Description
IT Product: KMT	This role is equivalent to the “Crypto Officer” role. It has access to the same functionalities as the latter.
IT Product: EMS	Equipment Management System
Threat Agent	A Threat Agent is a person or process changing the properties of the assets that are part of the TOE. The threat agent may intentionally or unintentionally cause damage. A Threat Agent may also be an attacker with the objective of causing damage or obtaining advantage of D_DATA. The Threat Agent has an Enhanced-Basic (AVA_VAN.3) potential of attack. He has an access to communication links between the TOE and a NE, and between the TOE and the management system (KMT and NMS).

Table 3.3: Subjects

3.3 Threats

T_REMOTE_MNGT

A Threat Agent eavesdrops, intercepts, replays or modifies configuration data or session cryptographic keys between the NMS or KMT and the TOE, resulting in ineffective security mechanisms.

Impacted data:

- D_CRYPTO_KEYS

- D_CONFIG_MANAGEMENT

Impacted security need: *Confidentiality, Integrity, Authentication, Replay*

T_LOCAL_MNGT

A Threat Agent eavesdrops, intercepts, replays or modifies configuration data or session cryptographic keys between the EMS and the TOE, resulting in ineffective security mechanisms.

Impacted data:

- CONFIG_KEYS

- D_CONFIG_MANAGEMENT

- D_DATABASE_BACKUP

Impacted security need: *Confidentiality, Integrity, Authentication, Replay*

T_MALICIOUS_UPDATES

A Threat Agent upload and install a malicious software or modifies a software update before it is uploaded and installed on the TOE, in order to trap and change the behaviour of the TOE.

Impacted data:

- D_SOFTWARE_UPDATE

Impacted security need: *Integrity, Authentication*

T_ADMIN_ERROR

An administrator or a Crypto Officer unintentionally installs or configures the TOE incorrectly, resulting in ineffective security mechanisms.

Impacted data:

- D_CONFIG_KEYS

- D_CONFIG_MANAGEMENT

Impacted security need: *Integrity*

T_TSF_FAILURE

Security mechanisms of the TOE fails, leading to a compromise of TSF Data or User Data or leading to TOE unavailability.

Impacted data:

- D _DATA

- D_CONFIG _MANAGEMENT

- D_CRYPTO_KEYS

Impacted security need: *Confidentiality*

T_REDUNDANCY_FAILURE

A failure within the redundancy mechanism (e.g. malicious change of the copy of the TOE configuration, failure of the configuration copy, …) leads to a TSF Data or User Data leakage.

Impacted data:

- D _DATA

- D_CONFIG_MANAGEMENT

- D_CRYPTO_KEYS

Impacted security need: *Confidentiality, integrity (of D_CONFIG_MANAGEMENT)*

T_UNDETECTED_ACTIONS

A Threat Agent takes actions that adversely affect the security of the TOE. He intercepts (and deletes) or modifies audit data or alarms sent by the TOE to the NMS or the KMT, in order to cover up the attack.

Impacted data:

- D_MONITORING_DATA

- D_AUDIT

Impacted security need: *Integrity, Authentication*

T_UNAUTHORISED_ACCESS

A Threat Agent gains unauthorized access to the TOE data and TOE executable code.

A Threat Agent (malicious user, process, or external IT entity) masquerades as an authorized entity in order to gain unauthorized access to data or TOE resources.

A Threat Agent (malicious user, process, or external IT entity) misrepresents itself as the TOE to obtain identification and authentication data.

Those actions could lead either to :

– Modification or retrieval of TOE data (that is TSF Data and User Data persistently stored within the TOE)

– Usurpation of an administrator identity in order to perform administration operations on the TOE

Impacted data:

- D _DATA

- D_CRYPTO_KEYS

- D_CONFIG_KEYS

- D_CONFIG_MANAGEMENT

- D_TIME_BASE

- D_DB_BACKUP

Impacted security need: *Confidentiality, Integrity*

T_TIME_BASE

A threat Agent disturbs or tampers with the TOE time base with the aim of falsifying audit data.

Impacted data:

- D_TIME_BASE

Impacted security need: *Integrity*

T_RESIDUAL_DATA

A Threat Agent acquires knowledge, through direct access to the TOE, of old value of TOE data (keys, configuration,…) during a change of operational context (assignment of the TOE in a new premise, maintenance…).

Impacted data:

- D_CONFIG_ MANAGEMENT

- D_CRYPTO_KEYS

- D_CONFIG_KEYS

Impacted security need: *Confidentiality*

3.4 Assumptions

The following assumptions apply to the TOE environment.

A_ORGANIZATION

It is assumed that the organization follows a systematic security standard or management process that ensures that security controls meet the organization security needs and provide an adequate management of security risks, threats, vulnerabilities and their impact.

A_ADMIN

It is assumed that TOE Crypto Officers and TOE Administrators are trusted and well trained.

They apply the procedure described in the administration guide.

A_AUDIT

It is assumed that alarms are monitored and SNMP logs and security event logs are regularly examined by the TOE Administrators and corrective actions are taken upon potential incident detection according to recommendations for managing the TOE.

A_CONFIGURATION

It is assumed that the TOE is configured following recommendations in order to properly protect the primary and secondary assets of the TOE.

It is assumed that Neighboring Equipment and non-TOE components, as defined in 1.4.2**Error! Reference source not found.**, are configured following the vendor security recommendations.

A_GENERAL_PURPOSE

It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

A_PROTECTION

It is assumed that:

a) The TOE is located in a controlled and secured zone in order to prevent unauthorized logical and physical access to the TOE.

b) Neighboring Equipment have at least the same level of physical and logical protection as the TOE.

c) Non-TOE management assets, secondary assets have at least the same level of physical and/or logical protection as the TOE.

d) User data D_DATA (coming from or sent to client equipment) intended for transmission via the TOE are protected.

A_KGF

It is assumed that key generation meets ANSSI requirements [RGS_B1] regarding key generation. It meets security requirements recognised by ANSSI (CC, CSPN or “ANSSI qualification label”).

A_MNGT_NETWORK

It is assumed that Management Network which interconnects the KMT, the NMS and the TOE (and its NEs) is a secured network. Security services provided by the secured management network are commensurate with the value of the user data protected by the TOE. They provide protections in confidentiality, integrity, authentication and/or non-replay.

A_MNGT_EQPT_SECURED

It is assumed that following equipment are properly and securely configured, according the sensitivity of assets they handle:

- NMS
- KMT
- EMS

A_MNGT_EQPT_PROTECTION

It is assumed that following equipment have at least the same level of physical and/or logical protection as the TOE:

- NMS
- KMT
- EMS

3.5 Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices or guidelines imposed by an organization upon its operations. The OSP are suggested as basic operational practices to be implemented in a properly managed datacenter environment. A datacenter environment, depending on the applications, services and country regulation may have to follow additional operational practices not covered by this list of objectives.

OSP_CRYPTO_RGS

The TOE shall implement cryptographic mechanisms compliant with ANSSI guidance [RGS_B1].

OSP_CRYPTO

The TOE shall provide D_DATA encryption and decryption.

OSP_MANAGEMENT

The TOE shall provide a management capability for the equipment and its cryptographic functions.

OSP_KEY_MANAGEMENT

The TOE shall provide mechanisms and procedures that allow the KMT to securely configure and manage D_CRYPTO_KEYS.

OSP_BANNER

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

4. Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment

4.1 Security Objectives for the TOE

The following TOE security objectives address the protection provided by the TOE independent of the TOE environment.

O_ACCESS

The TOE shall protect against all non-authorized logical access attempts. The TOE shall also provide mechanisms for authenticating Users prior to granting access to those functions which they are authorized to use based upon their assigned role.

O_ALARM

The TOE shall notify the User about the following potential intrusion events via the Management Interface:
- Loss of connection with NMS
- Loss of connection with KMT

O_AUDIT

The TOE shall record security relevant events, such as TOE configuration changes.
The TOE must transmit audit data to an external trusted entity for storage and viewing.

The TOE shall associate to generated audit data:
- The date and time of event generation
- A number (an incremental counter), offering a mean to detect audit data loss.
- A severity, offering a mean to discriminate informational, warning and critical audit data.
- A type.

O_CRYPTO_CONFORMITY

The TOE shall provide D_DATA encryption and decryption which conforms to ANSSI requirements [RGS_B1].

O_DATA_CONFIDENTIALITY

The TOE shall provide encrypted communication between itself and a NE, in order to protect the confidentiality of D_DATA.

O_KEY_MANAGEMENT

The TOE shall provide mechanisms that allow authenticated and authorized users to securely configure and manage D_CRYPTO_KEYS and D_CONFIG_KEYS.

O_MANAGEMENT

The TOE shall provide a management capability that allows authenticated and authorized users to manage the equipment and its cryptographic functions.

O_TIME_BASE

The TOE provides a time base upon which the audit records are based and ensures its reliability.

O_REDUNDANCY

The TOE shall provide redundancy capabilities in order to provide a secure state in case of CorEvo (supporting management and switching functionnalities) or MPT (supporting user communication protection) hardware failure.

O_SW_UPDATES

The TOE shall check software updates integrity and authentication, prior installing it.

O_ROLES

The TOE shall provide a RBAC mechanism for local management. The user management function allows defining users for operation and administration based on the general privilege categories listed in *Table 1*.4.
The roles are :
- Administrator
- Crypto Officer

O_I&A

The TOE shall require the identification of a device before granting it with the NMS or KMT access rights.
The TOE shall require the authentication of the user before granting him with his access rights.
The TOE shall provide means to protect user sessions (session lock or termination, user account blocking).

O_DISPLAY_BANNER

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

O_SELF_TESTING

The TOE shall run a set of tests at startup.

O_RESIDUAL_INFO_CLEARING

The TOE shall ensure that any D_DATA encryption cryptographic key (that is D_CRYPTO_KEYS) is made unavailable after use.

4.2 Environmental Security Objectives

The following security objectives for the TOE's operational environment address the protection provided by the TOE environment independent of the TOE itself.

4.2.1 TOE Development

OE_GENERAL_PURPOSE

There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

4.2.2 Organization and TOE Administration

OE_ORGANIZATION

The OE and all employees shall follow the organizational policies, guidelines and procedures, which have been established in regards to the organization security needs and result from an adequate management of security risks, threats, vulnerabilities and their impact.

OE_TRUSTED_ADMIN

The OE shall ensure that users are properly trained to perform TOE tasks according to their role.

In particular, TOE Crypto Officers and TOE Administrators shall be trained to configure and supervise the TOE and its security functions, and they shall apply the procedure described in the administration and the user guide.

OE_AUDIT

The OE shall ensure that TOE Users monitor alarms and TOE Administrators regularly reviews SNMP logs, security event logs and UAL.

The TOE Administrators shall also ensure that appropriate corrective actions, according to Nokia recommendations for managing the TOE, are taken upon potential incident detection.

OE_TOE_CONFIGURATION

The OE shall ensure that the TOE and its Neighboring Equipment are installed and commissioned following Nokia recommendations and procedures in order to properly protect user data (D_DATA) and secondary assets of the TOE.

OE_DB_BACKUP

The operational environment shall preserve database backup integrity and authentication, in order to prevent any malicious modification, trapping and substitution.

4.2.3 Management network

OE_KGF

The key generation shall meet ANSSI requirements [RGS_B1]. It shall meet security requirements recognised by ANSSI (CC, CSPN or “ANSSI qualification label”).

OE_MNGT_NETWORK

SSH, HTTPS, SNMP cryptographic support and other management protocols are outside the scope of the evaluation. The communication link between the NMS or the KMT and the TOE (respectively the NE) has to be protected in confidentiality, integrity, authentication and non-replay through a secured management network.

To keep reliability and integrity of the NMS and the KMT, prior to interconnecting it with any network (i.e. management or external network), the OE shall perform a risk analysis and determine necessary security technical and/or organizational measures to put in place between the NMS, the KMT and the networks, commensurate to the value of the TOE and the user data the TOE protects (D_DATA).

For instance, VPN IPSec devices, being approved at ANSSI “Qualification Standard level of security”, may be placed between the NMS (and KMT) and the TOE (respectively the NE). The OE shall ensure that the VPN IPSec device are installed and configured following vendor’s recommendations and procedures in order to properly protect management data (D_CRYPTO_KEYS, D_CONFIG_MANAGEMENT).

OE_LOCAL_MNGT

The OE provides physical and logical protections of the management communication link using the CRAFT and the CIT interfaces commensurate with the value of the TOE and the user data the TOE protects (D_DATA). The OE may perform a risk analysis to determine the appropriate security measures.

Those measures apply to:

– The EMS, which have to be physically and logically secured

– The link between the EMS and the TOE, which integrity has to be preserved

OE_MNGT_EQPT_SECURED

The OE shall ensure that non-TOE components are configured following the vendor security recommendations and settings.

The OE shall ensure that following equipment are properly and securely configured, according the sensitivity of assets they handle:

– NMS

– KMT

– EMS

It is assumed that their operating system is configured accordingly to the appropriate security guidance and that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on those devices, other than services necessary for the operation and support of their functionalities.

In case sensitive data are governmental data at Restricted level of classification (DR, NR, EUR), it is assumed that devices are configured in regards to appropriate rules and regulations.

OE_MNGT_EQPT_PROTECTION

The OE shall ensure the following equipment have at least the same level of physical and/or logical protection as the TOE:

– NMS

– KMT

– EMS

The overall solution allows individual access accounting (e.g. physical access restriction to the device hosting the software, user authentication by the operating system, etc.)

OE_SECONDARY_ASSETS_PROTECTION

It is also assumed that non-TOE management assets and the defined secondary assets have at least the same level of physical and/or logical protection as the TOE.

4.2.4 Protections

OE_TOE_PROTECTION

The OE shall ensure that the TOE is located in a controlled and secured zone in order to prevent unauthorized logical and physical access.

The Neighboring Equipment shall have at least the same level of physical and logical protection as the TOE.

OE_DATA_PROTECTION

The OE shall protect data intended for transmission to the TOE (that is D_DATA).

The OE shall handle data originating from the TOE securely.

4.3 Security Objectives Rationale

The following table provides an overview for security objectives coverage (TOE and its environment) also giving an evidence for sufficiency and necessity of the security objectives defined. It shows that all threats and OSPs are addressed by the security objectives. It also shows that all assumptions are addressed by the security objectives for the TOE environment.

		O_ACCESS	O_ALARM	O_AUDIT	O_CRYPTO_CONFORMITY	O_DATA_CONFIDENTIALITY	O_KEY_MANAGEMENT	O_MANAGEMENT	O_TIME_BASE	O_REDUNDANCY	O_SW_UPDATES	O_ROLES	O_I&A	O_DISPLAjY_BANNER	O_SELF_TESTING	O_RESIDUAL_INFO_CLEARING	OE.GENERAL_PURPOSE	OE_ORGANIZATION	OE_TRUSTED_ADMIN	OE_AUDIT	OE_TOE_CONFIGURATION	OE_DB_BACKUPS	OE_KGF	OE_MNGT_NETWORK	OE_LOCAL_MNGT	OE_MNGT_EQPT_SECURED	OE_MNGT_EQPT_PROTECTION	OE_SECONDARY_ASSETS_PROTECTION	OE_TOE_PROTECTION	OE_DATA_PROTECTION
Threats	T_REMOTE_MNGT		X	X																				X		X	X		X	
	T_LOCAL_MNGT			X																					X	X	X		X	
	T_MALICIOUS_UPDATES			X							X																			
	T_ADMIN_ERROR			X															X											
	T_TSF_FAILURE									X					X															
	T_REDUNDANCY_FAILURE														X															
	T_UNDETECTED_ACTIONS			X																				X		X	X			
	T_UNAUTHORISED_ACCESS	X	X	X								X	X											X	X	X	X			
	T_TIME_BASE								X																					
	T_RESIDUAL_DATA															X														
Assumptions	A_ORGANIZATION																	X												
	A_ADMIN																		X											
	A_AUDIT																			X										
	A_CONFIGURATION																				X					X				
	A.GENERAL_PURPOSE																X													
	A_PROTECTION																					X					X	X	X	X
	A_KGF																						X							
	A_MNGT_NETWORK																							X						
	A_MNGT_EQPT_SECURED																									X				
	A_MNGT_EQPT_PROTECTION																										X			
OSPs	OSP_CRYPTO_RGS				X																			X						
	OSP_CRYPTO				X	X																								
	OSP_MANAGEMENT							X				X	X																	

	O_ACCESS	O_ALARM	O_AUDIT	O_CRYPTO_CONFORMITY	O_DATA_CONFIDENTIALITY	O_KEY_MANAGEMENT	O_MANAGEMENT	O_TIME_BASE	O_REDUNDANCY	O_SW_UPDATES	O_ROLES	O_I&A	O_DISPLAjY_BANNER	O_SELF_TESTING	O_RESIDUAL_INFO_CLEARING	OE.GENERAL_PURPOSE	OE_ORGANIZATION	OE_TRUSTED_ADMIN	OE_AUDIT	OE_TOE_CONFIGURATION	OE_DB_BACKUPS	OE_KGF	OE_MNGT_NETWORK	OE_LOCAL_MNGT	OE_MNGT_EQPT_SECURED	OE_MNGT_EQPT_PROTECTION	OE_SECONDARY_ASSETS_PROTECTION	OE_TOE_PROTECTION	OE_DATA_PROTECTION
OSP_KEY_MANAGEMENT						X																	X		X	X	X		
OSP_BANNER													X																

Assumption, Threat or OSP	Rationale
A_ADMIN	OE_TRUSTED_ADMIN requires the operational environment to ensure that users are properly trained to perform TOE tasks according to their role as assumed by A_ADMIN. Furthermore OE_TRUSTED_ADMIN particularizes the training concepts for administrators and crypto officers.
A_AUDIT	OE_AUDIT requires the user to monitor alarms and an administrative user to regularly review SNMP Logs,security event logs and UAL,as assumed in A_AUDIT. Also OE_AUDIT requires that appropriate corrective actions, according to Nokia recommendations for managing the TOE are taken upon potential incident detection as assumed in A_AUDIT.
A_GENERAL_PURPOSE	OE_GENERAL_PURPOSE requires no other services available on the operating system of the TOE other than those necessary for the operation and management. In particular it requires no general-purpose computing capabilities.
A_CONFIGURATION	OE_TOE_CONFIGURATION covers what is assumed in A_CONFIGURATION, since it requires that the TOE and Neighboring Equipment areinstalled and commissioned following Nokia recommendations and procedures in order to properly protect the primary and secondary assets of the TOE. In addition, OE_MNGT_EQPT_SECURED requires that non-TOE components are configured following the vendor security recommendations and settings.
A_ORGANIZATION	OE_ORGANIZATION requires the operational environment and employees to follow organizational policies, guidelines and procedures as assumed in A_ORGANIZATION.
A_PROTECTION	OE_TOE_PROTECTION requires that the TOE and the Neighboring Equipment are located in a controlled and secured zone in order to prevent unauthorized logical and physical access. OE_MNGT_EQPT_PROTECTION requires that the management equipment are located in a controlled and secured zone in order to prevent unauthorized logical and physical access, with at least the same level of physical and logical protection as the TOE. OE_SECONDARY_ASSETS_PROTECTION requires that non-TOE management assets have at least the same level of physical and logical protection as the TOE. Specifically, OE_DB_BACKUPS requires that database backups are securely handled in order to preserve their integrity. Furthermore, OE_DATA_PROTECTION requires that data intended for transmission to the TOE including D_DATA is protected.
A_KGF	OE_KGF requires a key generation functionality compliant with ANSSI requirements regarding cryptography, stated within [RGS_B1].
A_MNGT_NETWORK	OE_MNGT_NETWORK requires a risk analysis to determine how secure should be the management network. In order to use the TOE in a context compliant with a “Qualification Standard” level of security, OE_MNGT_NETWORK recommends using ANSSI approved IPSec encryption devices.

Assumption, Threat or OSP	Rationale
A_MNGT_EQPT_SECURED	OE_MNGT_EQPT_SECURED requires management devices and subsystems to be secured following the vendor security recommendations and settings. Their operating system should be secured.accordingly to applicable security or governmental recommendations depending on the system that uses the TOE.
A_MNGT_EQPT_PROTECTION	OE_MNGT_EQPT_PROTECTION requires physical and logical protection for management devices and subsystems, at least at the same level of protection as the TOE. Furthermore, it requires the overall solution to allow individual access accounting to access those devices.
T_REMOTE_MNGT	Due to the evaluation scope, the threat is countered by environmental measures. The remote management network shall be secured by the environment (OE_MNGT_NETWORK). A risk analysis determines the technical and organisational means and measures. Nearby the TOE, the remote management link is protected by the organisational measures protecting the TOE itself (OE_TOE_PROTECTION). Furthermore, management subsystems (NMS and KMT) shall be protected too (OE_MNGT_EQT_PROTECTION), and their platform shall be properly secured (OE_MNGT_EQT_SECURED). O_AUDIT supports the OE by requiring event record generation for any management operation, and O_ALARM requires the TOE to warm the user when connection is lost with NMS or KMT.
T_LOCAL_MNGT	Due to the evaluation scope, the threat is countered by environmental measures. The local mangement interfaces and communication link are protected thanks to the organisational measures protecting the TOE itself (OE_LOCAL_MNGT and OE_TOE_PROTECTION) Furthermore, management device (EMS) shall be protected too (OE_MNGT_EQT_PROTECTION), and its platform shall be properly secured (OE_MNGT_EQT_SECURED). O_AUDIT supports the OE by requiring event record generation for any management operation.
T_MALICIOUS_UPDATES	This threat is countered by O_SW_UPDATES which requires the TOE to check integrity and authentication of software updates prior to install it, and by O_AUDIT which requires event record generation for security events (software updating is a security event).
T_ADMIN_ERROR	This threat is countered by OE.TRUSTED_ADMIN which ensures that administrators (U.LOCAL_ADMINISTRATOR and U.CENTRAL_ADMINISTRATOR) apply all guidance in a trusted manner. O.AUDIT contributes to the threat coverage by providing audit data generation for all operations (including viewing operations on TOE sensitive assets) performed by the administrators.
T_TSF_FAILURE	This threat is countered by O.SELF_TEST which requires checking of the integrity of the software which enforces security. It is also countered by O_REDUNDANCY which requires redundancy capabilities in order to provide secure state after listed hardware failure.
T_REDUNDANCY_FAILURE	This threat is countered by O.SELF_TEST which requires checking of the integrity of the configuration which enforces security.

Assumption, Threat or OSP	Rationale
T_UNDETECTED_ACTIONS	This threat is covered by O.AUDIT, which requires the TOE to generate audit for security-relevant operations performed by the TOE or concerning protected communication channels, and for actions performed by users. Security objectives for the environment support O.AUDIT by requiring secure management network, secured management devices and a secured SNMPv3 and SSH link: OE_MNGT_NETWORK, OE_MNGT_EQPT_SECURED, OE_MNGT_EQPT_PROTECTION.
T_UNAUTHORISED_ACCESS	The threat is countered by O.MANAGEMENT which requires that management can only be done by authorised entities This security objectives relies on identification & authentication: - O_ACCESS and O_I&A which requires the user to be authenticated before performing any management functions based upon their roles (O_ROLES). Protection of TOE local management communication is ensured through OE_LOCAL_MNGT, as management through MNGT ports is considered in clear text, whatever is the protocol (HTTP over TLS, etc.), due to the evaluation scope. - OE_MNGT_NETWORK which requires a secured remote management network commensurate to the overall security determined through a risk analysis. - OE_MNGT_EQPT_SECURED and OE_MNGT_EQT_PROTECTION which require protection of management devices and subsystems. The following objectives also contribute to the threat coverage: - O.ALARM requiring the TOE to emit an alarm in case of potential intrusion detection. - O.AUDIT ensures that operations (viewing, modification) performed on TOE sensitive assets are logged and that critical security events are generated to indicate TOE operational failures. Therefore, they provide the capability to detect and process errors or attacks after an analysis of audit events and security alarms.
T_TIME_BASE	This threat is covered by the security objective O_TIME_BASE which ensures the time base reliability.
T_RESIDUAL_DATA	This threat is countered by O.RESIDUAL_INFO_CLEARING to ensure that no unused user data remains in TOE's volatile memory.
OSP_CRYPTO_RGS	O_CRYPTO_CONFORMITY requires Layer 1 protection that complies to ANSSI requirements [RGS_B1]. Furthermore, for governmental use and depending on the risk analysis for the management network, O_MNGT_NETWORK requires VPN IPSec devices conformant to ANSSI “Qualification Standard” security level.
OSP_CRYPTO	O_DATA_CONFIDENTIALITY requires the TOE to provide conformity for D_DATA encryption and decryption. O_CRYPTO_CONFORMITY requires the TOE to provide crypto services conformant to ANSSI requirements [RGS_B1] which accepts internationally recognize cryptographic algorithms.
OSP_MANAGEMENT	O_MANAGEMENT requires the TOE to provide a management capability that allows authenticated and authorized users (through O_I&A and O_ROLES) to manage the equipment and its cryptographic functions.

Assumption, Threat or OSP	Rationale
OSP_KEY_ MANAGEMENT	O_KEY_MANAGEMENT exactly requires the provision of mechanisms that allow authenticated and authorized users to securely configure and manage D_CRYPTO_KEYS and D_CONFIG_KEYS. The environment shall maintain their security through procedural and technical means (OE_MNGT_NETWORK, OE_MNGT_EQPT_SECURED, OE_MNGT_EQPT_PROTECTION, OE_SECONDARY_ASSETS_PROTECTION)
OSP_BANNER	O_DISPLAY_BANNER requires the TOE to display a banner at user login to describe restrictions of use and legal agreements by accessing the TOE.

Table 4.1: Security Objective Rationale

5. Extended Components Definition

5.1 Extended TOE Security Functional Family

This Security Target defines new security functional families, which are used to define the security requirements for this ST.

5.1.1 FPT_TUD_EXT – Trusted Update

The FPT_TUD_EXT family, defines requirements for software update and integrity.

5.1.1.1 Definition

Family Behaviour

This family FPT_TUD_EXT (Trusted Update) extends the functional class FPT with the capability to update TSF firmware/software parts.

Component levelling

FPT_TUD_EXT.1 Trusted Update, requires the TSF to provide a trusted firmware/software update mechanism.

Management: FPT_TUD_EXT.1

There are no management activities foreseen.

Audit: FPT_TUD_EXT.1

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

a) Minimal: Initiation of update.

FPT_TUD_EXT.1	**Trusted Update**
	Hierarchical to: No other components.
	Depedencies: FCS_COP.1 Cryptographic operation
FPT_TUD_EXT.1.1	The TSF shall provide [assignment: list of users or roles] the ability to query the current version of the TOE firmware/software.
FPT_TUD_EXT.1.2	The TSF shall provide [assignment: list of users or roles] the ability to initiate updates to TOE firmware/software.
FPT_TUD_EXT.1.3	The TSF shall provide a means to verify firmware/software updates to the TOE using a [selection: digital signature mechanism, published hash] prior to installing those updates.

5.1.1.2 Rationale

This family was defined because part 2 of [CC] does not contain any SFR which allows specifying requirements about trusted firmware/software update.

5.2 Extended TOE Security Functional Components

This Security Target defines new security functional components, which are used to define the security requirements for this ST.

5.2.1 Class FAU: Security Audit

The FAU class, as defined in CC Part 2, addresses requirements for security auditing.

5.2.1.1 FAU_STG

The FAU_STG family, as defined in CC Part 2, defines requirements for creating, maintaining and storing a security audit trail.

5.2.1.1.1 FAU_STG_EXT

FAU_STG_EXT.1 External Audit Trail Storage specifies that audit records can be transmitted to an external IT entity.

FAU_STG_EXT.2 External Audit Trail Storage specifies that audit records can be transmitted to an external IT entity using a trusted channel.

FAU_STG_EXT.3 Action in Case of Loss of Management Connection specifies actions to be taken when connection to management system is lost.

Management FAU_STG_EXT.1, FAU_STG_EXT.2

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

a) Configuring and maintaining the external IT entity to which the TSF sends the audit records.

Management: FAU_STG_EXT.3

There are no management activities foreseen.

Audit: FAU_STG_EXT.1, FAU_STG_EXT.2

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

a) Basic: Modifying the external IT entity to which the TSF sends the audit records.

Audit: FAU_STG_EXT.3

The following actions should be auditable if FAU_STG_EXT.3 Action in Case of Loss of Management Connection is included in the PP/ST:

a) Minimal: Loss of connection.

FAU_STG_EXT.1	**External Audit Trail Storage**
	Hierarchical to: No other components.
	Depedencies: FAU_GEN.1 Audit data generation
FAU_STG_EXT.1.1	The TSF shall be able to [selection: transmit the generated audit data to an external IT entity, receive and store audit data from an external IT entity].

FAU_STG_EXT.2	**External Audit Trail Storage**
	Hierarchical to: FAU_STG_EXT.1 External audit trail storage.
	Depedencies: FAU_GEN.1 Audit data generation
FAU_STG_EXT.2.1	The TSF shall be able to [selection: transmit the generated audit data to an external IT entity, receive and store audit data from an external IT entity] **using a trusted channel implementing the [selection: Ipsec, SSH, TLS, TLS/HTTPS, SNMPv3] protocol**.

FAU_STG_EXT.3	**Action in Case of Loss of Management Connection**
	Hierarchical to: No other components.
	Dependencies: FAU_STG_EXT.1 External audit trail storage
FAU_STG_EXT.3.1	The TSF shall [assignment: action] when the communication link to the external IT entity remotely managing the TOE is not available.

5.2.1.1.2 Rationale

This family was defined because part 2 of [CC] does not contain any SFR which allows transmitting audit trail to an external storage capability. For the TOE described in this ST it was necessary to provide such capability.

5.3 Extended TOE Security Assurance Components

There are no extended TOE security assurance components defined for this evaluation.

6. Security Requirements

6.1 Security Functional Requirements

The following format will be used to represent assignment, selection, refinement and iteration operations:

- An assignment operation will be identified as normal text in square brackets.
  - [value_1, value_2]
- A selection operation will be identified as italic text in square brackets.
  - [*value_1, value_2*].
- An assignment operation inside a selection operation will be identified as bold italic text in square brackets.
  - [*value_1, **value_2**, value_3*]
- A refinement operation will be identified as bold text for when new text has been inserted into the security functional requirement and strikethrough text will be used when text has been deleted.
  - original_text_1 **new_text** original_text_2 ~~removed_text~~ original_text_3
- An iteration of a security functional requirement will be identified by appending an additional identifier in round brackets next to their original identifier.
  - FCS_COP.1(1).

6.1.1 Security Audit (FAU)

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*] level of audit; and c) [Other auditable events: - Enabling and disabling of any of the auditing and alarming mechanisms; - All time changes; - Use of the defined management functions; - Unsuccessful login; - Key destruction; - Configure and manage cryptographic keys; and - Successful import of user data (keys)].

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, [other audit relevant information: - SNMP log will contain information about the change of the system or network configuration, the source IP address, the user name and the action itself; and - The User Activity Log that contains information about user activity on WebCT interface].
Hierarchical to: Dependencies:	No other components. FPT_STM.1 Reliable time stamps
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.
Hierarchical to: Dependencies:	No other components. FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification
FAU_STG_EXT.1	**External Audit Trail Storage**
FAU_STG_EXT.1.1	The TSF shall be able to [*transmit the generated audit data to an external IT entity*].
Hierarchical to: Dependencies:	No other components. FAU_GEN.1 Audit data generation
FAU_STG_EXT.3	**Action in Case of Loss of Management Connection**
FAU_STG_EXT.3.1	The TSF shall [*warn the user through a visual mean*] when the communication link to the external IT entity remotely managing the TOE **(meaning NMS and KMT)** is not available.
Hierarchical to: Dependencies:	No other components. FAU_STG_EXT.1 External audit trail storage

6.1.2 Cryptographic support (FCS)

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 [Nokia's cryptographic key destruction method] that meets the following: [defined in ADV documentation].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_COP.1(1)	**Cryptographic operation**
FCS_COP.1.1	The TSF shall perform [encryption and decryption of data] in accordance with a specified cryptographic algorithm [AES (as specified in FIPS 197) encryption in CTR mode] and cryptographic key sizes [256 binary digits in length] that meet the following: [RGS_B1].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1(2)	**Cryptographic operation**
FCS_COP.1.1	The TSF shall perform [software update cryptographic signature verification] in accordance with [SHA512 and RSA Digital Signature Algorithm] and cryptographic key sizes [4096 bits] that meet the following: [- FIPS 180-4 (Secure Hash Standard, SHS) - FIPS 186-4 (Digital Signature Standard)].
Application note:	*This requirement is for software updates.* The correctness of the SHA512 and RSA Digital Signature Algorithm cryptographic implementation regarding FIPS standards is not covered by this evaluation and the algorithms have not yet been FIPS certified. It is covered by vendor assertion.
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes,

	or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

6.1.3 User Data Protection (FDP)

The **Access Control Policy** uses the following definitions:

The subjects are

- a user or process attempting to perform configuration and advanced equipment and service management functions.

The objects are

- MIBs which store the TOE Secondary Assets outlined in Table 3.2: TOE Secondary Assets.
- Software

The operations that can be performed with the MIB objects are

- read-view (reading an object)
- write-view (writing an object)
- notify-view (sending objects in a notification)

The operation that can be performed with the Software object is

- update

FDP_ACC.1	**Subset access control**
FDP_ACC.1.1	The TSF shall enforce the [Access Control Policy] on [• Subjects: Users or processes attempting to perform management functions using an SNMP MIB • Objects: MIBs • Operations: read-view, write-view, notify-view].
Hierarchical to: Dependencies:	No other components. FDP_ACF.1 Security attribute based access control
FDP_ACF.1	**Security attribute based access control**
FDP_ACF.1.1	The TSF shall enforce the [Access Control Policy] to objects based on the following: [Subject Security Attributes: Role(s) assigned Object Security attributes: role / access rights (read-view, write-view, notify-view, update)].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

	- the user's role must be assigned the requested access right in the object's set of security attributes].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [- The IP address of the remote device (NMS or KMT) is an authorized address.]
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [- Software update performed from remote management system (NMS or KMT)].
Hierarchical to: Dependencies:	No other components. FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ITC.1	**Import of user data without security attributes**
FDP_ITC.1.1	The TSF shall enforce the [Access Control Policy] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [no additional rules].
Hierarchical to: Dependencies:	No other components. [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation

6.1.4 Identification and Authentication (FIA)

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.
Hierarchical to: Dependencies:	FIA_UAU.1 Timing of authentication. FIA_UID.1 Timing of identification.
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.
Hierarchical to:	FIA_UID.1 Timing of identification.
Dependencies:	No dependencies.
FIA_AFL.1	**Authentication failure handling**
FIA_AFL.1.1	The TSF shall detect when [**5**] unsuccessful authentication attempts occur related to [the user authentication functionality].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall : [- Send an alert message (FAU_STG_EXT.1) - Lock the authentication functionality for a period of time (180 seconds times the number of locks : 180 seconds the first time the authentication is locked, 360 seconds the second time, 540 seconds the third time, …) - After the locking duration, authentication functionality the TSF shall unlock the authentication functionality: the user can try again to log on (FIA_AFL.1.1).]
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication.
FTA_SSL.3	**TSF-initiated termination**
FTA_SSL.3.1	The TSF shall terminate an interactive session after a [10 minutes of user inactivity].
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SSL.4	**User-initiated termination**
FTA_SSL.4.1	The TSF shall allow user-initiated termination of the user's own interactive session.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_TAB.1	**TOE access banner**
FTA_TAB.1.1	Before establishing a user session, the TSF shall display **a security specific** advisory **notice and consent** warning message regarding unauthorised use of the TOE.
Application note :	*This requirement is only for logon via HTTPS.*

Hierarchical to:	No other components.
Dependencies:	No dependencies.

6.1.5 Security Management (FMT)

FMT_SMF.1	**Specification of Management Functions**
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [- Management of the configuration of IO cards, ports, interfaces and circuits. - Software update - Management of user logoff. - Management of security and privilege information. - Management D_CONFIG_MANAGEMENT. - Management of cryptographic functions. -].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FMT_SMR.1	**Security roles**
FMT_SMR.1.1	The TSF shall maintain the roles [Crypto Officer, and Administrator].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

6.1.6 Protection of the TSF (FPT)

FPT_STM.1	**Reliable time stamps**
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_TST.1	**TSF testing**
FPT_TST.1.1	The TSF shall run a suite of self tests [*during initial start-up*] to demonstrate the correct operation of [*cryptographic functions*].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of [*TSF configuration data*].

FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of [*TSF software part*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_RCV.2	**Automated recovery**
FPT_RCV.2.1	When automated recovery from [COREVO main failure, Integrity check failure] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.
FPT_RCV.2.2	For [COREVO main failure or MPT main failure], the TSF shall ensure the return of the TOE to a secure state using automated procedures **(COREVO (respectively MPT) switching)**.
Hierarchical to:	FPT_RCV.1
Dependencies:	AGD_OPE.1

FPT_TUD_EXT.1	**Trusted Update**
FPT_TUD_EXT.1.1	The TSF shall provide **Crypto Officer, Administrator, NMS and KMT** the ability to query the current version of the TOE firmware/software.
FPT_TUD_EXT.1.2	The TSF shall provide **Administrator and NMS** the ability to initiate updates to TOE firmware/software.
FPT_TUD_EXT.1.3	The TSF shall provide a means to verify firmware/software updates to the TOE using a [*digital signature mechanism*] prior to installing those updates.
Hierarchical to:	No other components.
Dependencies:	FCS_COP.1 Cryptographic operation

6.2 Security Assurance Requirements

The security target claims an EAL3 security assurance level augmented with AVA_VAN.3 and ALC_FLR.3.

Class	Component
Development	**ADV_ARC.1** Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
Guidance Documents	**AGD_OPE.1** Operational user guidance

Class	Component
	AGD_PRE.1 Preparative procedures
Lifecycle Support	**ALC_CMC.3** Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model
Security Target	**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
Tests	**ATE_COV.2** Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability Assessment	**AVA_VAN.3** Vulnerability analysis

Table 6.1: Security Assurance Components

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

The following table provides an overview for security functional requirements coverage also giving an evidence for sufficiency and necessity of the SFRs chosen.

	O_ACCESS	O_ALARM	O_AUDIT	O_CRYPTO_CONFORMITY	O_DATA_CONFIDENTIALITY	O_MANAGEMENT	O_TIME_BASE	O_REDUNDANCY	O_SW_UPDATES	O_KEY_MANAGEMENT	O_ROLES	O_I&A	O_DISPLAY_BANNER	O_SELF_TESTING	O_RESIDUAL_INFO_CLEARING
FAU_GEN.1 Audit data generation		X	X												
FAU_GEN.2 User identity association			X												
FAU_STG_EXT.1 External Audit Trail Storage			X												
FAU_STG_EXT.3 Action in Case of Loss of Management Connection		X													
FCS_CKM.4 Cryptographic key destruction					X										X
FCS_COP.1(1) Cryptographic operation				X	X										
FCS_COP.1(2) Cryptographic operation				X					X						
FDP_ACC.1 Subset access control					X	X				X					
FDP_ACF.1 Security attribute based access control					X	X				X		X			
FDP_ITC.1 Import of user data without security attributes					X										
FIA_UAU.2 User authentication before any action	X		X			X				X		X			
FIA_UID.2 User identification before any action	X		X		X	X				X	X	X			
FIA_AFL.1 Authentication failure handling												X			
FTA_SSL.3 TSF-initiated termination												X			
FTA_SSL.4 User-initiated termination												X			
FTA_TAB.1 TOE access banner													X		
FMT_SMF.1 Specification of Management Functions					X	X				X	X	X			
FMT_SMR.1 Security roles					X	X				X	X	X			
FPT_STM.1 Reliable time stamps		X	X				X								
FPT_TST.1 TSF testing														X	
FPT_RCV.2 Automated recovery								X							
FPT_TUD_EXT.1 Trusted Update									X						

Table 6.2: Security Requirements to Security Objectives Mapping

A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given in the following table.

Security Objective(s)	Rationale
O_ACCESS	O_ACCESS requires the TOE to protected against non-authorized logical access and provide mechanisms for authenticating users before granting access to the functions. The security functional requirements FIA_UAU.2 and FIA_UID.2 require the TOE to implement a user identification and authentication before allowing any other TSF-mediated actions on behalf of that user as demanded by O_ACCESS. Therefore, FIA_UAU.2 and FIA_UID.2 are suitable to meet the security objective.
O_ALARM	The security objective is covered as follows. FAU_STG_EXT.3 requires the TOE to notify the user when a NMS or KMT connection loss occurs. FAU_GEN.1 defines the generation of audit records more precisely and FPT_STM.1 provides these records with reliable time stamps.
O_AUDIT	O_AUDIT requires the TOE to provide logs which are write-protected and only accessible to an Administrator. The SFR FAU_GEN.2 requires for audit events resulting from actions of identified users an association of each auditable event with the identity of the user that caused the event. Therefore, the audit records must reliably be generated as defined by FAU_GEN.1 and FPT_STM.1. The users must be identified and authenticated as defined by FIA_UID.2 and FIA_UAU.2 to bind actions to a user.The SFR FAU_STG_EXT.1 requires audit records be sent to an external IT entity for storage and viewing. All SFRs mentioned exactly require to implement SNMP Logs, security event logs and user activity log as defined by O_AUDIT.
O_CRYPTO_CONFORMITY	The security requirement FCS_COP.1 defines the cryptographic operations, encryption and decryption, in more detail. AES 256 that meet the FIPS 140-2 L2 standard and ANSSI RGS Annex B1 shall be provided.

Security Objective(s)	Rationale
O_DATA_CONFIDENTIALITY	O_DATA_CONFIDENTIALITY requires the TOE to protect the confidentiality of D_DATA. This is fulfilled by the security functional requirements FCS_COP.1(1) and its dependent SFRs. FCS_COP.1(1) depends on FDP_ITC.1 and FCS_CKM.4. Whereas, FDP_ITC.1 describes the import of user data without security attributes and is related to the Security Function Policy (SFP) “Access Control Policy”. The keys are stored in volatile memory and the key data is lost upon power-off or the extraction of the cryptographic module from the TOE. For key replacement, the encryption module provides a procedural method controlled via the management interface that includes overwriting the volatile key in RAM at least once. In addition, the dependend security functional requirements FDP_ACC.1, FDP_ACF.1, FMT_SMR.1 and FMT_SMF.1 are needed. They are also related to the SFP “Access Contorl Policy”. FDP_ACC.1 and FDP_ACF.1 enforce this SFP on subjects, objects, operations and attributes. The security roles needed and the identification of users are defined within FMT_SMR.1 and FIA_UID.2. Additionally, FMT_SMF.1 specifies management functions for cryptography.
O_KEY_MANAGEMENT	O_KEY_MANAGEMENT requires the TOE to provide authenticated and authorized users management and configuration mechanisms for D_CRYPTO_KEYS, D_CONFIG_KEYS, the equipment and its cryptographic functions. The security functional requirements FDP_ACC.1, FDP_ACF.1, FMT_SMR.1, FMT_SMF.1, FIA_UAU.2 and FIA_UID.2 and the related SFP “Access Control” exactly require to implement this kind of management and configuration mechanisms. FDP_ACC.1 and FDP_ACF.1 enforce the Access Control Policy on subjects, objects, operations and attributes. The security roles and the identification of users are defined within FMT_SMR.1 and FIA_UID.2. Additionally, the users authentication is required within FIA_UAU.2. FMT_SMF.1 specifies different management functions. For example, the management of advanced equipment and service management functions is specified here. Therefore, the mentioned SFRs in combination with the related SFP “Access Control Policy” provide authenticated and authorized users management and configuration mechanisms for the defined objects. In particular, these objects comprise D_CRYPTO_KEYS, D_CONFIG_KEYS, the equipment and its cryptographic functions as demanded by O_KEY_MANAGEMENT and O_MANAGEMENT.

Security Objective(s)	Rationale
O_MANAGEMENT	O_MANAGEMENT requires the TOE to provide authenticated and authorized users management and configuration mechanisms for D_AUDIT, D_CONFIG_KEYS, D_TIME_BASE and D_CONFIG_MANAGEMENT, the equipment and its cryptographic functions. The security functional requirements FDP_ACC.1, FDP_ACF.1, FMT_SMR.1, FMT_SMF.1, FIA_UAU.2 and FIA_UID.2 and the related SFP “Access Control” exactly require to implement this kind of management and configuration mechanisms. FDP_ACC.1 and FDP_ACF.1 enforce the Access Control Policy on subjects, objects, operations and attributes. The security roles and the identification of users are defined within FMT_SMR.1 and FIA_UID.2. Additionally, the users authentication is required within FIA_UAU.2. FMT_SMF.1 specifies different management functions. For example, the management of advanced equipment and service management functions is specified here. Therefore, the mentioned SFRs in combination with the related SFP “Access Control Policy” provide authenticated and authorized users management and configuration mechanisms for the defined objects. In particular, these objects comprise D_AUDIT, D_CONFIG_KEYS, D_TIME_BASE and D_CONFIG_MANAGEMENT, the equipment and its cryptographic functions as demanded by O _MANAGEMENT.
O_TIME_BASE	This objective is covered by the requirement FPT_STM.1.
O_REDUNDANCY	FPT_RCV.2 covers the security objective as it requires automatic recovery in case of COREVO or MPT failure.
O_SW_UPDATES	The security objective is covered by FPT_TUD_EXT.1 which requires software integrity and authentication checking prior installing the update. FCS_COP.1(2) specifies the cryptographic algorithms to be used for this operation.
O.ROLES	The security functional requirement FMT_SMR.1 and FIA_UID.2 require the maintenance of the Administrator and Crypto Officer role as well as the identification before any action of these users. FMT_SMF.1 specifies role management functions. This is exactly required by O_ROLES and therefore O_ROLES is fulfilled.

Security Objective(s)	Rationale
O_I&A	The security objective O_I&A is covered as follows. The security functional requirement FIA_UID.2 and FIA_UAU.2 require the identification and authentication of a user before any action of these users. FMT_SMR.1 requires the TOE to manage user roles, while FMT_SMF.1 specifies role management functions. FIA_AFL.1 specifies the behavior of the TOE in case of user authentication failure. FTA_SSL.3 and FTA_SSL.4 requires TSF and User-initiated session termination. For remote management, FDP_ACF.1 requires the device to be identified before granting it access to management functionalities. FIA_AFL.1 requires the TOE to detect when a configurable number of authentication attempts is met.
O_DISPLAY_BANNER	The security objective is covered by FTA_TAB.1 which requires the TOE to display a banner to the user regarding unauthorized use of the TOE.
O_SELF_TESTING	FPT_TST.1 covers the security objective as it requires TOE self-tests.
O_RESIDUAL_INFO_CLEARING	The security objective is covered by FCS_CKM.4 which requires destruction of D_CRYPTO_KEYS after use.

Table 6.3: Security Objectives to Security Requirements Rationale

6.3.2 Rationale for SFR Dependencies

SFR	Dependencies	Fulfilled by SFRs in this ST
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_STG_EXT.1	FAU_GEN.1	FAU_GEN.1
FAU_STG_EXT.3	FAU_STG_EXT.1	FAU_STG_EXT.1
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1
FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 FCS_CKM.4
FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	--
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 See discussion below.
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1 See discussion below
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	--	--
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FTA_SSL.3	--	--
FTA_SSL.4	--	--
FTA_TAB.1	--	--
FMT_SMF.1	--	--
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_STM.1	--	--
FPT_TST.1	--	--
FPT_RCV.2	AGD_OPE.1	AGD_OPE.1
FPT_TUD_EXT.1	FCS_COP.1	FCS_COP.1(2)

Table 6.4: Dependencies for Security Functional Requirements

The dependencies of FDP_ACF.1 and FDP_ITC.1 address the management of security attributes and their initialisation. The dependency FMT_MSA.3 is not included within this Security Target, since security attributes are only implicitely contained within the definition of subjects. There do not exist any explicitly defined security attributes.

The dependencies of FCP_COP.1(2) address the cryptographic keys used to verify the integrity and authentication:

- The dependency “[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]” is replaced by the software update itself (FPT_TUD_EXT.1) : cryptographic keys are renewed during this operation.
- The dependency “FCS_CKM.4” is unsatisfied otherwise no more software update could be performed after a key erasing.

6.3.3 Security Assurance Requirements Rationale

The TOE evaluation is performed in regards to ANSSI "Qualification" process, claiming a "Standard" assurance level. This level requires a CC EAL3 security assurance level augmented with ALC_FLR.3 and AVA_VAN.3.

7. TOE Summary Specification

The TOE provides the following security services:

- Layer 1 transport protocol encryption
- Secure Management
- Self-testing
- User Authentication, Authorization and Audit Logs
- Redundancy

7.1 Layer 1 transport protocol encryption

The following table provides the rationale and evidence for how the TOE meets each of the SFRs for Cryptographic Support.

SFR	Rationale
FCS_COP.1	The TOE implements AES CTR 256 bits:The MPT contains a FPGA which encrypts all traffic on the radio interface.
FCS_CKM.4	The TOE implements a destruction methods of cryptographic keys when they are no more used.

Table 7.1: Rationale For Cryptographic Support

7.2 Secure Management

The following table provides the rationale and evidence for how the TOE meets each of the SFRs for Secure Management.

SFR(s)	Rationale
FDP_ACC.1 **FDP_ACF.1** **FDP_ITC.1**	The access to management and encryption functions is only possible after successful user authentication and authorization as an Administrator. The MPT session encryption key is an AES-256 key that is imported across an encrypted SNMPv3 link from the KMT.
FMT_SMF.1	An important and critical part of the TOE configuration is the initial configuration, during which the Secure Management interfaces (with NMS and KMT), authentication parameters and other security settings are configured. The initialization of the keys for the Secure Management interfaces is done out-of-band and using pre-shared keys. The TOE performs management functions of initialization; activation and deactivation on fault detection during system startup and provides logging of successful selftest completions and alarms and logs for unsuccessful selftests.

SFR(s)	Rationale
FMT_SMR.1	The TOE provides different user roles for different operators (Administrator, Crypto Officer). Refer to Table *1.4*: User Roles for a list of the functions that can be performed by each role.
FCS_COP.1(2)	The TOE checks the integrity and authentication of software updates after software download and prior installing it. This verification is based on SHA-512 and RSA 4096 bits operations performed on the full software RPM.
FPT_TUD_EXT.1	The TOE offers to the Crypto Officer, the Administrator, the NMS and the KMT the capability to query the current software version It provides also a software update funtionality to Administrator and the NMS, that checks the integrity and authentication of software updates after software download and prior installing it.

Table 7.2: Rationale for Secure Management

7.3 Self-testing

The following table provides the rationale and evidence for how the TOE meets each of the SFRs for Self-test.

SFR(s)	Rationale
FPT_TST.1	A start-up, the TOE performs selt-tests on the software and on the cryptographic functions. After software integrity self test, crypto self test are performed on : - AES CTR - SHA - SHA with RSA signature Self-test results are logged in the audit record. The TOE provides also the Administrator and the Crypto Officer with the capability to request integrity testing on configuration data and on the software.

7.4 User Authentication, Authorization and Audit Logs

The following table provides the rationale and evidence for how the TOE meets each of the SFRs for the SNMP log, security event log and user activity log.

SFR(s)	Rationale
FAU_GEN.1 **FAU_GEN.2**	The TOE will record security relevant user activities in the SNMP log which is in a user-readable format. Each entry in the SNMP log will contain the time and date of the action, the source IP address, the user name and the action itself. The TOE also records the important security relevant events not resulting directly from an SNMP request in the security event log. Each entry will contain the date and time of the alarm, the alarm source (shelf/slot/port), the severity (Critical, Major, Minor, Warning), description of the alarm, alarm type, indicator if a service has been affected, and additional information/data about the alarm.
FAU_STG_EXT.1	The TOE will transmit audit records sent to the SNMP log and security event log to an external IT entity using SNMP v3. The audit records are usually sent to an NMS or external log server.
FAU_STG_EXT.3	The TOE raises an alarm in case of connection loss with the NMS or the KMT.
FIA_UAU.2 **FIA_UID.2** **FIA_AFL.1** **FTA_TAB.1** **FIA_SSL.3** **FIA_SSL.4**	An individual must be successfully authenticated as either an Administrator, or Crypto Officer before the TOE will provide access to any of it's services. In case of too much unsuccessful authentication attempts, the user account is blocked during a period of time. When opening a user session via HTTPS, the TOE displays a security specific advisory notice message regarding unauthorised use of the TOE. The user session is terminated after 3 minutes of user inactivity or at user request.
FPT_STM.1	The TOE maintains a reliable time to be used in time stamps for audit records.

Table 7.3: Rationale for User Authentication, Authorization and Audit Logs

7.5 Redundancy

The following table provides the rationale and evidence for how the TOE meets the SFR regarding redundancy capability.

SFR(s)	Rationale
FPT_RCV.2	The TOE automatically switches from the main COREVO to the satnd-by one is case of main hardware failure. It also automatically switches from the main MPT to the secondary one is case of MPT main hardware failure. In order to be operational, there automatic recovery capabilities has to be configured by the Administrator.

END OF DOCUMENT

