Security Target of
Huawei 3900 Series LTE eNodeB Software

Version: 2.6

Last Update: 2011-10-17

Author: Huawei Technologies Co., Ltd.

Table of Contents

List of figures

List of tables

Changes control

Version	Date	**Author**	Changes to previous version
V0.10	2010-12-13	**Fangxiaolei**	---
V1.3	2011-04-22	**Songzhuo**	Modify as suggestion as expert adviser
V1.4	2011-05-05	**Songzhuo**	Modify as suggestion as expert adviser
V1.5	2011-05-17	**Songzhuo**	Modify as suggestion as expert adviser
V1.6	2011-05-26	**Songzhuo**	Modify as suggestion as expert adviser
V1.7	2011-05-30	**Songzhuo**	Modify as suggestion as expert adviser
V1.8	2011-05-31	**Songzhuo**	Modify as suggestion as expert adviser
V1.9	2011-06-01	**Songzhuo**	Modify as suggestion as expert adviser
V2.0	2011-06-01	**Songzhuo**	Modify as suggestion as expert adviser
V2.1	2011-06-02	**Songzhuo**	Modify as suggestion as expert adviser
V2.2	2011-06-08	**Songzhuo**	Modify as suggestion as expert adviser
V2.3	2011-06-22	**Liubin**	Changed the word “GRE” into “SCTP”
V2.4	2011-08-12	**Jiang Liang**	Modify according to ORs
V2.5	2011-09-01	**Jiang Liang**	Modify according to ORs
V2.6	2011-10-17	**Jiang Liang**	Modify according to ORs

1. Introduction

1 This Security Target is for the CC evaluation of Huawei 3900 Series LTE (Long Term Evolution) eNodeB Software, the TOE Version is V100R004C00SPC100 and is based on Huawei HERT-BBU (Huawei Enhanced Radio Technology-Base Band Unit) V2R7C01.

1.1. ST Reference

Title	Security Target of Huawei 3900 Series LTE eNodeB Software
Version	v2.6
Author	Fang Xiaolei, Song Zhuo
Publication Date	2011-10-17

1.2. TOE Reference

TOE Name	Huawei 3900 Series LTE eNodeB Software (a.k.a. eNodeB)
TOE Version	V100R004C00SPC100
TOE Developer	Huawei

1.3. TOE Overview

2 3GPP Long Term Evolution (LTE), is the latest standard in the mobile network technology tree that produced the GSM/EDGE and UMTS/HSDPA network technologies. It is a project of the 3rd Generation Partnership Project (3GPP), operating under a name trademarked by one of the associations within the partnership, the European Telecommunications Standards Institute.

3 The current generation of mobile telecommunication networks is collectively known as 3G (for "third generation"). Although LTE is often marketed as 4G, first-release LTE does not fully comply with the IMT Advanced 4G requirements. The pre-4G standard is a step toward LTE Advanced, a 4th generation standard (4G) of radio technologies designed to increase the capacity and speed of mobile telephone networks. LTE Advanced is backwards compatible with LTE and uses the same frequency bands, while LTE is not backwards compatible with 3G systems.

4 Huawei 3900 series LTE eNodeB is the base station in LTE radio networks. Its coverage and capacity are expanded through multi-antenna technologies, its maintainability and testability are improved, and thus it provides subscribers with the wireless broadband access services of large capacity and high quality.

5 The ST contains a description of the security objectives and the requirements, as well as the necessary functional and assurance

measures provided by the TOE. The ST provides the basis for the evaluation of the TOE according to the Common Criteria for Information Technology Security Evaluations (CC).

1.3.1. TOE usage

6 The TOE can be widely used to support the broadband wireless access of home and enterprise users. Besides, it is used to support mobile broadband access. In Huawei LTE solution, the TOE adopts a star topology, in which the transmission equipment is directly connected to the BS through FE or GE ports. The TOE networking supports various access modes, including the FE, GE, optical fibber, x digital subscriber line (xDSL), passive optical network (PON), microwave access, and satellite.

7 The TOE possesses the following features:

1. Eight-antenna MIMO, increasing coverage with fewer sites;
2. High integration, reducing the overall size;
3. On an all-IP platform, thus supporting smooth upgrade;
4. Industry-leading technologies, delivering excellent performance;
5. Easy maintenance through the Web LMT; Flexible networking.

8 The major security features implemented by the TOE and subject to evaluation are:

A. Authentication

9 Operators using local access to the TOE in order to execute device management functions are identified by individual user names and authenticated by passwords.

10 Authenticated access through the integrated port is enforced using SSL client authentication.

B. Access control

11 The TOE implements role-based access control, limiting access to different management functionality to different roles as defined in administrator-defined access control associations.

C. Auditing

12 Audit records are created for security-relevant events related to the use of the TOE.

D. Communications security

13 The TOE offers SSL/TLS channels for FTP, MML (man-machine language, which is a kind of Command Line Interface), and BIN (Huawei's private binary message protocol) access to the TOE.

E. UU Interface encryption

14 The TOE air interface support AES and SNOW 3G service data encryption, which ensures the privacy of user session.

F. S1 Interface encryption

15 The IPSec protocol is used in the communication with the MME/S-GW.

G. X2 Interface encryption

16 The IPSec protocol is used in the communication with other LTE eNodeBs.

H. Resource management

17 VLAN (Virtual Local Area Network) are implemented to separate the traffic from different flow planes, which reduce traffic storms and avoid resource overhead.

18 ACL (Access Control List) implements packet filtering features to restrict resource use via IP address, ports, etc. Those features protect the TOE against various unauthorized access from unauthorized NEs.

I. Security function management

19 The TOE offers management functionality for its security functionality.

J. Digital signature

20 In the production and distribution phases, the digital signature scheme, protect the software package by message digest and signature.

1.3.2. TOE type

21 The TOE comprises management and control software that is deployed into a LTE eNodeB base station. That software includes identification and authentication, system access control, audit management, enforcement of network transmission against data peeking, management functionality to manage the security functions of LTE eNodeB, and digital signature validation to guarantee the confidentiality and integrity of the software packages that are deployed.

22 It complies with 3GPP standards. A LTE/SAE system consists of the EPC Network/Backhaul Network/Radio Network/Terminal Network. The LTE eNodeB provides subscribers with wireless broadband access services of large capacity and high quality.

23 Figure 1 shows the position of the TOE in a LTE/SAE network.

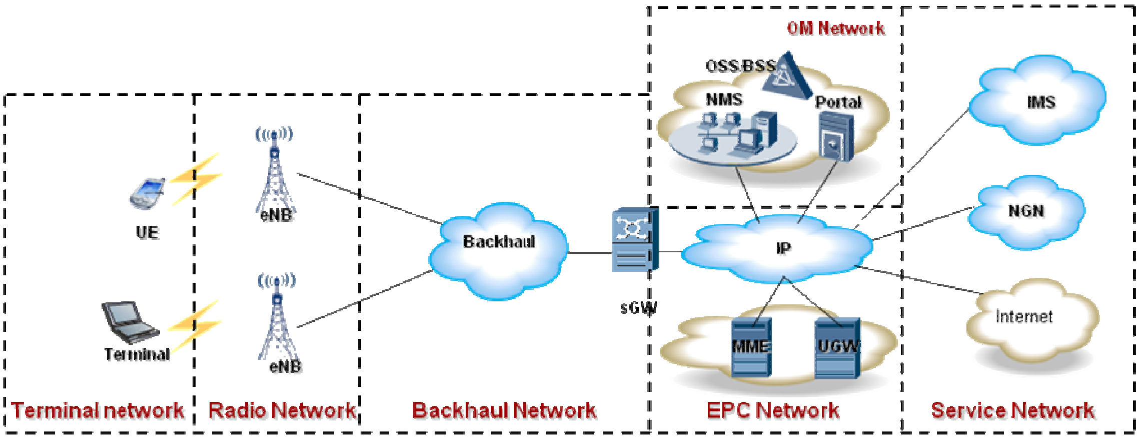


***Figure 1** LTE/SAE network*

24 The UE/Terminal is the subscriber terminal in the LTE network. With the UE/Terminal, the subscriber gains access to the services provided by the operator and Service Network.

25 The eNB is LTE eNodeB, which provides wireless access service for the UE/Terminal.

26 The EPC network is the Evolved Packet Core network and consists of the MME (Mobility Management Entity), the SGW (Service Gateway) and UGW (User plane Gateway). It performs functions such as mobility management, IP connection, QoS management, and billing management.

27 The NMS is Network Management System, which provides network management to LTE eNodeB.

1.3.3. Non TOE Hardware and Software

28 The TOE runs into the BBU3900 subrack and in the RRU. The structure of BBU3900 is shown in the following figure:

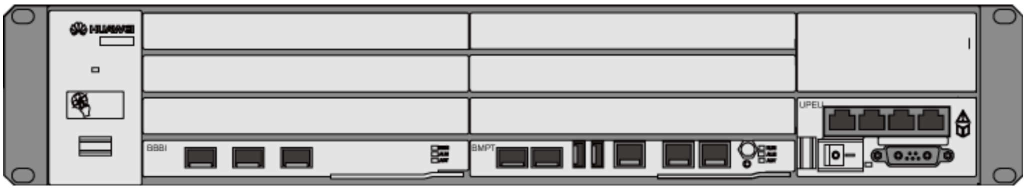


***Figure 2** BBU3900 subrack*

29 The BBU3900 contains, at least, the following mandatory boards:

- The LTE Baseband Processing and radio Interface Unit (LBBI), whose purpose is to provide an interface between BBU3900 and Radio Remote Unit (RRU).

- The LTE Main Processes and Transmission unit (LMPT), which is the main board of BBU3900. It controls and manages the entire BS system, provides clock synchronization signals for the BS system and provides the S1/X2 interface for transmission.
- The Universal Power and Environment Interface Unit (UPEU), whose purpose is providing power to the whole BBU3900 subrack.
- The FAN unit of the BBU3900 controls the fan speed, monitors the temperature of the FAN unit, and dissipates the heat from the BBU.

30 The TOE is LTE eNodeB software packages. It is deployed on the boards of base band unit (BBU) and Remote Radio Unit (RRU). These hardware boards are TOE environment. The OS and part of BS software which is provided by Huawei's particular products are also TOE environment.

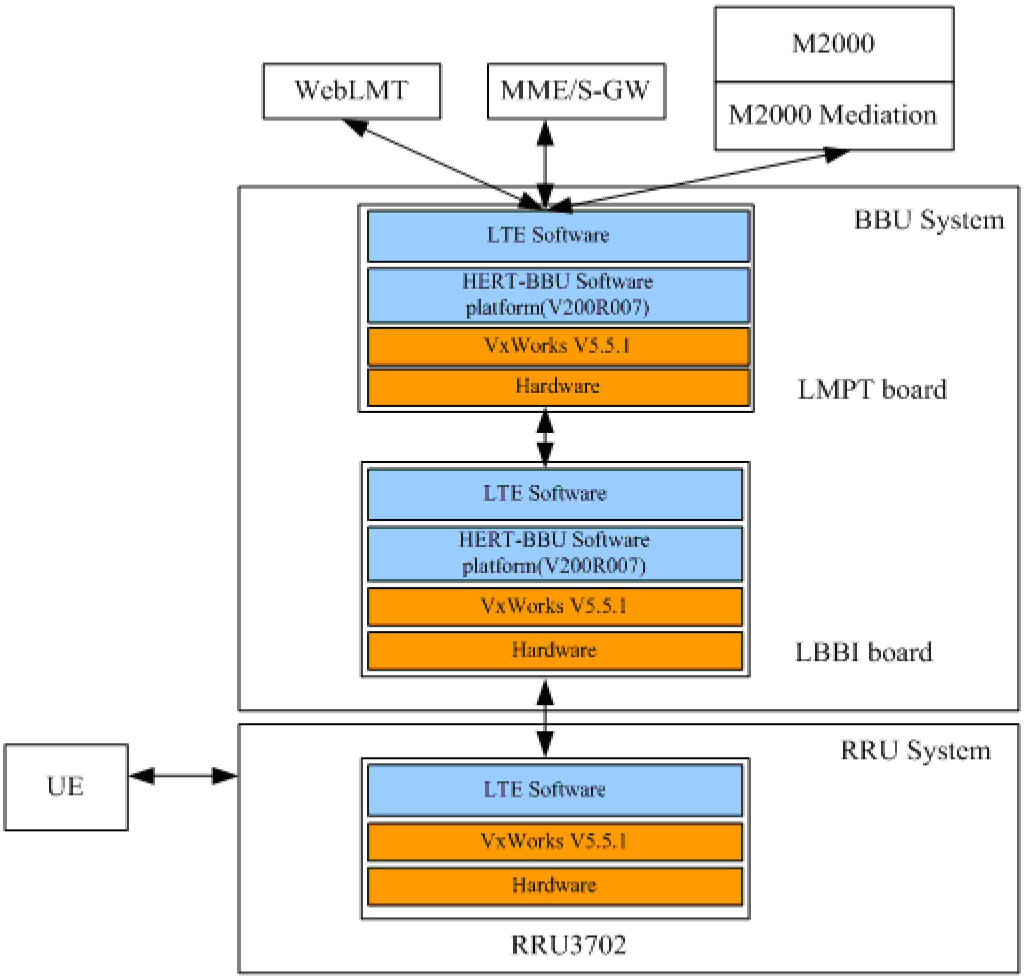


Figure 3 *Non TOE hardware and software environment*

31 In the above diagram, the light blue box area belongs to the TOE while the orange box area belongs to the TOE environment.

32 The components of the TOE environment are the following:

- Physical networks, such as Ethernet subnets, interconnecting various networking devices.

- LTE eNodeB Operating System: Vxworks, version 5.5.1.

- An M2000 server providing access to the management functions of the TOE via SSL. M2000 version must be V2R11.

- M2000 Mediation Software: The M2000 server software consists of the main version software and mediation software. The main version software implements system functions, and the mediation software is used for the adaptation of different NE interfaces. The M2000 can manage new NEs after the corresponding mediation software is installed.

- The physical structure of LTE eNodeB includes BBU3900 and RRU. BBU3900 is based on HERT hardware platform. HERT BBU is a common platform for wireless multiple products, different boards can be configured according to each product. Beside the hardware support platform subsystem, in most cases only need to configure the LTE Main Processes and Transmission board (LMPT) and LTE BaseBand processing (LBBI)

- S-GW: Serving Gateway, Within the EPC the S-GW is responsible for tunnelling user plane traffic between the eNB and the PDN-GW. To do this its role includes acting as the mobility anchor point for the User Plane during handovers between eNB as well as data buffering when traffic arrives for a mobile in the LTE Idle state. Other functions performed by the S-GW include routing, Lawful Interception and billing.

- MME: Mobility Management Entity terminates the control plane with the mobile device.

- UE: User Equipment, by air interface data encryption, can share the wireless access through LTE network.

- RRU: The RRU is the remote radio unit (RRU) for Huawei Worldwide Interoperability for LTE eNodeB. The RRU mainly performs the following functions:

    - Amplifies weak signals from the antenna system, down-converting the signals to intermediate frequency (IF) signals, performing analog-to-digital conversion, digital down-conversion, filtering, and AGC on the IF signals, and transmitting these signals to the baseband unit (BBU) through the high-speed transmission link

  - o Receives the downlink baseband digital signals from the BBU, performing matched filtering, digital up-conversion, clipping on the signals, modulating the output I/Q differential signals to required TX signals, amplifying the signals, and transmitting them through antennas.

33 The TOE can be deployed in one of the following physical configurations with no changes in the functionality, or in the installation procedures to be followed:

- DBS3900 LTE FDD: Distributed base station. The DBS3900 LTE FDD is characterized by its small footprint, easy installation, and low power consumption. Therefore, the DBS3900 LTE FDD can be easily installed in a spare space at an existing site. The RRU is also compact and light. It can be installed close to the antenna to reduce feeder loss and to improve system coverage. With these characteristics, the DBS3900 LTE FDD fully addresses operators' concern over site acquisition and reduces network deployment time. Therefore, the DBS3900 LTE FDD enables operators to efficiently deploy a high-performance LTE network with a low Total Cost of Ownership (TCO) by minimizing the investment in electricity, space, and manpower.

  The DBS3900 LTE FDD has flexible applications to meet the requirement of fast network deployment in different scenarios.

- DBS3900 LTE TDD: Distributed base station. The DBS3900 LTE TDD, a future-oriented E-UTRAN NodeB (eNodeB) product launched by Huawei, is a distributed eNodeB supporting TDD. The DBS3900 LTE TDD fully exploits Huawei platform resources and uses a variety of technologies.

  The DBS3900 LTE TDD is characterized by its small footprint, easy installation, and low power consumption. Therefore, the DBS3900 LTE TDD can be easily installed in a spare space at an existing site. The RRU is also compact and light. It can be installed close to the antenna to reduce feeder loss and to improve system coverage. With these characteristics, the DBS3900 LTE TDD fully addresses operators' concern over site acquisition and reduces network deployment time. Thus, the DBS3900 LTE TDD enables operators to efficiently deploy a high-performance LTE network with a low Total Cost of Ownership (TCO) by minimizing the investment in electricity, space, and manpower.

  The DBS3900 LTE TDD has flexible applications to meet the requirement of fast network deployment in different scenarios.

- BTS3900 LTE: Indoor cabinet macro base station. The BTS3900 LTE is a compact indoor macro eNodeB. It applies to the scenarios of centralized installation and replacement of traditional macro base stations.

The BTS3900 LTE provides the following features:

  - The BBU3900 and RFUs are installed in the BTS3900 LTE in centralized mode. This helps to reduce the cost of maintenance on the tower.
  - The BTS3900 LTE provides compact size, low weight, large space, and excellent scalability, and it supports stack installation and combined installation of two BTS3900s.
  - The BTS3900 LTE, BTS3900 GSM, and BTS3900 UMTS can share one indoor macro cabinet. This saves installation space and facilitates smooth evolution.

- BTS3900A LTE: Outdoor cabinet macro base station. The BTS3900A LTE is a compact outdoor macro eNodeB. It applies to the scenarios of centralized installation and replacement of traditional macro base stations.

  The BTS3900A LTE provides the following features:

  - The BBU3900 and RFUs are installed in the BTS3900A LTE in centralized mode. This helps to reduce the cost of maintenance on the tower.
  - The BTS3900A LTE supports stack installation. This reduces the weight of a single cabinet and facilitates transportation.
  - The BTS3900A LTE, BTS3900A GSM, and BTS3900A UMTS can share RFCs. This saves installation space and facilitates smooth evolution.

- BTS3900L LTE: Large indoor cabinet macro base station. The BTS3900L LTE is a compact indoor macro eNodeB. It applies to the scenarios of centralized installation and replacement of traditional macro base stations.

  The BTS3900L LTE has the following features:

  - The BBU3900 and RFUs are installed in the BTS3900L LTE in centralized mode. This helps to reduce the cost of maintenance on the tower.
  - The BTS3900L LTE provides compact size, low weight, large space, and excellent scalability, and it supports combined installation of two BTS3900Ls.

- o The BTS3900L LTE, BTS3900L GSM, and BTS3900 UMTS can share one indoor macro cabinet. This saves installation space and facilitates smooth evolution.

1.4. TOE Description

1.4.1. Logical Scope

34 This section will define the logical scope of the TOE. The software architecture of the TOE is indicated in the following figure:

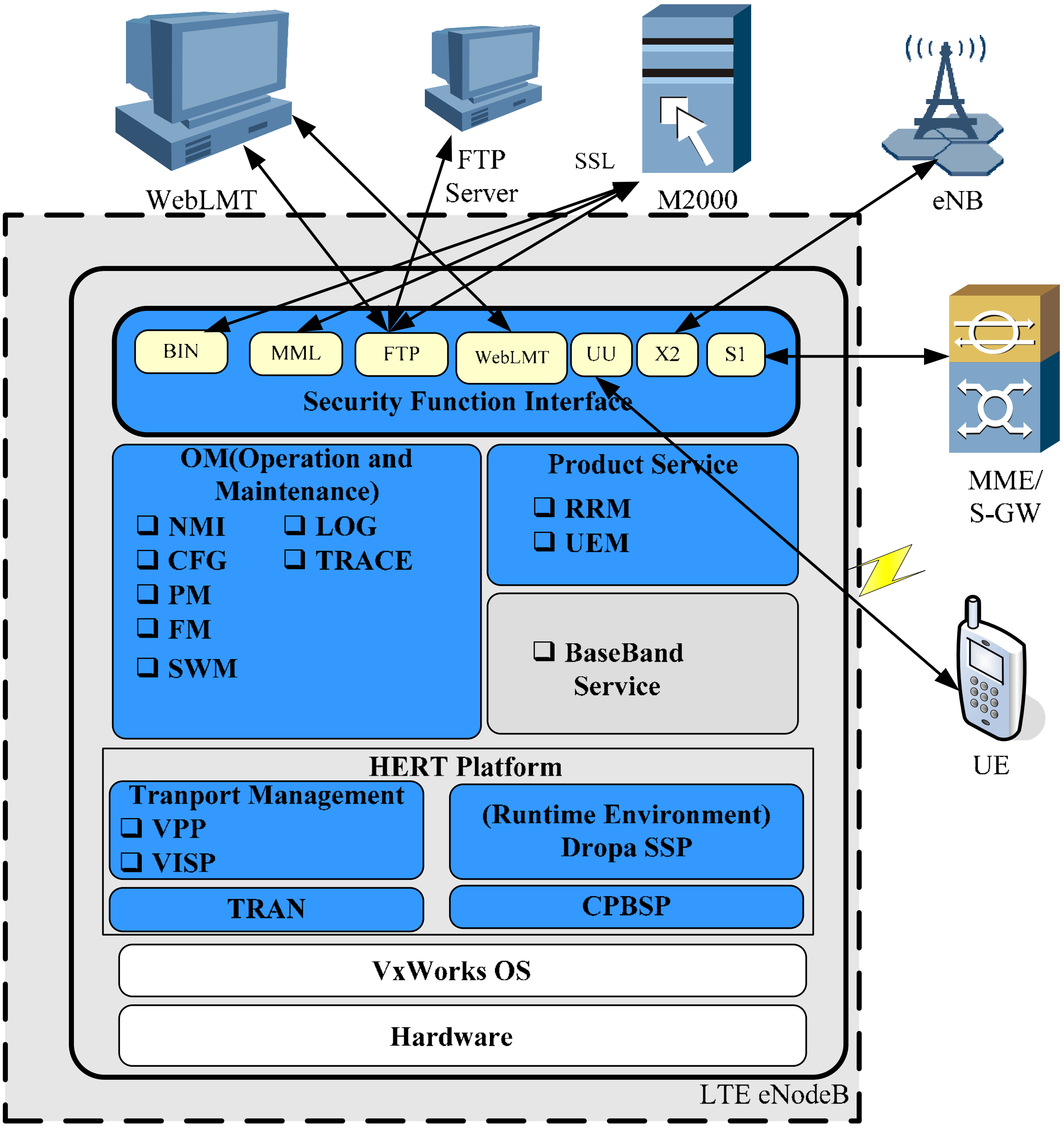


Figure 4 *Software architecture*

35 An explanation of each identified part is described below.

36 From the Logical point of view, the following figure includes the TOE Logical Scope, where all the connections to the TOE are indicated, and also the way the TOE is deployed in the different boards of the product.

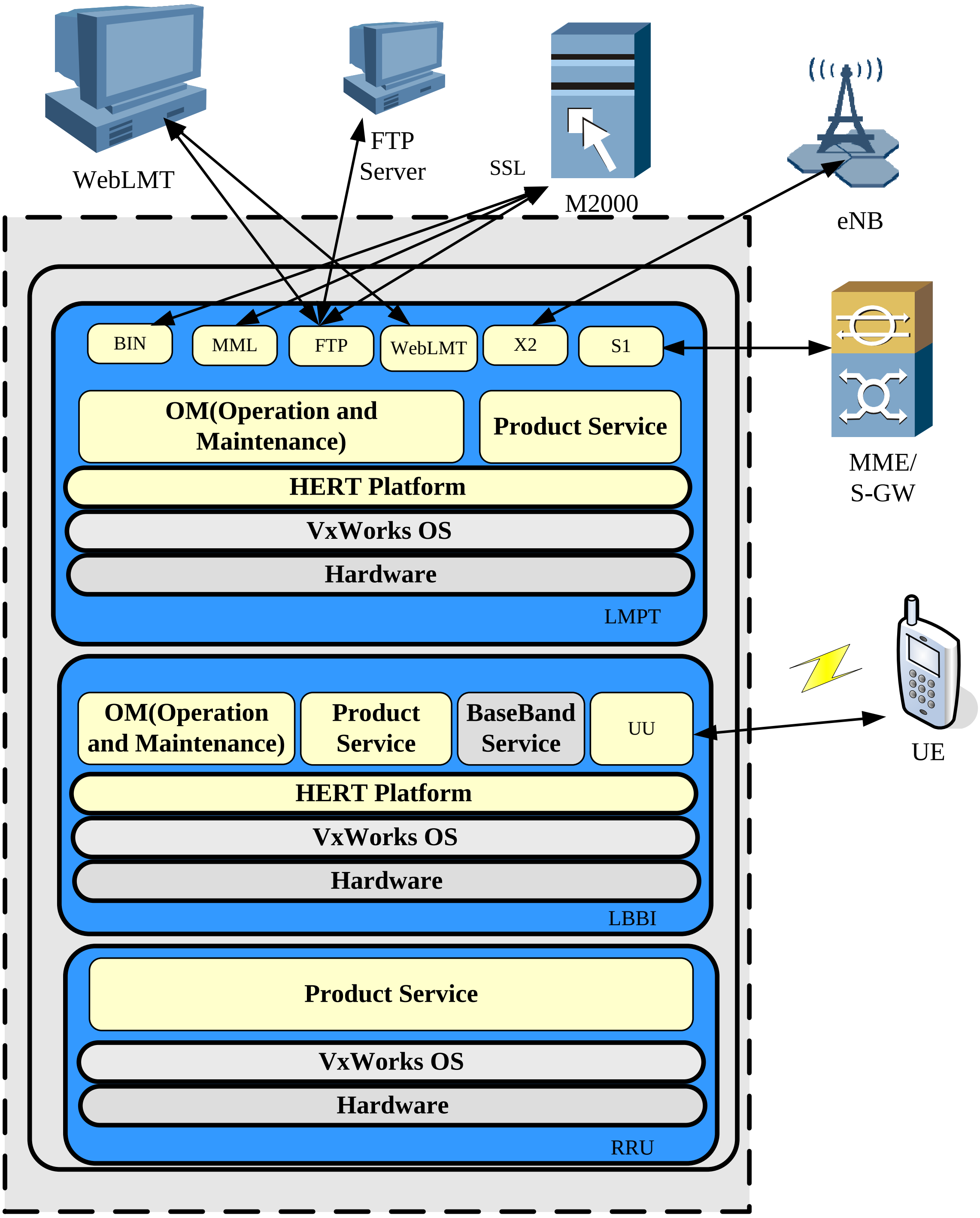


***Figure 5** TOE Logical Scope*

37 The TOE is pure software. OS and other software provided by particular products is TOE environment. In the above diagrams, the content of the blue areas (excluding the grey boxes) are parts of the

TOE. The TOE includes Operation and Maintenance (OM), Product Service, and HERT platform.

38 The TOE security functionality, as stated in the section **1.3 TOE Overview** is:

- Authentication.
- Access control.
- Auditing.
- Communications security.
- UU Interface encryption
- S1 Interface encryption
- X2 Interface encryption
- Resource management.
- Security functionality management.
- Digital signature.

39 As shown in ***Figure 4*** *Software Architecture*, the TOE is entirely composed by software. The Operating System, and other software provided by particular products belong to the TOE environment. The TOE itself includes OM, Product Service, Transport Management, TRAN, CPBSP and Dopra SSP.

40 For each of the identified parts of the TOE, a correspondence between them and the TOE security functionality can be achieved. That way, for each part, the appropriate security associated functionality is indicated in the following table:

Element	Part	Associated security functionality
Security Function Interface	All the interfaces	Resource management
	UU: interface with the User Equipment	UU Interface encryption
	S1: Interface with the MME/S-GW	S1 Interface encryption
	X2: Interface with other eNodeBs.	X2 Interface encryption
	Communications through the following	Communications

	protocols: BIN: Huawei's private binary message protocol. MML: Man-Machine Language. FTP: File transmission Protocol	security
Operation and Maintenance (OM)	NMI: network management interface: which is the interface for external element	NA
	CFG: Configuration Management, responsible for the managed element configuration.	Security functionality management
	PM: Performance management, responsible for the calculation of performance data and the storage of it.	NA
	FM: Fault management, which include fault and alarm monitoring.	NA
	SWM: Software management, responsible for software upgrade and rollback.	Digital signature
	LOG: Responsible for the audit and storage of security log and operational log.	Auditing
	TRACE: Responsible for the trace messages which show the state of the eNodeB and UE within the LTE network.	NA
HERT Platform Transport Management (TM)	VPP: Voice Protocol Platform, which is composed of voice and signal processing component, such as XML Parser, Stream Control Transmission Protocol (SCTP) and Signaling ATM Adaptation Layer (SAAL). VISP: Versatile IP and Security Platform, which provides TCP / IP protocol stack management interface.	Communication Security
HERT Platform TRAN	Huawei's wireless transmission platform, which provide hardware driver management interface.	Communication Security
HERT Platform Dopra SSP (Runtime Environment)	Provide Operating System mid-ware layer. It function includes: Operation System Adapter, Memory management, Timer management, etc.	NA

CPBSP	Provide a standard API interface for the hardware.	NA
Product Service	Radio resource management (RRM): Responsible for the management of all wireless resources, such as site, sector, carrier frequency, etc., including the establishment, monitoring, modify, and delete	NA
	User entity management (UEM): Deal with the user call control management and signal processes in control plane, such as network entrance signal flow, traffic and connection management, security, end-state machine, etc.	NA

41 System control and security management are performed on LMPT board via a secure channel enforcing SSL. The management of the functionality of the TOE can be done through different interfaces:

- BIN/MML through an M2000 server providing management functions to the TOE (in the TOE environment).
- WebLMT used by users to connect to the TOE for access through LMPT via a secure channel enforcing SSL.

1.4.2. Physical Scope

42 The release packages for LTE eNodeB are composed of software and documents. The LTE eNodeB software packages are in the form of binary compressed files.

43 The LTE eNodeB software packages can be downloaded and stored in the LMPT board, and then, they will be checked up, unpacked, and then distributed to each board module.

44 The list of the files and documents required for the products is the following:

Software and Documents	Description	Remark
Software.csp	Board software package (In the form of binary compressed files)	The software packages which are the TOE will be digitally signed to ensure their legitimacy and integrity.
Firmware.csp	BootROM package (In the form of binary compressed files)	

Software and Documents	Description	Remark
LTE eNodeB Software documents	Release notes, MML command reference, and alarm reference.	The guidance documents of LTE eNodeB Software

Table 1 *Physical Scope*

2. Conformance claim

45 This ST is CC Part 2 conformant [CC] and CC Part 3 conformant [CC]. The CC version of [CC] is 3.1R3.

46 This ST is EAL3 conformant as defined in [CC] Part 3, with the assurance level of EAL3 Augmented with ALC_CMC.4, ALC_CMS.4.

47 The methodology to be used for evaluation is CEM3.1 R3

48 No conformance to a Protection Profile is claimed.

3. Security Problem Definition

3.1. TOE Assets

49 The following table includes the assets that have been considered for the TOE:

Asset	Description	Asset value
A1.Software and patches	The integrity and confidentiality of the system software and the patches when in transit across the management network should be protected from modification and disclosure.	Integrity Confidentiality
A2.Stored configuration data	The integrity and confidentiality of the stored configuration data should be protected. Configuration data includes the security related parameters under the control of the TOE (such as user account information and passwords, audit records, etc).	Integrity Confidentiality
A3. In transit configuration data	The integrity and confidentiality of the configuration data when travelling in the management network.	Integrity Confidentiality
A4. Service	Recoverability in terms of the capacity of recovery in case of denial of service.	Recoverability

Table 2 *TOE assets*

3.2. Threats

50 This section of the security problem definition shows the threats to be countered by the TOE, its operational environment, or a combination of both. The threat agents can be categorized as either:

Agent	Description
Eavesdropper	An eavesdropper from the management network served by the TOE is able to intercept, and potentially modify or re-use the data that is being sent to the TOE.
Internal attacker	An unauthorized agent who is connected to the management network.
Restricted authorized user	An authorized user of the TOE who has been granted authority to access certain information and perform certain actions.

Table 3 *Threats agents*

51 In the first and second cases, the users are assumed to be potentially hostile with a clear motivation to get access to the data. In the last

case, all authorized users of the TOE are entrusted with performing certain administrative or management activities with regard to the managed device. Consequently, organizational means are expected to be in place to establish a certain amount of trust into these users. However, accidental or casual attempts to perform actions or access data outside of their authorization are expected. The assumed security threats are listed below.

3.2.1. Threats by Eavesdropper

Threat: T1.InTransitConfiguration	
Attack	An eavesdropper in the management network succeeds in accessing the content of the BS file while transferring, violating its confidentiality or integrity.
Asset	A3.In transit configuration data
Agent	Eavesdropper

Threat: T2. InTransitSoftware	
Attack	An eavesdropper in the management network succeeds in accessing the content of the BS software/patches while transferring, violating its confidentiality or integrity.
Asset	A1.Software and patches;
Agent	Eavesdropper

3.2.2. Threats by Internal Attacker

Threat: T3.UnwantedNetworkTraffic	
Attack	Unwanted network traffic sent to the TOE will cause the TOE's processing capacity for incoming network traffic to be consumed thus failing to process legitimate traffic. This may further causes the TOE fails to respond to system control and security management operations. The TOE will be able to recover from this kind of situations.
Asset	A4. Service
Agent	Internal Attacker

Threat: T4.UnauthenticatedAccess	
Attack	An attacker in the management network gains access to the TOE disclosing or modifying the configuration date stored in the TOE in a way that is not detected.
Asset	A2.Stored configuration data
Agent	Internal Attacker

3.2.3. Threats by restricted authorized user

Threat: T5.UnauthorizedAccess	
Attack	A user of the TOE authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for.
Asset	A2.Stored configuration data

Agent	Restricted authorized user

3.3. Organizational Policies

3.3.1. P1.Audit

52 The TOE shall provide audit functionality:

- Generation of audit information.
- Storage of audit log.
- Review of audit records.

3.3.2. P2.S1_Encryption

53 The TOE shall encrypt/decrypt of the data exchanged over the S1 interface.

3.3.3. P3.X2_Encryption

54 The TOE shall encrypt/decrypt of the data exchanged over the X2 interface.

3.3.4. P4.UU_Encryption

55 The TOE shall encrypt/decrypt of the data exchanged over the UU interface.

3.4. Assumptions

3.4.1. Physical

A.PhysicalProtection

56 It is assumed that the TOE is protected against unauthorized physical access.

3.4.2. Personnel

A.TrustworthyUsers

57 It is assumed that the organization responsible for the TOE and its operational environment has measures in place to establish trust into and train users of the TOE commensurate with the extent of authorization that these users are given on the TOE. (For example, super users and users that are assigned similar privileges are assumed to be fully trustworthy and capable of operating the TOE in a secure manner abiding by the guidance provided to them.)

3.4.3. Connectivity

A.NetworkSegregation

58 It is assumed that the network interfaces that allow access to the TOE's user interfaces are in a management network that is separated from the UU, S1 and X2 interface networks.

3.4.4. Support

A.Support

59 The operational environment must provide the following supporting mechanisms to the TOE: Reliable time stamps for the generation of audit records.

3.4.5. SecurePKI

A.SecurePKI

60 There exists a well managed protected public key infrastructure. The certificates used by the TOE and its client are managed by the PKI.

4. Security Objectives

4.1. Security Objectives for the TOE

61 The following objectives must be met by the TOE:

O.Authentication

62 The TOE must authenticate users and control the session establishment.

O.Authorization

63 The TOE shall implement different authorization levels that can be assigned to administrators in order to restrict the functionality that is available to individual local users.

O.SecureCommunication

64 The TOE shall provide a secure remote communication channel for remote administration of the TOE via SSL.

O. SoftwareIntegrity

65 The TOE must provide functionality to verify the integrity of the received software patches.

O.Resources

66 The TOE must implement VLAN separation and IP based ACLs to avoid resource overhead.

O.Audit

67 The TOE shall provide audit functionality:

- Generation of audit information.
- Storage of audit log.
- Review of audit records.

O.S1_Encryption

68 The TOE shall encrypt/decrypt of the data exchanged over the S1 interface.

O.X2_Encryption

69 The TOE shall encrypt/decrypt of the data exchanged over the X2 interface.

O.UU_Encryption

70 The TOE shall encrypt/decrypt of the data exchanged over the UU interface.

4.2. Security Objectives for the Operational Environment

OE. PhysicalProtection

71 The TOE (i.e., the complete system including attached interfaces) shall be protected against unauthorized physical access.

OE.NetworkSegregation

72 The TOE environment shall assure that the network interfaces that allow access to the TOE's user interfaces are in a management network that is separated from the networks that the TOE serves over the UU and S1 and X2 interfaces.

OE.TrustworthyUsers

73 Those responsible for the operation of the TOE and its operational environment must be trustworthy, and trained such that they are capable of securely managing the TOE and following the provided guidance.

OE.Support

74 Those responsible for the operation of the TOE and its operational environment must ensure that the operational environment provides the following supporting mechanisms to the TOE: Reliable time stamps for the generation of audit records.

OE. SecurePKI

75 There exists a well managed protected public key infrastructure. The certificates used by the TOE and its client are managed by the PKI.

4.3. Security Objectives rationale

4.3.1. Coverage

76 The following tables provide a mapping of security objectives to the environment defined by the threats, policies and assumptions, illustrating that each security objective covers at least one threat and that each threat is countered by at least one objective, assumption or policy.

	T1.InTransitConfiguration	T2.InTransitSoftware	T3.UnwantedNetworkTraffic	T4.UnauthenticatedAccess	T5.UnauthorizedAccess	A.PhysicalProtection	A.TrustworthyUsers	A.NetworkSegregation	A.Support	A. SecurePKI	P1.Audit	P2.S1_Encryption	P3.X2_Encryption	P4.UU_Encryption
O.Authentication				X	X									
O.Authorization					X									
O.SecureCommunication	X	X			X									
O.SoftwareIntegrity		X												
O.Resources			X											
O.Audit											X			
O.S1_Encryption												X		
O.X2_Encryption													X	
O.UU_Encryption														X
OE.PhysicalProtection				X	X	X								
OE.TrustworthyUsers					X		X							
OE.NetworkSegregation								X						
OE.Support									X					
OE.SecurePKI	X	X			X					X				

Table 4 *Mapping of security objectives*

4.3.2. Sufficiency

77 The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat:

Threat	Rationale for security objectives
T1.InTransitConfiguration	The threat T1.InTransitConfiguration is countered by requiring communications security via SSL for network communication between entities in the management network and the TOE (O.SecureCommunication). A secure PKI will be needed to assure the validity of the used certificates. (OE.SecurePKI)
T2. InTransitSoftware	The threat T2.InTransitSoftware is countered by O.SecureCommunication which establishes a secure communication channel between the TOE and external entities in the management network. A secure PKI will be needed to assure the validity of the used certificates. (OE.SecurePKI) This threat is also countered by O.SoftwareIntegrity: when a software package is loaded, its message digest and signature are verified.

T3.UnwantedNetworkTraffic	The threat T3.UnwantedNetworkTraffic is directly counteracted by the security objective for the TOE O.Resources.
T4.UnauthenticatedAccess	The threat T4.UnauthenticatedAccess is countered by the security objective for the TOE O.Authentication which requires the TOE to implement an authentication mechanism for the local users. The security objective for the operational environment OE.PhysicalProtection contributes to the mitigation of the threat assuring that the software and configuration files stored in the TOE will not be modified.
T5.UnauthorizedAccess	The threat T5.UnauthorizedAccess is countered by the security objective for the TOE O.Authentication which requires the TOE to implement an authentication mechanism for the local users. It is also countered by requiring the TOE to implement an access control mechanism (O.Authorization). It is also countered by requiring the TOE to implement secure communications between TOE and its users (O.SecureCommunication). A secure PKI will be needed to assure the validity of the used certificates. (OE.SecurePKI). The security objective for the operational environment OE.TrustworthyUsers contributes to the mitigation of this threat requiring the users to be responsible with their passwords. The security objective for the operational environment OE.PhysicalProtection contributes to the mitigation of the threat assuring that the software and configuration files stored in the TOE, will not be modified

Table 5 *Sufficiency analysis for threats*

Assumption	Rationale for security objectives
A.PhysicalProtection	This assumption is directly implemented by the security objective for the environment OE.PhysicalProtection.
A.TrustworthyUsers	This assumption is directly implemented by the security objective for the environment OE.TrustworthyUsers.
A.NetworkSegregation	This assumption is directly implemented by the security objective for the environment OE.NetworkSegregation.
A.Support	This assumption is directly implemented by the security objective for the environment OE.Support.
A. SecurePKI	This assumption is directly implemented by the security objective for the environment. OE. SecurePKI

Table 6 *Sufficiency analysis for assumptions*

Policy	Rationale for security objectives
P1.Audit	This policy is directly implemented by the security objective for the TOE O.Audit

P2.S1_Encryption	This policy is directly implemented by the security objective for the TOE O.S1_Encryption
P3.X2_Encryption	This policy is directly implemented by the security objective for the TOE O.X2_Encryption
P4.UU_Encryption	This policy is directly implemented by the security objective for the TOE O.UU_Encryption

Table 7 *Sufficiency analysis for organizational security policy*

5. Security Requirements for the TOE

5.1. Security Requirements

5.1.1. Security Audit (FAU)

5.1.1.1. FAU_GEN.1 Audit data generation

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

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

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

c) [assignment: *The following auditable events:*

i. user activity

1. login, logout (SEC)

2. operation requests (OPE)

ii. user management

1. add, delete, modify (SEC & OPE)

2. password change (OPE)

3. authorization modification (SEC & OPE)

iii. locking, unlocking (manual or automatic) (SEC & OPE)

iv. command group management

1. add, delete, modify (OPE)

]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST. [assignment: *workstation IP (if applicable), user (if applicable), and command name (if applicable).*]

Application note: There are two kinds of log files, security log file and operation log file.

5.1.1.2. FAU_GEN.2 User identity association

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

5.1.1.3. FAU_SAR.1 Audit review

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

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

5.1.1.4. FAU_SAR.3 Selectable Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [assignment: *selection*] of audit data based on [assignment: *date and time range, user name, terminal type, and/or result*.]

5.1.1.5. FAU_STG.1 Protected audit trail storage

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

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

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

FAU_STG.3.1 The TSF shall [assignment: *delete the oldest files*] if the audit trail exceeds [assignment: *the pre-defined limited size of 1Mbyte*].

Application note: For each kind of log file, there are two audit files, when the new file is full, the old one is deleted.

5.1.2. Cryptographic Support (FCS)

5.1.2.1. FCS_COP.1/Sign Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: *digital signature verification*] in accordance with a specified cryptographic algorithm [assignment: *RSA with underlying SHA-256*] and cryptographic key sizes [assignment: *1024bits*] that meet the following: [assignment: *none*]

Application note: This requirement addresses the digital signature verification of the remote loaded software packages.

5.1.2.2. FCS_COP.1/SSL Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: *cipher and decipher of TOE access channels*] in accordance with a specified cryptographic algorithm [assignment: *algorithms supported by SSL/TLS*] and cryptographic key sizes [assignment: *key sizes supported by SSL/TLS*] that meet the following: [assignment: *none*]

Application note: This requirement addresses the encryption of the communication through the WebLMT , the integrated port, or with the FTP servers.

5.1.2.3. FCS_COP.1/UU Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: *cipher and decipher of TOE communication with the UE*] in accordance with a specified cryptographic algorithm [assignment: *AES/SNOW 3G*] and cryptographic key sizes [assignment: *128 bits*] that meet the following: [assignment: *none*]

Application note: This requirement addresses the encryption of the channel with the UE.

5.1.2.4. FCS_COP.1/S1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: *cipher and decipher of TOE communication with the MME/S-GW*] in accordance with a specified cryptographic algorithm [assignment: *algorithms supported by IPSec/IKE*] and cryptographic key sizes [assignment: *key sizes supported by IPSec/IKE*] that meet the following: [assignment: *none*]

Application note: This requirement addresses the encryption of the channel with the MME/S-GW.

5.1.2.5. FCS_COP.1/X2 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: *cipher and decipher of TOE communication with other LTE eNodeB*] in accordance with a specified cryptographic algorithm [assignment: *algorithms supported by IPSec/IKE*] and cryptographic key sizes [assignment: *key sizes supported by IPSec/IKE*] that meet the following: [assignment: *none*]

Application note: This requirement addresses the encryption of the channel with other LTE eNodeB.

5.1.2.6. FCS_CKM.1/SSL Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation methods supported by SSL/TLS*] and cryptographic key sizes [assignment: *key sizes supported by SSL/TLS*] that meet the following: [assignment: *none*]

5.1.2.7. FCS_CKM.1/UU Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *AKA protocol*] and cryptographic key sizes [assignment: *128 bits*] that meet the following: [assignment: *none*]

5.1.2.8. FCS_CKM.1/S1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation methods supported by IPSec/IKE*] and cryptographic key sizes [assignment: *key sizes supported by IPSec/IKE*] that meet the following: [assignment: *none*]

5.1.2.9. FCS_CKM.1/X2 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation methods supported by IPSec/IKE*] and cryptographic key sizes [assignment: *key sizes supported by IPSec/IKE*] that meet the following: [assignment: *none*]

5.1.3. User Data Protection (FDP)

5.1.3.1. FDP_ACC.1/Local Subset access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: *Local access control policy*] on [assignment: *local users as subjects, commands as objects, and execution of commands by local users*].

5.1.3.2. FDP_ACF.1/*Local* Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [assignment: ***Local access control policy*****] to objects based on the following:**

[assignment:

a) local users and their following security attributes:

- ***i. user name***
- ***ii. user group (role)***

b) commands and their following security attributes:

- ***i. command name***
- ***ii. command groups.*****]**

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

[assignment:

if the user belongs to a user group that is assigned to a command group that includes the controlled command, then access is granted.

If the user belongs to the custom user group, and he is associated to the command group that includes the controlled command, then access is granted**]**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: ***If the user name is admin, access is always granted*****]**

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

5.1.3.3. FDP_ACC.1/*Domain* Subset access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: ***Domain access control policy*****] on [assignment:** ***domain users as subjects, commands as objects, and execution of commands by domain users*****].**

5.1.3.4. FDP_ACF.1/*Domain* Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [assignment: ***Domain access control policy*****] to objects based on the following:**

[assignment:

a) domain users and their following security attributes:

- ***i. user name***

b) commands and their following security attributes:

- ***ii. command name*****]**

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

[assignment: ***if the user is assigned to the requested commands, then access is granted.*****]**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: ***If the user group assigned to the user in the M2000 is Administrators, access is always granted*****]**

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

Application note: This requirement implements the domain users' access control policy. The users will login through the TOE but authentication is performed by an external entity which will send the operational rights to the TOE so it can exercise the access control policy.

5.1.3.5. FDP_ACC.1/EMSCOMM Subset access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: ***EMSCOMM access control policy*** **] on [assignment:** ***EMSCOMM user as subject, commands as objects, and execution of commands by the EMSCOMM user*****].**

5.1.3.6. FDP_ACF.1/EMSCOMM Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [assignment: ***EMSCOMM access control policy*****] to objects based on the following:**

[assignment:

a) EMSCOMM user and its following security attributes:

i. user name

b) commands and their following security attributes:

*ii. command name***]**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: ***the EMSCOMM user will always have execution permission of the targeted command.*****]**

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

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

Application note: This requirement implements the M2000 access control policy.

5.1.4. Identification and Authentication (FIA)

5.1.4.1. FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [selection: ***an administrator configurable positive integer within [assignment: 1 and 255]*** **] unsuccessful authentication attempts occur related to [assignment:** ***authentication of local users since the last successful authentication of the user and before the counter for these attempts is reset after an administrator configurable time frame either between 1 and 60 minutes*****].**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: ***surpassed*****], the TSF shall [assignment:** ***lockout the account for an administrator configurable duration either between 1 and 65535 minutes*****]**

Application note: The EMSCOMM user is not considered in this requirement. The EMSCOMM user is authenticated in the TOE by automatic method and not by user and password. Domain users are authenticated in the M2000 element of the TOE environment, so they are also not considered in this requirement neither by the TOE authentication functionality.

5.1.4.2. FIA_ATD.1 User attribute definition

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

[assignment:

a) User name

b) User group

c) Password

d) Number of unsuccessful authentication attempts since last successful authentication attempt

e) Login allowed start time

f) Login allowed end time

g) Lock status**]**

Application note: The EMSCOMM user is not considered in this requirement. The EMSCOMM user is authenticated in the TOE by automatic method and not by user and password. Domain users are authenticated in the M2000 element of the TOE environment, so they are not considered in this requirement neither by the TOE authentication functionality.

5.1.4.3. FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet:

[assignment:

a) *an administrator configurable minimum length between 6 and 32 characters,*

b) *an administrator configurable combination of the following:*

i. at least one lower-case alphanumerical character,

ii. at least one upper-case alphanumerical character,

iii. at least one numerical character,

iv. at least one special character.

c) *that they are different from an administrator configurable number between 1 to 10 previous used passwords* **]**

5.1.4.4. FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 the TSF shall allow [assignment:

a) *Handshake command*

b) *Parameter negotiation*

c) *New web session ID request*

d) *CAPTCHA management***]**

On behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.4.5. FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [assignment:

a) *Authentication for Local Users*

b) *Authentication for Domain Users*

c) *Authentication for EMSCOMM user*

] to support user authentication.

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

a) *Local Users are authenticated in the TOE by user and password stored in the TOE.*

b) *Domain users authentication is delegated in the M2000 management element of the environment by user and password*

c) *EMSCOMM user applies a special arithmetic procedure common to both parties, the TOE and the M2000 to proof the knowledge of the algorithm.*

]

5.1.4.6. FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [assignment:

a) *Handshake command*

b) *Parameter negotiation*

c) *New web session ID request*

d) *CAPTCHA management*]

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

FIA_UID.1.2 the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.5. Security Management (FMT)

5.1.5.1. FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [assignment: *Local access control policy*] **to restrict the ability to [selection:** *query and modify*] **the security attributes [assignment:**

a) *Command groups*

b) *User groups*]

to [assignment: *users with the appropriate rights*]**.**

5.1.5.2. FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [assignment: *Local access control policy*] **to provide [selection:** *permissive*] **default values for security attributes that are used to enforce the SFP.**

FMT_MSA.3.2 The TSF shall allow the [assignment: *administrator defined roles with the appropriate rights*] **to specify alternative initial values to override the default values when an object or information is created.**

5.1.5.3. FMT_SMF.1 Specification of Management Functions

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

a) *Local User management*

b) *Command group management (creation, deletion, modification, commands membership)*

c) *Local users authorization management (User group authorization on Command groups)*

d) *Configuration of SSL (Certificates and auth mode)*

e) *Configuration of IPSec*

f) *Configuration of ACL*

g) *Configuration of VLAN*

h) *Configuration of UU interface*

i) *Enable/Disable software digital signature*

j) *FIA_SOS.1.1 configurable values (Password policy)*

k) *FIA_AFL.1.1 configurable values (Authentication failure handling)*]

Application note: The TOE includes default users whose associated parameters (but the password) cannot be modified. These users are *admin* and *guest*.

5.1.5.4. FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: [assignment: *Administrator, User, Operator, Guest, Custom*]

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

Application note: These roles are only applicable to the local users. The domain users are not maintained in the TOE, no role neither user group is assigned to a domain user. Also, the EMSCOMM user can not be assigned to any role.

Application note: The custom user group means that the command groups are directly assigned to the user. The domain users are not maintained by the TOE, no role neither user group is assigned to a domain user.

5.1.6. TOE access (FTA)

5.1.6.1. FTA_TSE.1/SEP TOE session establishment

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

a) Protocol type (IP, ICMP, TCP, UDP or SCTP)
b) Source IP address and mask
c) Source port range
d) Destination IP address and mask
e) Destination port range
f) DSCP value
***g) VLAN id*]**

Application note: This requirement addresses the VLAN separation and IP based ACLs to avoid resource overhead in the S1/X2 interface and in the management network.

5.1.6.2. FTA_TSE.1/Local TOE session establishment

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

a) Login allowed start time
b) Login allowed end time
***c) Lock status.*]**

Application note: The EMSCOMM user is not considered in this requirement. The EMSCOMM user is authenticated in the TOE by automatic method and not by user and password. Domain users are authenticated in the M2000 element of the TOE environment, so they are not considered in this requirement neither by the TOE authentication functionality.

5.1.7. Trusted Path/Channels (FTP)

5.1.7.1. FTP_TRP.1/WebLMT Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection : ***remote*****] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection:** ***disclosure*****].**
FTP_TRP.1.2 The TSF shall permit [selection: ***remote users*****] to initiate communication via the trusted path.**
FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection:
[assignment: execution of MML commands]**]**

Application note: Assured identification between both parties is achieved after the user authentication has been performed.

5.1.7.2. FTP_ITC.1/IntegratedPort Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 The TSF shall permit [selection: ***another trusted IT product*****] to initiate communication via the trusted channel.**
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: ***execution of MML/BIN commands*****].**

Application note: Assured identification between both parties is achieved thanks to the SSL server and peer bi directional authentication.

5.2. Security Functional Requirements Rationale

5.2.1. Coverage

78 The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

	O.Audit	O.Authentication	O.Authorization	O.SecureCommunication	O.Resources	O.SoftwareIntegrity	O.UU_Encryption	O.S1_Encryption	O.X2_Encryption
FAU_GEN.1	×								
FAU_GEN.2	×								
FAU_SAR.1	×								
FAU_SAR.3	×								
FAU_STG.1	×								
FAU_STG.3	×								
FDP_ACC.1/Local			×						
FDP_ACF.1/Local			×						
FDP_ACC.1/Domain			×						
FDP_ACF.1/Domain			×						
FDP_ACC.1/EMSCOMM			×						
FDP_ACF.1/EMSCOMM			×						
FIA_AFL.1		×							
FIA_ATD.1		×							
FIA_UAU.1		×	×						
FIA_UAU.5		×	×						
FIA_UID.1	×	×	×						
FIA_SOS.1		×							
FMT_MSA.1			×						
FMT_MSA.3			×						
FMT_SMF.1		×	×	×	×		×	×	×
FMT_SMR.1			×						
FTA_TSE.1/SEP					×				
FTA_TSE.1/Local		×							
FCS_COP.1/SSL				×					
FCS_CKM.1/SSL				×					
FCS_COP.1/UU							×		
FCS_CKM.1/UU							×		
FCS_COP.1/S1								×	
FCS_CKM.1/S1								×	
FCS_COP.1/X2									×
FCS_CKM.1/X2									×
FCS_COP.1/Sign						×			
FTP_TRP.1/WebLMT				×					
FTP_ITC.1/IntegratedPort				x					

Table 8 *Mapping SFRs to objectives*

5.2.2. Sufficiency

79 The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable.

Security objectives	Rationale
O.Audit	The generation of audit records is implemented by FAU_GEN.1. Audit records are supposed to include user identities (FAU_GEN.2) where applicable, which are supplied by the authentication mechanism (FIA_UID.1). Functionality is provisioned to read these records (FAU_SAR.1, FAU_SAR.3). The protection of the stored audit records is implemented in FAU_STG.1. Functionality to prevent audit data loss is provided by FAU_STG.3.
O.Authentication	User authentication is implemented by FIA_UAU.1 and FIA_UAU.5 and supported by individual user identification in FIA_UID.1. The necessary user attributes are spelled out in FIA_ATD.1. The authentication mechanism supports authentication failure handling (FIA_AFL.1), and a password policy (FIA_SOS.1), restrictions as to the validity of accounts for logon (FTA_TSE.1/Local). Management functionality is provided in FMT_SMF.1.
O.Authorization	User authentication is implemented by FIA_UAU.1 and FIA_UAU.5 and supported by individual user identification in FIA_UID.1. The requirements for the local users' access control policy are modelled in FDP_ACC.1/Local, FDP_ACF.1/Local, FMT_MSA.1 and FMT_MSA.3. This access control is based on the definition of roles (FMT_SMR.1). Management functionality for this access control policy is provided in FMT_SMF.1. The domain users' access control policy is modelled in FDP_ACC.1/Domain and FDP_ACF.1/Domain. The EMSCOMM access control policy is modelled in FDP_ACC.1/EMSCOMM and FDP_ACF.1/ EMSCOMM.
O.SecureCommunication	Communications security is implemented using encryption for the communication with WebLMT users, with the M2000 through the integration port interface and in the communication with the FTP servers. The keys used for the channels are generated as part of the SSL connection establishment process. (FCS_COP.1/SSL, FCS_CKM.1/SSL) A trusted channel is provided for the use of the TOE through the Integrated Port interface (FTP_ITC.1/IntegratedPort) A trusted path is provided for the use of the TOE through the WebLMT (FTP_TRP.1/WebLMT) Management functionality to enable these

	mechanisms is provided in FMT_SMF.1.
O.UU_Encryption	Encryption over the UU interface is addressed ciphering the channel between the TOE and the UE. The keys used for the channels are generated using Diffie-Hellman (FCS_COP.1/UU, FCS_CKM.1/UU) Management functionality to configure the channel is provided in FMT_SMF.1.
O.S1_Encryption	Encryption over the S1 interface is addressed ciphering the channel between the TOE and the MME/S-GW. The keys used for the channels are generated as part of the IPSec connection establishment process. (FCS_COP.1/S1, FCS_CKM.1/S1) Management functionality to configure the channel is provided in FMT_SMF.1.
O.X2_Encryption	Encryption over the X2 interface is addressed ciphering the channel between the TOE and others eNodeBs. The keys used for the channels are generated as part of the IPSec connection establishment process. (FCS_COP.1/X2, FCS_CKM.1/X2) Management functionality to configure the channel is provided in FMT_SMF.1.
O.Resource	FTA_TSE.1/SEP implements the separation of traffic based on VLANs and the IP based ACL to avoid resource overhead. Management functionality to configure the ACL and the VLANs is provided in FMT_SMF.1.
O.SoftwareIntegrity	The software integrity objective is directly implemented with FCS_COP.1/Sign so the TOE performs digital signature verification over the software patches.

Table 9 *SFR sufficiency analysis*

5.2.3. Security Requirements Dependency Rationale

80 The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

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

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	Not resolved. The system hardware or an external time source using NTP protocol will provide a reliable time.
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UID.1

FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FCS_COP.1/Sign	[FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1]	Not resolved. The digital certificate used for signature verification is loaded as part of the manufacture process.
	FCS_CKM.4	Not resolved. The digital certificate used for signature verification is loaded as part of the manufacture process and are never destructed.
FDP_ACC.1/Local	FDP_ACF.1	FDP_ACF.1/Local
FDP_ACF.1/Local	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Local FMT_MSA.3
FDP_ACC.1/Domain	FDP_ACF.1	FDP_ACF.1/Domain
FDP_ACF.1/Domain	FDP_ACC.1	FDP_ACC.1/Domain
	FMT_MSA.3	Not resolved. The dependency with FMT_MSA.3 is not resolved because the attributes of the access control policy are not under the control of the TOE.
FDP_ACC.1/EMSCOMM	FDP_ACF.1	FDP_ACF.1/ EMSCOMM
FDP_ACF.1/EMSCOMM	FDP_ACC.1	FDP_ACC.1/ EMSCOMM
	FMT_MSA.3	Not resolved. The dependency with FMT_MSA.3 is not resolved because the attributes of the access control policy are not under the control of the TOE.
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	None	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.5	None	
FIA_UID.1	None	
FIA_SOS.1	None	
FMT_MSA.1	[FDP_ACC.1 | FDP_IFC.1]	FDP_ACC.1
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FTA_TSE.1/SEP	None	
FTA_TSE.1/Local	None	
FCS_COP.1/SSL	[FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1]	FCS_CKM.1/SSL
	FCS_CKM.4	Not resolved. The generated keys are not externally accessible so they do not

		need to be securely removed.
FCS_CKM.1/SSL	[FCS_CKM.2 | FCS_COP.1]	FCS_COP.1/SSL
	FCS_CKM.4	Not resolved. The generated keys are not externally accessible so they do not need to be securely removed.
FCS_COP.1/UU	[FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1]	FCS_CKM.1/UU
	FCS_CKM.4	Not resolved. The generated keys are not externally accessible so they do not need to be securely removed.
FCS_CKM.1/UU	[FCS_CKM.2 | FCS_COP.1]	FCS_COP.1/UU
	FCS_CKM.4	Not resolved. The generated keys are not externally accessible so they do not need to be securely removed.
FCS_COP.1/X2	[FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1]	FCS_CKM.1/X2
	FCS_CKM.4	Not resolved. The generated keys are not externally accessible so they do not need to be securely removed.
FCS_CKM.1/X2	[FCS_CKM.2 | FCS_COP.1]	FCS_COP.1/X2
	FCS_CKM.4	Not resolved. The generated keys are not externally accessible so they do not need to be securely removed.
FCS_COP.1/S1	[FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1]	FCS_CKM.1/S1
	FCS_CKM.4	Not resolved. The generated keys are not externally accessible so they do not need to be securely removed.
FCS_CKM.1/S1	[FCS_CKM.2 | FCS_COP.1]	FCS_COP.1/S1
	FCS_CKM.4	Not resolved. The generated keys are not externally accessible so they do not need to be securely removed.
FTP_TRP.1/WebLMT	None	
FTP_ITC.1/IntegratedPort	None	

Table 10 *Dependencies between TOE Security Functional Requirements*

5.3. Security Assurance Requirements

82 The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components as specified in [CC] Part 3, augmented with ALC_CMC.4 and ALC_CMS.4. No operations are applied to the assurance components.

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level
Development	ADV_ARC	1
	ADV_FSP	3
	ADV_IMP	NA
	ADV_INT	NA
	ADV_SPM	NA
	ADV_TDS	2
Guidance documents	AGD_OPE	1
	AGD_PRE	1
Life-cycle support	ALC_CMC	4
	ALC_CMS	4
	ALC_DEL	1
	ALC_DVS	1
	ALC_FLR	NA
	ALC_LCD	1
	ALC_TAT	NA
Security Target evaluation	ASE_CCL	1
	ASE_ECD	1
	ASE_INT	1
	ASE_OBJ	2
	ASE_REQ	2
	ASE_SPD	1
	ASE_TSS	1
Tests	ATE_COV	2
	ATE_DPT	1
	ATE_FUN	1
	ATE_IND	2
Vulnerability assessment	AVA_VAN	2

Table 11 Security Assurance Requirements

5.4. Security Assurance Requirements Rationale

83 The evaluation assurance level has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

6. TOE Summary Specification

6.1. TOE Security Functionality

6.1.1. Authentication

84 The TOE offers the enforcement of timer-based account lockouts: administrators can specify after how many consecutive failed authentication attempts an account will be temporarily locked, and whether the counter for failed attempts will be reset automatically after a certain amount of minutes. (FIA_AFL.1)

85 The TOE authenticates the local users based on individual user IDs and passwords. User IDs are unique within the TOE and stored together with associated passwords and other security attributes in the TOE's configuration database. Those attributes can be configured by users with the appropriate rights. (FIA_ATD.1, FMT_SMF.1)

86 The TOE can identify users in the management network by a unique ID and enforces their authentication before granting them access to the TSF management interfaces. Warning of "error username or password" will be prompted when the user fails to provide a correct username or password. Some not security related actions can be performed before identification and authentication (FIA_UID.1,FIA_UAU.1)

87 Several authentication mechanisms are provided for the different available users:

1. Local users
2. Domain users
3. EMSCOMM

88 This functionality implements FIA_UAU.5.

89 If applicable, i.e., if an administrator has specified values for these parameters for a specific user, the TOE will deny authentication of the user if the user tries to authenticate in a timeframe that lies outside of the "login start time" and "login end time" specified for the user. (FMT_SMF.1, FTA_TSE.1/Local)

90 The TOE also provide login time control mechanism: Each account can be configured with the login time segment, including the valid date range, time segment, and week restriction. Any login is prohibited beyond the configured time segment. (FMT_SMF.1, FTA_TSE.1/Local)

6.1.2. Access control

91 The Local access control policy is enforced in the following way:

1. The system sorts users with the same operation rights into a group to facilitate authorization and user management of the administrator. The TOE supports five predefined user groups (Administrator, Operator, User, Guest and Custom). The TOE grants default command group rights to Administrator, Operator, User and Guest which can't be modified. (FMT_SMR.1)

2. The TOE divides the system commands to different groups which is called command groups according to different functions. LTE eNodeB creates 22 default command groups in which the commands are preconfigured and can't be modified by user. And it provides 10 non-default command groups to which user adds or removes commands. (FDP_ACF.1/Local)

3. User groups are allowed to access one or more command groups. (FDP_ACF.1/Local)

4. The users that have a custom user group are directly related to the command groups accessible by them.

5. Therefore, a user has access to a command if its user group is associated with a command group that contains the command the user wants to access. (FDP_ACC.1/Local)

6. This access control policy is used to restrict the ability to modify the users and commands relationship. (FMT_MSA.1, FMT_MSA.3)

7. If the user is the admin special user, access is always granted regardless the command group.

92 To allow the customization of the product, ten configurable commands groups and one configurable user group exist. (FMT_SMF.1)

93 The domain access control policy allows users managed by the M2000 to execute commands in the TOE. The management of the security attributes of this access control policy is out of the scope of the TOE. Each time a domain user logs in the TOE (through the integration port or through the WebLMT), the TOE send the used user and password to the M2000 which performs user authentication and return to the user the commands that the user can execute. If the M2000 user belongs to the Administrator group, access to all functionality is always granted. (FDP_ACC.1/Domain, FDP_ACF.1/Domain).

94 The EMSCOMM user is a built-in user that is used by the M2000 to operate the TOE. This user has permission to execute all the commands of the TOE and cannot be modified neither deleted. This user can only be implicitly accessed through the integration port. (FDP_ACC.1/EMSCOMM, FDP_ACF.1/EMSCOMM).

95 Note that some MML commands can only be executed through the appropriate interface, for example, is non sense using the MOD PWD

command to modify the password of the *emscomm* user because it doesn't have password.

96

6.1.3. Auditing

97 Removing the logs is always forbidden (FAU_STG.1)

98 There exist two kinds of audit files, the operation log and the security log.

1. Security log: Records user operations related to the system security, including user behaviour and configuration commands, for example, account locking due to consecutive login failure and updating the security policy

2. Operation log: Records all MML commands run by users.

99 For each of these kinds there exist two files that are rotated in the following way: if one exceeds 1MB the oldest file is deleted and a new one is created. (FAU_STG.3)

100 The auditing functionality of the TOE cannot be started or stopped independently from the operational TOE. The TOE generates audit records for the start and shutdown of base station, and for several auditable events, storing the audit data in the appropriate file (FAU_GEN.1)

101 Where available, the data recorded with each audit record includes the unique user ID associated with a subject during authentication. (FAU_GEN.2)

102 Users with the appropriate rights can review the audit records available in the database. The TOE offers search functionality based on time intervals, user IDs, interface, and/or result. (FAU_SAR.1, FAU_SAR.3)

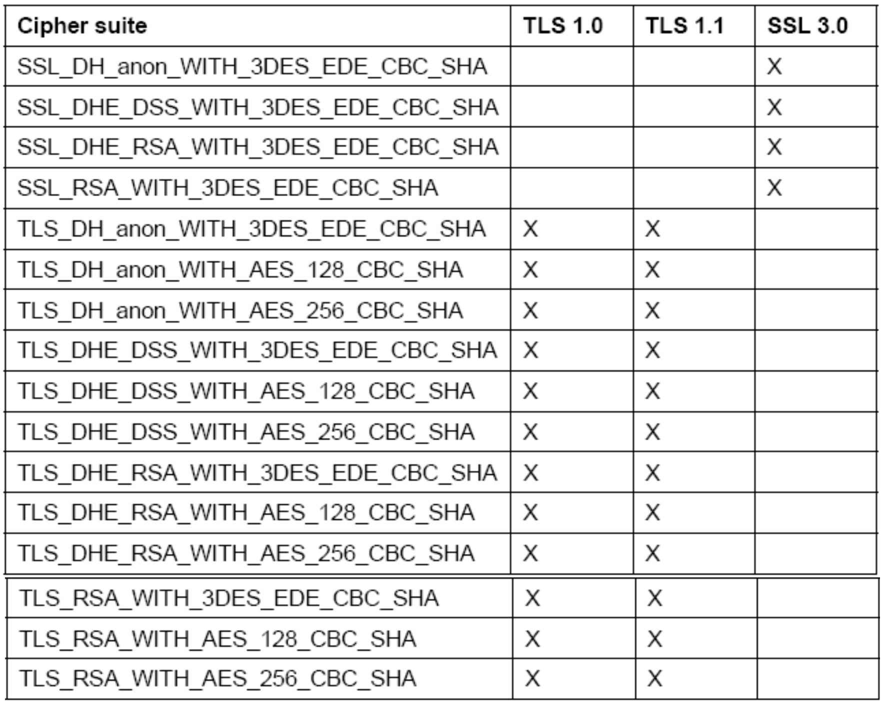
6.1.4. Communications security

103 The TOE provides communications security for network connections to the MPT. This includes connections via the following interfaces:

- Connections to the integrated port (MML/BIN/ALARM) using SSL/TLS. The SSL connection must include client authentication, this way, a trusted channel is established (FTP_ITC.1/IntegratedPort)

- The TOE includes a FTP client which can connect and authenticate with a FTP server. The authentication parameters include the username and password and the IP address of the FTP server, which can be configured. SSL/TLS is used in this connection.

104 The SSL/TLS cipher suites supported for SSL connections are:



Cipher suite	TLS 1.0	TLS 1.1	SSL 3.0
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA			X
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA			X
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA			X
SSL_RSA_WITH_3DES_EDE_CBC_SHA			X
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_DH_anon_WITH_AES_128_CBC_SHA	X	X	
TLS_DH_anon_WITH_AES_256_CBC_SHA	X	X	
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	X	X	
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	X	X	
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	X	X	
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	X	X	
TLS_RSA_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_RSA_WITH_AES_128_CBC_SHA	X	X	
TLS_RSA_WITH_AES_256_CBC_SHA	X	X	

105 This functionality is implemented through FCS_COP.1/SSL and FCS_CKM.1/SSL.The connection with the WebLMT also uses SSL/TLS and authentication based on user id and password, providing a trusted path (FTP_TRP.1/WebLMT)

106 This functionality is configurable. (FMT_SMF.1)

6.1.5. UU Interface Encryption

107 LTE eNodeB air interface channel refers to and wireless channel between the eNodeB and UE. It uses 128-bit AES/SNOW 3G encryption to prevent unauthorized access to communications content. These functions are performed in the PDCP layer and can be activated by RRC message between UE and eNodeB. (FCS_COP.1/UU)

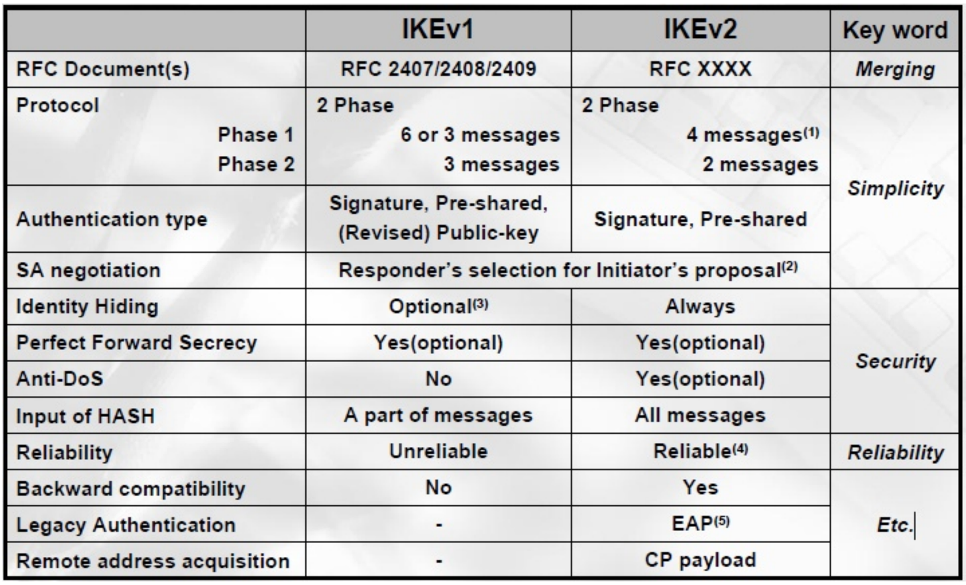
108 Keys are generated using the AKA protocol (FCS_CKM.1/UU)

109 This functionality is configurable. (FMT_SMF.1)

6.1.6. S1 Interface Encryption

110 The TOE provides secure communication protocols for the S1 interface using IPSec/IKE. (FCS_COP.1/S1)

111 The keys are generated according to the IPSec/IKEv2 protocol (FCS_CKM.1/S1)



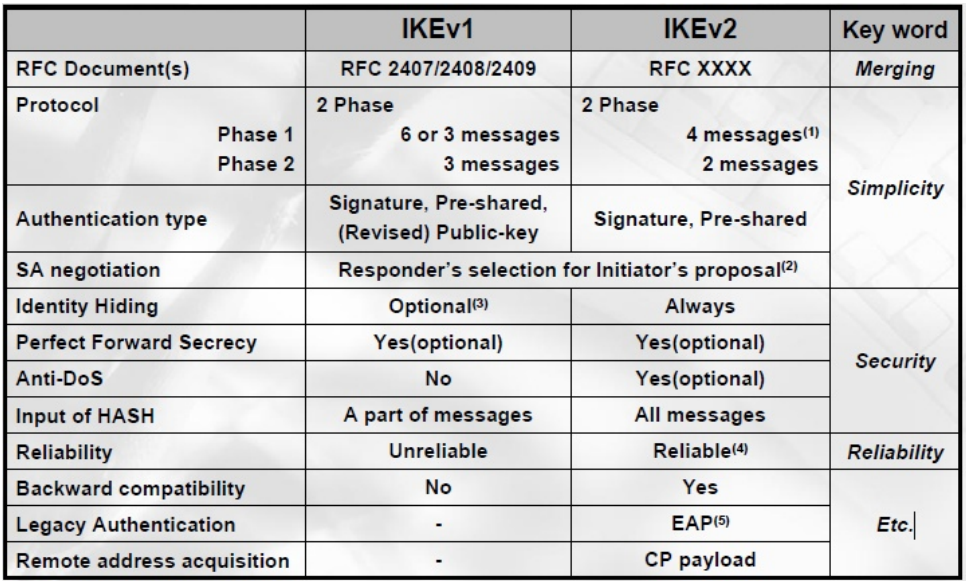
	IKEv1	IKEv2	Key word
RFC Document(s)	RFC 2407/2408/2409	RFC XXXX	*Merging*
Protocol Phase 1 Phase 2	2 Phase 6 or 3 messages 3 messages	2 Phase 4 messages(1) 2 messages	*Simplicity*
Authentication type	Signature, Pre-shared, (Revised) Public-key	Signature, Pre-shared	
SA negotiation	Responder's selection for Initiator's proposal(2)		
Identity Hiding	Optional(3)	Always	*Security*
Perfect Forward Secrecy	Yes(optional)	Yes(optional)	
Anti-DoS	No	Yes(optional)	
Input of HASH	A part of messages	All messages	
Reliability	Unreliable	Reliable(4)	*Reliability*
Backward compatibility	No	Yes	*Etc.*
Legacy Authentication	-	EAP(5)	
Remote address acquisition	-	CP payload	

112 This functionality is configurable. (FMT_SMF.1)

6.1.7. X2 Interface Encryption

113 The TOE provides secure communication protocols for the X2 interface using IPSec/IKE. (FCS_COP.1/X2)

114 The keys are generated according to the IPSec/IKEv2 protocol (FCS_CKM.1/X2)



	IKEv1	IKEv2	Key word
RFC Document(s)	RFC 2407/2408/2409	RFC XXXX	*Merging*
Protocol Phase 1 Phase 2	2 Phase 6 or 3 messages 3 messages	2 Phase 4 messages(1) 2 messages	*Simplicity*
Authentication type	Signature, Pre-shared, (Revised) Public-key	Signature, Pre-shared	
SA negotiation	Responder's selection for Initiator's proposal(2)		
Identity Hiding	Optional(3)	Always	*Security*
Perfect Forward Secrecy	Yes(optional)	Yes(optional)	
Anti-DoS	No	Yes(optional)	
Input of HASH	A part of messages	All messages	
Reliability	Unreliable	Reliable(4)	*Reliability*
Backward compatibility	No	Yes	*Etc.*
Legacy Authentication	-	EAP(5)	
Remote address acquisition	-	CP payload	

115 This functionality is configurable. (FMT_SMF.1)

6.1.8. Resource management

116 The TOE provides VLAN to separate the traffic from different flow planes, which reduce traffic storms and avoid resource overhead.

117 The TOE support VLAN division based on flows such as signalling flows, media flows, or management flows. In other words, different VLAN tags are marked on the three types of flows passing the BS and they are separate from each other.

118 The TOE supports IP-based Access Control List (ACL) to filter traffic destined to TOE which might cause system overload and service interruption.

119 The ACL provides a simple security policy that controls the incoming and outgoing data of unauthorized users. The ACL determines what data is allowed to enter the transmission port and what data is not allowed to enter the transmission port. In this way, the ACL filters the illegitimate data.

120 The ACL controls the network access, preventing the network attacks. In addition, the ACL filters out illegitimate data flows, improving the network performance.

121 The ACL consists of multiple rules. Each rule contains the following filtering conditions:

1. Protocol type (IP, ICMP, TCP, UDP, and SCTP)
2. Source IP address and mask
3. Source port range
4. Destination IP address and mask
5. Destination port range
6. Differentiated Services Code Point (DSCP) value
7. ACL Action (Deny, Permit)

122 The ACL rules can be preset in the S1/X2 network interfaces, and the ACL Action can be designated in advance. In this way, the communication flows can be permitted or denied, and the illegitimate data can be filtered. This method effectively prevents illegitimate intrusions and malicious packet attacks, ensuring the security of network devices. (FMT_SMF.1, FTA_TSE.1/SEP).

6.1.9. Security function management

123 The TOE offers management functionality for its security functions, where appropriate. This is partially already addressed in more detail in the previous sections of the TSS, but includes:

1. User management, including User Group memberships, passwords, account lockout, validity periods for an account and/or

password, etc. Verification of the password policy is performed when creating or modifying users (FIA_SOS.1).

2. Access control management, including the definition of Command Groups, and the association of users and User Groups with Command Groups.

3. Configuration of SSL for the communication between WebLMT/M2000 and the TOE.

4. Configuration of IPSec for the communication between MME/S-GW and the TOE.

5. Configuration of IPSec for the communication between the TOE and others LTE eNodeB.

6. Configuration of VLAN for the different plane between the TOE environment and the TOE.

7. Configuration of ACL for the communication between the TOE environment and the TOE.

8. Configuration of the Air interface.

9. Authorized administrators are able to configure a system-wide password policy that is then enforced by the TOE. Besides the minimum length of the password, which can be set to be between 6 and 32 characters, administrator has the option to enforce the use of specific characters (numeric, alphanumeric low or capital, and special characters).

124 All these management options are available. (FMT_SMF.1)

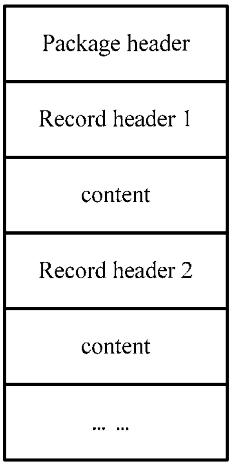
6.1.10. Digital Signature

125 To address security issues, digital signature mechanism to ensure the legitimacy and integrity of the software packages are provided.

126 The TOE automatically checks the digital signature of the software when the user runs the DLD SOFTWARE command to download the software.

127 The CSP files will be the files downloaded from the FTP server to update the TOE software and this way exercise the digital signature mechanism implemented in the TOE.

128 In the following image the CSP structure is depicted:



129 This way, a directory structure is stored in the CSP file. This structure is expected to contain some important files:

130 VERDES.SGN contains the signature of the VERDES.XML file. This way, the TOE will verify the hash and CRC value of each of the files using the VERDES.XML file, and that the file VERDES.XML has not been tampered using the VERDES.SGN stored signature (FCS_COP.1/SGN).

131 This way, the integrity chain is warrantee.

7. Abbreviations, Terminology and References

7.1. Abbreviations

Abbreviations	Full Spelling
ACL	Access Control List
AKA	Authentication and Key Agreement
ASPF	Application Specific Packet Filter
BS	Base Station
BIN	Huawei’s binary interface
CC	Common Criteria
CPBSP	Common Platform Board Support Package
CPRI	Common Public Radio Interface
DSCP	Differentiated Services Code Point
EMS/M2000	Element Management System(M2000)
ETH	Ethernet
FE	Fast Ethernet
FTP	File Transfer Protocol
FTPs	FTP-over-SSL
SCTP	Stream Control Transport Protocol
GE	Gigabit Ethernet
GSM	Global System for Mobile Communications
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
HERT	Huawei Enhanced Radio Technology
HERT -BBU	Huawei Enhanced Radio Technology-Base Band Unit
IPSec	IP Security Protocol
LTE	Long term evolution
NE	Network Element
NMS	Network Management System
NTP	The Network Time Protocol
MAC	Medium Access Control
MML	Man-Machine Language
MPT	Main Processing&Transmission unit
BBI	Base-Band Interface board
OAM (OM)	Operation Administration and Maintenance
OSS	Operations Support System
RRM	Radio Resource Management
SEC	Operator Security management
SFP	Small form-factor pluggable
SFR	Security Functional Requirement
SSL	Security Socket Layer
ST	Security Target
SWM	Software management
TCP	Transfer Control Protocol

TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TR	Transfers Management
TRAN	Transport of Radio Access Network
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial BUS
VISP	Versatile IP and Security Platform
VLAN	Virtual Local Area Network
VPP	Voice Protocol Platform

7.2. Terminology

132 This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

133 **Administrator**: An administrator is a user of the TOE who may have been assigned specific administrative privileges within the TOE. This ST may use the term administrator occasionally in an informal context, and not in order to refer to a specific role definition – from the TOE's point of view, an administrator is simply a user who is authorized to perform certain administrative actions on the TOE and the objects managed by the TOE.

134 **Operator:** See User.

135 **User:** A user is a human or a product/application using the TOE.

7.3. References

136 [CC] Common Criteria for Information Technology Security Evaluation. Part 1-3. July 2009. Version 3.1 Revision 3.

137 [CEM] Common Methodology for Information Technology Security Evaluation. July 2009. Version 3.1 Revision 3.