CC HUAWEI LTE eNodeB Core Software V100R015C10SPC270 Security Target

Version: 1.6
Last Update: 2021-07-15
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	2019-05-16	Dong Changcong	Finish draft release for BTS3900 V100R015C10SPC150 version, based on security target for BTS 3900 V100R011C10SPC112T version.
V0.11	2019-06-12	Dong Changcong	Update description about emscomm user and log file size.
V0.12	2019-07-08	Dong Changcong	Update description about configuration during the evaluation.
V0.20	2019-07-29	Dong Changcong	Update description according to expert review suggestions.
V0.30	2019-09-02	Dong Changcong	Modified to solve issue 1~4 listed in “HUA_LTE-Docs Issues v1.0.docx”
V 0.40	2020-01-06	Dong Changcong	Fix issues mentioned in ‘HUA-LTE-NG-5-OR-004’
V 0.50	2020-03-24	Dong Changcong	Update after review.
V 1.0	2020-10-14	Dong Changcong	Updated based on ORs submitted by DERKA experts, and aligning the version number according to [CMC61].
V 1.1	2020-11-24	Dong Changcong	Updated based on ORs submitted by DERKA experts.
V 1.2	2020-12-14	Dong Changcong	Updated based on advices by DERKA experts.
V 1.3	2020-12-18	Dong Changcong	Updated based on advices by DERKA experts.
V 1.4	2021-01-30	Dong Changcong	Updated version of the TOE.
V 1.5	2021-02-09	Dong Changcong	Update after review.
V 1.6	2021-07-15	Dong Changcong	Update after review.

1. Introduction

1 This Security Target is for the CC evaluation of Huawei 3900 Series LTE (Long Term Evolution) eNodeB Core Software, the TOE Version is V100R015C10SPC270.

1.1. ST Reference

Title	CC HUAWEI LTE eNodeB Core Software V100R015C10SPC270 Security Target
Version	v1.6
Author	Dong Changcong
Publication Date	2021-07-15

1.2. TOE Reference

TOE Name	Huawei 3900 Series LTE eNodeB Core Software
TOE Version	V100R015C10SPC270
TOE Developer	Huawei

1.3. Product Overview

2 3GPP Long Term Evolution (LTE), is a 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 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. The current release of Huawei 3900 series LTE eNodeB is complies with 3GPP Release 15 standards. It supports both LTE FDD mode and LTE TDD mode. It supports LTE-Advanced features such as: Carrier aggregation (CA) and coordinated multi-point (CoMP). It also

support LTE evolution features like EN-DC (E-UTRA New Radio - Dual Connectivity) and L&NR (LTE & New Radio) mobility control. 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.

1.4. TOE Overview

5 The TOE is the core part of the software that is deployed into a Huawei 3900 series LTE eNodeB base station. 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.

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

1.4.1. TOE usage

7 The TOE is the core part of the software that is deployed into a LTE eNodeB base station, which is the wireless access node in LTE/SAE system. It provides the communication with the EPC/Backhaul network (through S1 and X2 interfaces), the management interfaces and other security related functionality.

8 It can be widely used to support access control and events records for the product used for the broadband wireless access of home and enterprise users.

1.4.2. Major security features

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

- Management network:
  - Identification and Authentication.
  - Access control.
  - Communications security.
- Telecom network: S1 and X2 backhaul interface protection.
- Resource management: session establishment mechanisms and VLAN separation.
- Security function management: command groups, trusted channels, users, etc.

- Digital signature: for the verification of software packages when loaded.
- Auditing of security events.

1.4.3. TOE type

10 The TOE is the core part of the software that is deployed into a LTE eNodeB base station, which is the wireless access node in LTE/SAE system. It provides the communication with the EPC/Backhaul network (through S1 and X2 interfaces), the management interfaces and other security related functionality.

11 The S1-C interface is used to transfer control plane signalling between eNodeB and MME.

12 The S1-U interface is used to transfer user plane data between eNodeB and S-GW

13 The X2 interface (including X2-C and X2-U) is used to transmit the control plane and user plane traffic between eNodeBs.

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

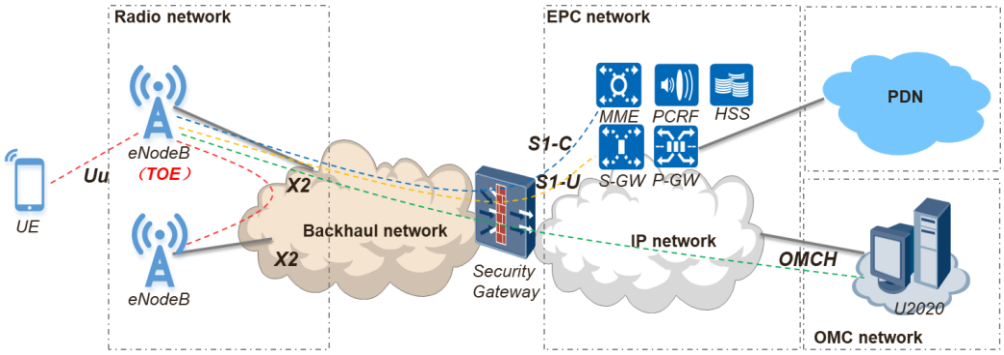


Figure 1 *LTE/SAE network*

15 The following components are not part of the TOE and they are listed here in order describe the EPC network to understand the role of the TOE within the network.

16 The EPC network is the Evolved Packet Core network, it consists of the following NEs.

- Security Gateway (SeGW): is located at the entrance from the eNodeB to the EPC/OMC network.
- Serving gateway (S-GW): a user plane gateway of the EPC. It carries user data between the E-UTRAN and the P-GW.

- Mobility management entity (MME): a primary signalling node, responsible for mobility management in the control plane, including user context and mobility status management and temporary user identifier allocation.

- Packet data network gateway (P-GW): a gateway that terminates the SGi interface between the EPC and the PDN.

- Home subscriber server (HSS): a server that manages and stores the subscription information of end users.

- Policy and charging rules function (PCRF): a policy and charging unit that delivers policies related to quality of service (QoS), charging, and network resource access control to the P-GW.

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

- The OMC (Operations & Maintenance Center) provides network management to LTE eNodeB, such as software management, configuration management, fault management, performance management, and so on. The OMCH (Operation & Maintenance channel) is used to transmit the operation and maintenance traffic between eNodeB and OMC (U2020). The OMCH is also used for local and domain user communications using MML/BIN interface.

1.4.4. Non TOE Hardware and Software

17 The TOE runs into the BBU3900 or BBU 3910 subrack. The structure of BBU3900 is shown in the following figure:

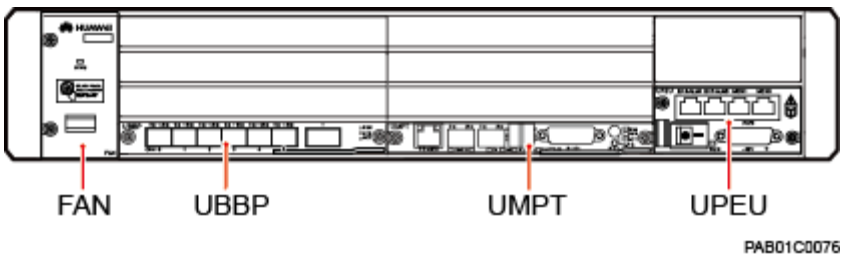


Figure 2 *BBU3900 subrack*

18 The BBU subrack contains, at least, the following mandatory boards:

- The LTE Universal Baseband processing unit (UBBP) whose purpose is to provide an interface between BBU and Radio Remote Unit (RRU).

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

19 The TOE is deployed on the boards of base band unit (BBU). These hardware boards are TOE environment. The OS and part of BS software which is provided by Huawei's particular products is also TOE environment.

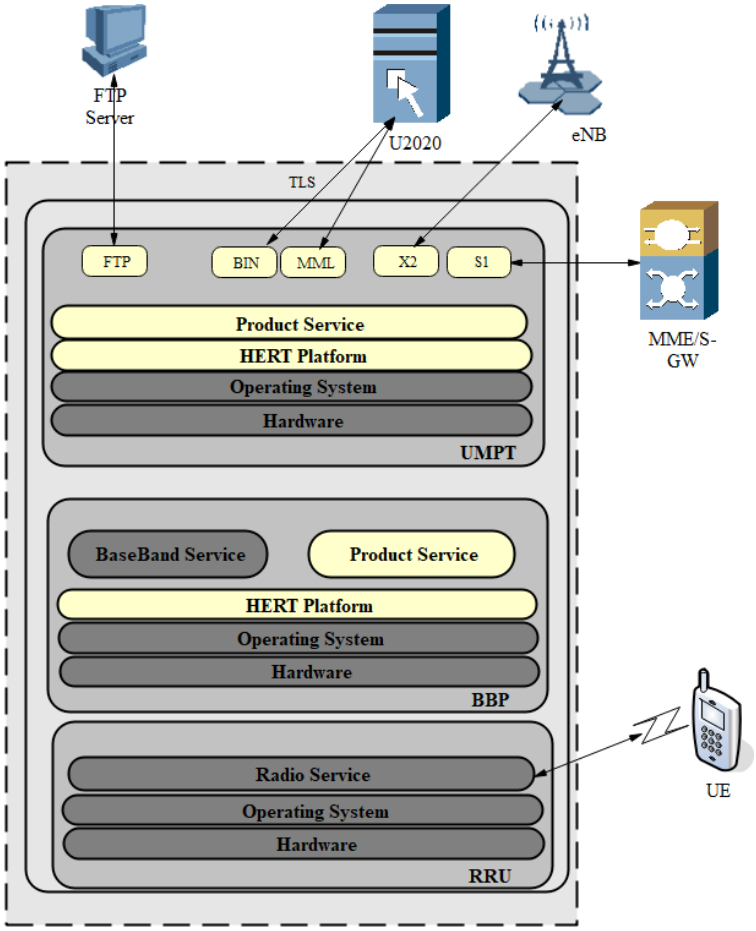


Figure 3 *Non TOE hardware and software environment*

20 In the above diagram, the yellow area belongs to the TOE while the grey box area belongs to the TOE environment.

21 The components of the TOE environment are the following:

22 Note：The TOE environment components are not evaluated given that they are not part of the TOE and therefore there is no assurance regarding these components.

- Physical networks, such as Ethernet subnets, interconnecting various networking devices.
- A Public Key Infrastructure (PKI) which is a set of policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. There exists a well-managed protected public key infrastructure. The certificates used by the TOE and its client are managed by the PKI.
- Another neighbouring LTE eNodeB base station for communication.
- An FTP server used for download software and configuration data to, or upload configuration data and log files from the TOE. The TOE use FTP over TLS to secure the FTP protocol communication. Please notice that FTP server can also be provided by U2020 server.
- An U2020 server providing access to the management functions of the TOE via MML and BIN interface with TLS. U2020 version must be iManager U2020 V300R019C00, U2020 also provides FTP server used for TOE software upgrade.
- 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.
- MME: Mobility Management Entity terminates the control plane with the mobile device.
- LTE eNodeB Operating System RTOS that provides reliable time stamps.
- BaseBand Service is a physical layer conversion such as channel coding and modulation and demodulation.
- RRU: The RRU is the remote radio unit (RRU) for Huawei Worldwide Interoperability. It provides radio service for LTE eNodeB.

1.5. TOE Description

1.5.1. Evaluated configuration

23 The TOE has been deployed in two base stations with different type of RRU configurations: DBS3900 LTE FDD and DBS3900 LTE TDD. The TOE works in the same mode of operation with no changes in the TOE functionality, or in the installation procedures to be followed.

24 U2020 version must be iManager U2020 V300R019C00

25 LTE eNodeB Operating System RTOS V200R007C00.

1.5.2. Logical Scope

26 This section will define the logical scope of the TOE. The TOE is pure software. It is the core part of the software that is deployed into a LTE eNodeB base station.

27 The TOE security functionality is:

A. Identification and Authentication (Management network)

28 The TOE can be accessed by different entities, including local users, domain users and EMSCOMM users. All these accesses are done through a physical port (Ethernet) using the same logical ports (MML and BIN).

29 The Identification and Authentication of the users differ depending on the entity storing the credentials.

30 Local access to the TOE: refers to “local users”, which are the users whose credentials are stored within the TOE. These users access the TOE in order to execute device management functions are identified by individual user names and authenticated by passwords. There is NO vendor special account in the system. Unauthorized users without permission of operators can NOT bypass the system authentication.

31 Domain users (also called EMS domain user) are users that created and managed by the U2020 (Formerly known as U2000 or M2000). Information of domain users is stored on the U2020. The users will login the TOE through the MML or BIN interface, but authentication is performed by the U2020 which will send the result of the authentication procedure to the TOE so it can grant the accessing or deny it. Unauthorized users other than domain users, as well as the users failed the authentication of U2020, can NOT access to the TOE.

32 EMS access to the TOE carried out by “EMSCOMM users” (including emscomm, emscommneteco, emscommcum and emscommts). The identification and authentication procedure of these 4 users are the same, thus EMSCOMM is used to refer to these 4 users in the following sections of this document. EMS access through the MML or BIN interface is enforced using a password based challenge-response protocol at the application layer. Unauthorized users other than EMSCOMM users can NOT bypass the challenge-response protocol without knowledge of corresponding password. There does NOT exist certain user privileges without limitation in the authentication system, i.e. such as a hidden super account or a super password.

33 The TOE provides configurable authentication failure handling to lockout the account of TOE users when the defined number of unsuccessful authentication attempts has been met. This functionality only applies to Local users since they are those stored in the TOE.

34 The TOE maintain user information like user name, user group, password, login allowed start time, login allowed end time and lock status. This functionality only applies to Local users since they are those stored in the TOE.

35 The TOE is able to verify whether the password of local users meet the defined quality metrics.

B. Access control (Management network)

36 The TOE implements role-based access control, limiting access to different management functionality to different roles as defined in administrator-defined access control associations. This feature is implemented only for the access through MML and BIN interface.

C. Management Interfaces protection (Management network)

37 The TOE provides the cryptographic mechanisms to provide integrity and confidentiality in the TLS communications of the MML, BIN and FTPS protocols.

38 The TOE establishes a **trusted** channel for the communications with the U2020 (MML and BIN are used internally) providing the following secure features:

- Integrity
- Confidentiality
- Authentication

D. Backhaul Interface protection (telecom network)

39 IPsec is used in the backhaul interfaces to protect the traffic between the TOE and other network elements such as neighbouring eNodeB (X2) or security gateway (S1).

40 The TOE provides the cryptographic mechanisms to provide integrity and confidentiality in the IPSec communications.

E. Resource management

41 The TOE can limit the user access to the TOE device or application using the ACL (Access Control List) feature by matching information contained in the headers of connection-oriented or connectionless IP packets against ACL rules specified.

42 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.

F. Security function management

43 The following means are provided by the TOE for management of security functionality:

- User and group management
- Trusted channels management
- Session establishment management
- Access control management (by means of defining command groups, and association of users with particular command groups)

G. Digital signature

44 Software package and patches integrity are protected by a digital signature scheme (message digest and signature) which is verified by the TOE before loading it. This contributes to prevent malicious software installation, such as virus, worms or malware.

H. Auditing

45 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 the operational commands run by users.

46 Audit records are created for security-relevant events related to the use of the TOE. The TOE provides the capability to read all the information from the audit records. The TOE protects the audit records from unauthorized deletion, and unauthorized modification.

1.5.3. Physical Scope

47 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.

48 The list of the files and documents required for the products is the following, the software and documents are available on Huawei support website (support.huawei.com), can be downloaded by authenticated user.

Software and Documents	**Description**
BTS3900_5900 V100R015C10SPC270_ALL(Software).7z	Board software package (In the form of 7z package containing binary compressed files)
The following package must be downloaded: CC Huawei 3900 Series LTE eNodeB Software V100R015C10SPC270 Reference document.zip	Once decompressed, this package contains the documents listed in the following table (*).

Table 1 Physical Scope

The following documents are also delivered together with this security target, as guidance for evaluation:

Document	Format	SHA-256 value
Security Management Guide of Huawei 3900 Series LTE eNodeB Core Software V0.9	DOC	6A92DF4267CF8C604BADA7FE29F6E7A50FC55395276D4FDDF3543D83DBAEEEBC
Installation Guide of Huawei 3900 Series LTE eNodeB Core Software V2.4	DOC	1D999B53C2F20CF3CBC97A8F330F74BD5D724C642CAB5D336C34F1656C977EEB
BTS3900&BTS5900 V100R015C10SPC270 MML Command Reference v1.3	ZIP	040FFB14F623E618D34F4DD2200D5CC2D79B6008BB6C4B6916D80A55C3D039C5

BTS3900&BTS5900 V100R015C10SPC270 Error codes V0.2	XLSX	FDA05D4B2AF3D0395F23C22878402B4F867E76BA944603AFE4C70BF3F0CDD99A

2. Conformance claim

49 This ST is CC Part 2 conformant [CC] and CC Part 3 conformant [CC], no extended. The CC version of [CC] is Version 3.1Revision 5.

50 This ST is EAL4 conformant as defined in [CC] Part 3, with the assurance level of EAL4 Augmented with ALC_FLR.1.

51 The methodology to be used for evaluation is CEM3.1 R5

52 No conformance to a Protection Profile is claimed.

3. Security Problem Definition

3.1. TOE Assets

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

Asset	Description
A1.Software and patches	The integrity and confidentiality of the system software and the patches when loaded by the TOE or when in transit across the management network should be protected from malicious modification and unauthorized disclosure.
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).
A3. In transit configuration data	The integrity and confidentiality of the configuration data when travelling in the management network.
A4. User Traffic	The user traffic includes the user data packets transferred upon the S1/X2 interface (telecom network). Confidentiality and integrity of the user traffic in the telecom network are protected by security functions implemented by the TOE.
A5. Service	Availability in terms of the capacity to limit the connectivity of the TOE in order to avoid denial of service.

Table 2 *TOE assets*

3.2. Threats

54 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
Telecommunication network attacker	An attacker from the telecommunication network who can connect to the TOE through S1/X2 interface is able to intercept, and potentially modify or re-use the data that is being sent to the TOE.

Management network attacker	An unauthorized or malicious user who is connected to the management network. These typical attackers are trying to get access to system, such as using remote access Trojan, malicious code or virus.
Restricted authorized user	An authorized user of the TOE who belongs to the management network and has been granted authority to access certain information and perform certain actions. Typical attacks are from restricted authorized account, or undocumented account, or via secret/hidden login method.

Table 3 *Threats agents*

3.2.1. Threats by Management Network Attacker

Threat: T1.InTransitConfiguration	
Attack	An attacker in the management network succeeds in accessing the content of the BS configuration data file before or while transmitting, violating its confidentiality or integrity.
Asset	A3.In transit configuration data
Agent	Management Network Attacker

Threat: T2. InTransitSoftware	
Attack	An attacker in the management network succeeds in accessing the content of the BS software/patches while transmitting, violating its confidentiality or integrity.
Asset	A1.Software and patches
Agent	Management Network Attacker

Threat: T3.UnauthenticatedAccess	
Attack	An unauthenticated attacker in the management network gains access to the TOE disclosing or modifying the configuration data stored in the TOE in a way that is not detected, including unauthorized access or malicious backdoors
Asset	A2.Stored configuration data
Agent	Management Network Attacker

Threat: T4.UnwantedNetworkTraffic_M	
Attack	Unwanted network traffic sent to the TOE from management network 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.
Asset	A5. Service
Agent	Management Network Attacker

3.2.2. Threats by Telecommunication Network Attacker

Threat: T5.UnwantedNetworkTraffic_T	
Attack	Unwanted network traffic sent to the TOE from telecommunication network (S1 and X2 interfaces) also 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. .
Asset	A5. Service
Agent	Telecommunication Network Attacker

Threat: T6. UserTraffic	
Attack	An attacker who is able to modifying/reading external network traffic and thereby gain unauthorized knowledge about the user data transmitting between TOE and SGW (S1) and other eNodeB(X2).
Asset	A4.User Traffic
Agent	Telecommunication Network Attacker

3.2.3. Threats by restricted authorized user

Threat: T7.UnauthorizedAccess	
Attack	A user of the TOE accessing through the management network who is authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for, in an undetected manner
Asset	A2.Stored configuration data
Agent	Restricted authorized user

3.3. Organizational Policies

3.3.1. P1.Audit

55 The TOE shall provide audit functionality:

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

3.3.2. P2. RoleManagement

56 Different personnel who access the TSF needs to be divided according to different roles with different permissions, as far as possible, the user has the minimum required permissions.

3.4. Assumptions

3.4.1. Physical

A.PhysicalProtection

57 It is assumed that the TOE and the base station where is deployed (including boards BBU, UMPT and RRU) is protected against unauthorized physical access.

3.4.2. Personnel

A.TrustworthyUsers

58 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.

3.4.3. Connectivity

A.NetworkSegregation

59 It is assumed that the management network and the telecom network are physically and logically separated between each other.

A.TrustNetwork

60 It is assumed that the **telecom network** between security gateway and EPC (S-GW/MME) is secure and trusted. Security is implemented from the TOE to the security gateway.

3.4.4. Support

A.Support

61 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

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

4. Security Objectives

4.1. Security Objectives for the TOE

63 The following objectives must be met by the TOE:

O.Authentication

64 The TOE must authenticate users and control the session establishment. The I&A mechanism shall be implemented in the following logical users: Local, EMSCOMM.

65 The TOE shall implement a session establishment mechanism restricting the local users to access the TOE based on time.

O.Authorization

66 The TOE shall implement different authorization levels that can be assigned to users in order to restrict the functionality that is available to them. This access control mechanism shall be implemented for the following users: Local, Domain and EMSCOMM. And these different authorizations should be properly managed, in order to prevent abuse of limited authorized users.

O.SecureCommunication

67 The TOE provides the cryptographic mechanisms to provide integrity and confidentiality in the TLS communications of the MML, BIN and FTPS protocols.

68 The TOE establishes a **trusted** channel for the communications with the U2020 (MML and BIN are used internally) providing the following secure features:

- Integrity
- Confidentiality
- Authentication

O. SoftwareIntegrity

69 The TOE must provide functionality to verify the integrity of the loaded software patches.

O.Resources

70 The TOE shall implement a session establishment mechanism (SEP) controlled by IP, port, protocol and VLAN id for telecom (S1, X2) and management network (MML, BIN & FTPS) allowing VLAN separation and IP based ACLs to avoid resource overhead.

O.Audit

71 The TOE shall provide audit functionality:

- Generation of audit information.
- Secure storage of audit log.
- Review of audit records.

O.UserTrafficProtection

72 The TOE shall provide integrity and encryption protection for the IPSec communcations of the S1 and X2 data exchanged over the backhaul network.

4.2. Security Objectives for the Operational Environment

OE. PhysicalProtection

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

OE.TrustworthyUsers

74 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.NetworkSegregation

75 The TOE environment shall assure that the management network, the telecom network and the radio network are separated between each other.

OE. TrustNetwork

76 The telecom network between security gateway and EPC(S-GW/MME/P-GW/HSS/PCRF) is trusted and secure.

OE.Support

77 The reliable time stamps are provided by the underlying operating system of the base station (RTOS).

78 Those responsible for the operation of the TOE and its operational environment must ensure that the operating system is working properly to provide reliable time stamps to the TOE for the generation of audit records.

OE. SecurePKI

79 A well-managed protected public key infrastructure is implemented in the operational environment. The certificates used by the TOE and its client are managed by the PKI.

4.3. Security Objectives rationale

4.3.1. Coverage

80 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.UnauthenticatedAccess	T4.UnwantedNetworkTraffic_M	T5.UnwantedNetworkTraffic_T	T6. UserTraffic	T7.UnauthorizedAccess	A.PhysicalProtection	A.TrustworthyUsers	A.NetworkSegregation	A.TrustNetwork	A.Support	A. SecurePKI	P1.Audit	P2.RoleManagement
O.Authentication			X												
O.Authorization							X								X
O.SecureCommunication	X	X	X												
O.SoftwareIntegrity		X													
O.Resources				X	X										
O.Audit														X	
O.UserTrafficProtection						X									
OE.PhysicalProtection								X							
OE.TrustworthyUsers									X						
OE.NetworkSegregation										X					
OE.TrustNetwork						X					X				

OE.Support												X			
OE.SecurePKI	X	X	X			X							X		

Table 4 *Mapping of security objectives*

4.3.2. Sufficiency

81 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 TLS 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	O.SecureCommunication contributes also as a secure communication channel between the TOE and external entities in the management network is established. A secure PKI will be needed to assure the validity of the used certificates. (OE.SecurePKI)
T3.UnauthenticatedAccess	The threat T3.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 together with O.Authorization which requires the TOE to implement an access control mechanism for the users in the management network. It is also countered by requiring communications security via TLS for network communication between entities in the management network and the TOE (O.SecureCommunication). The threat T3.UnauthenticatedAccess is countered by

	O.SoftwareIntegrity: when a software package is loaded, its message digest and signature are verified to avoid possible modifications of the TOE software by unauthenticated users. A secure PKI will be needed to assure the validity of the used certificates. (OE.SecurePKI)
T4.UnwantedNetworkTraffic_M	The threat T4.UnwantedNetworkTraffic_M is directly counteracted by the security objective for the TOE O.Resources.
T5.UnwantedNetworkTraffic_T	The threat T5.UnwantedNetworkTraffic_T is also directly counteracted by the security objective for the TOE O.Resources.
T6.UserTraffic	The Threat T6.UserTraffic is countered by the security objective for the TOE (O.UserTrafficProtection). This provides IPsec tunnels between eNodeB and security gateway. The IPsec tunnels are used to protect S1 and X2 traffic in backhaul network between eNodeB and security gateway. The S1 interface traffic between security gateway and MME/SGW is protected by OE.TrustNetwork A secure PKI will be needed to assure the validity of the used certificates. (OE.SecurePKI)
T7.UnauthorizedAccess	The threat T7.UnauthorizedAccess is countered by the security objective for the TOE O.Authorization which requires the TOE to implement an access control mechanism for the users in the management network. The threat T7.UnauthorizedAccess is countered by O.SoftwareIntegrity: when a software package is loaded, its message digest and signature are verified to avoid possible modifications of the TOE software by unauthorized users.

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.TrustNetwork	This assumption is directly implemented by the security objective for the environment OE.TrustNetwork.
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.RoleManagement	This policy is directly implemented by the security objective for the TOE O.Authorization

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 that triggered by manual operation. (OPE)

ii. user management

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

2. password change through MML (MOD OP command) (SEC & OPE)

3. authorization modification (SEC & OPE)

4. enable, disable of local user management through MML (SET OPSW command) (SEC & OPE)

iii. Locking, unlocking (manual or automatic) (SEC)

1. Locking (automatic) (SEC)

2. Locking (manual: through SET OPLOCK command) (SEC & OPE)

3. unlocking (automatic) (SEC)

4. unlocking (manual: through ULK USR command) (SEC & OPE)

iv. Command group management

1. Add/ delete commands into/from command group (SEC & OPE)

2. Modify name of command group name (SEC &OPE)

]

Application note:

Domain users are managed by U2020, so except logins and logouts, other record (use management, locking, unlocking, command group management) related to domain users are record on U2020, not record on the TOE.

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).*]

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*].

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: *2048bits*] that meet the following: [assignment: *none*]

5.1.2.2. FCS_COP.1/TLS Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: *encryption, decryption, cryptographic checksum generation for integrity and verification of checksum on TOE access channels*] in accordance with a specified cryptographic algorithm [assignment: *algorithms supported by TLS*] and cryptographic key sizes [assignment: *key sizes supported by TLS*] that meet the following: [assignment: *none*]

Application note: The supported TLS cipher suites are defined in the section 6 TOE Summary Specification.

5.1.2.3. FCS_COP.1/IPsec Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: *encryption, decryption, cryptographic checksum generation for integrity, verification of checksum*] in accordance with a specified cryptographic algorithm [assignment:

AES for encryption/decryption,

HMAC-SHA1 and HMAC-SHA256 for integrity protection] **and cryptographic key sizes [assignment:**

128 bits for AES-CBC-128 and AES-GCM-128,

256 bits for AES-CBC-256 and AES-GCM-256,

128 bits for HMAC-SHA1,

256 bits for HMAC-SHA256 **] that meet the following: [assignment:** ***none*****]**

Application note: The supported IPsec algorithms are defined in the section 6 TOE Summary Specification.

5.1.2.4. FCS_CKM.1/TLS 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 TLS*****] and cryptographic key sizes [assignment:** ***key sizes supported by TLS*****] that meet the following: [assignment:** ***none*****]**

5.1.2.5. FCS_CKM.1/IPsec Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: ***PRF_HMAC_SHA1, PRF_AES128_CBC, PRF_HMAC_SHA256, PRF_HMAC_SHA384*****] 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 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.

]

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 group]

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***]**

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 U2020 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*]

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 group]

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:

a) *emscomm will always have execution permission of the targeted command.*

emscommts will always have execution permission of the base command(G_0).

emscommcum will always have execution permission of all the command groups except command group(G_15).

emscommneteco will always have execution permission of the base command(G_0) and energy management commands. **]**

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*]

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: *met*], the TSF shall [assignment: *lockout the account for an administrator configurable duration either between 1 and 65535 minutes*]

Application note: Only local users are taken into account in this requirement.

The EMSCOMM user is not considered in this requirement. The EMSCOMM user is authenticated in the TOE by automatic method. Domain users are authenticated in the U2020 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) Login allowed start time
e) Login allowed end time
f) Lock status]

Application note: Only local users are taken into account in this requirement. The EMSCOMM user is not considered in this requirement. The EMSCOMM user is authenticated in the TOE by automatic method. Domain users are authenticated in the U2020 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) minimum length 8 characters,
b) contain combination of the following:

i. at least one lower-case alphanumerical character,

ii. at least one digit.

]

Application note:

a. Only local users are taken into account in this requirement.

5.1.4.4. FIA_UAU.1/Local Timing of authentication

FIA_UAU.1.1 the TSF shall allow [assignment:

a) Handshake command (SHK HAND)
b) Parameter negotiation (NEG OPT, used to negotiate language information; Base Site Information: NR/LTE/UMTS/GSM/Multimode)
c) Login request (LGI REQUEST, used to request public key before login)
d) Logout (LGO, used to logout) **]**

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.2/EMSCOMM 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.

5.1.4.6. FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [assignment:

a) Authentication for Local Users

b) 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 username and password stored in the TOE.

b) EMSCOMM user is authenticated in the TOE by a password based challenge-response protocol.

]

5.1.4.7. FIA_UID.1/Local Timing of identification

FIA_UID.1.1 The TSF shall allow [assignment:

a) Handshake command (SHK HAND)

b) Parameter negotiation (NEG OPT, used to negotiate language information; Base Site Information: NR/LTE/UMTS/GSM/Multimode)

c) Logout (LGO, used to logout) **]**

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.

5.1.4.8. FIA_UID.2/ EMSCOMM User identification before any action

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: *restrictive*] 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 TLS (Certificates and auth mode)
e) Configuration of IPSec
f) Configuration of ACL
g) Configuration of VLAN
h) FIA_SOS.1.1 configurable values (Password policy)
i) FIA_AFL.1.1 configurable values (Authentication failure handling)]

5.1.5.4. FMT_SMR.1 Security roles

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

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*]**

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) Account status.*]**

Application note: Only local users are taken into account in this requirement.

5.1.7. Trusted Path/Channels (FTP)

5.1.7.1. FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: *U2020*] 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*].

5.2. Security Functional Requirements Rationale

5.2.1. Coverage

82 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.UserTrafficProtection
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/Local		×	×				
FIA_UAU.2/EMSCOMM		×	×				
FIA_UAU.5		×	×				
FIA_UID.1/Local	×	×	×				
FIA_UID.2/EMSCOMM	×	×	×				
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/TLS				×			
FCS_CKM.1/TLS				×			
FCS_COP.1/IPsec							×
FCS_CKM.1/IPsec							×
FCS_COP.1/Sign						×	
FTP_ITC.1				×			

Table 8 *Mapping SFRs to objectives*

5.2.2. Sufficiency

83 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 identification mechanism (FIA_UID.1/Local and FIA_UID.2/EMSCOMM). 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	Local user authentication is implemented by FIA_UAU.1/Local, EMSCOMM user authentication is implemented by FIA_UAU.2/EMSCOMM. FIA_UAU.5 is implemented for multi-user authentication. 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	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 the MML or BIN interface and in the communication with the FTP servers. The keys used for the channels are generated as part of the TLS connection establishment process. (FCS_COP.1/TLS, FCS_CKM.1/TLS) A trusted channel is provided for the use of the TOE through the U2020 (FTP_ITC.1) Management functionality to enable these mechanisms is provided in FMT_SMF.1.
O.UserTrafficProtection	Encryption over the S1/X2 interface is addressed ciphering the channel between the TOE and peer NE (security gateway or neighbouring eNodeB). The keys used for the channels are generated as part of the IPSec connection establishment process using Diffie-Hellman. (FCS_COP.1/IPsec, FCS_CKM.1/IPsec) 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

84 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.

85 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	OE.Support : the operational environment provides Reliable time stamps for the generation of audit records.
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 is 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/Local
FIA_ATD.1	None	None
FIA_UAU.1/Local	FIA_UID.1/Local	FIA_UID.1/Local
FIA_UAU.2/EMSCOMM	FIA_UID.2/EMSCOMM	FIA_UID.2/EMSCOMM
FIA_UAU.5	None	None
FIA_UID.1/Local	None	None
FIA_UID.2/EMSCOMM	None	None
FIA_SOS.1	None	None
FMT_MSA.1	[FDP_ACC.1 | FDP_IFC.1]	FDP_ACC.1/Local
	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	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1/Local
FTA_TSE.1/SEP	None	None
FTA_TSE.1/Local	None	None
FCS_COP.1/TLS	[FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1]	FCS_CKM.1/TLS
	FCS_CKM.4	Due to the security problem the memory where the keys are stored is not physically accessible. Furthermore, the memory cannot be downloaded through the available logical paths. Therefore, the keys cannot be obtained and, according to the CEM, it is considered that the dependency with FCS_CKM.4 is not necessary or useful.
FCS_CKM.1/TLS	[FCS_CKM.2 | FCS_COP.1]	FCS_COP.1/TLS
	FCS_CKM.4	Due to the security problem the memory where the keys are stored is not physically accessible.

		Furthermore, the memory cannot be downloaded through the available logical paths. Therefore, the keys cannot be obtained and, according to the CEM, it is considered that the dependency with FCS_CKM.4 is not necessary or useful.
FCS_COP.1/IPsec	[FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1]	FCS_CKM.1/IPsec
	FCS_CKM.4	Due to the security problem the memory where the keys are stored is not physically accessible. Furthermore, the memory cannot be downloaded through the available logical paths. Therefore, the keys cannot be obtained and, according to the CEM, it is considered that the dependency with FCS_CKM.4 is not necessary or useful.
FCS_CKM.1/IPsec	[FCS_CKM.2 | FCS_COP.1]	FCS_COP.1/IPsec
	FCS_CKM.4	Due to the security problem the memory where the keys are stored is not physically accessible. Furthermore, the memory cannot be downloaded through the available logical paths. Therefore, the keys cannot be obtained and, according to the CEM, it is considered that the dependency with FCS_CKM.4 is not necessary or useful.
FTP_ITC.1	None	None

Table 10 *Dependencies between TOE Security Functional Requirements*

5.3. Security Assurance Requirements

86 The security assurance requirements for the TOE are the Evaluation Assurance Level 4 components as specified in [CC] Part 3, augmented with ALC_FLR.1. No operations are applied to the assurance components. Note that for EAL 4 or higher level assurance, source code evaluation including keyword search or static scan could be applied to prevent against backdoors or malicious programs.

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level
Development	ADV_ARC	1
	ADV_FSP	4
	ADV_IMP	1
	ADV_INT	NA
	ADV_SPM	NA
	ADV_TDS	3
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	1
	ALC_LCD	1
	ALC_TAT	1
Security Target evaluation	ASE_CCL	1
	ASE_ECD	1
	ASE_INT	1
	ASE_OBJ	2
	ASE_REQ	2
	ASE_SPD	1
	ASE_TSS	1
Tests	ATE_COV	2
	ATE_DPT	1
	ATE_FUN	1
	ATE_IND	2
Vulnerability assessment	AVA_VAN	3

Table 11 Security Assurance Requirements

5.4. Security Assurance Requirements Rationale

87 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

88 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) This functionality only applies to the local users.

89 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). FIA_ATD.1 only applies to the local users because the attributes of the rest of the users are not under the control of the TOE. The EMSCOMM user is not considered in this requirement.

90 Verification of the password policy is performed when creating or modifying users (FIA_SOS.1). This functionality only applies to the local users.

91 The TOE can identify local 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/Local,FIA_UAU.1/Local). These are the MML commands corresponding to these actions:

a) Handshake command (SHK HAND)
b) Parameter negotiation (NEG OPT)
c) Login request (LGI REQUEST)
d) Logout (LGO)

92 The TOE can identify and authenticate EMSCOMM users in the management network by their unique ID and enforces authentication before granting it access to the TSF management interfaces. (FIA_UID.2/EMSCOMM, FIA_UAU.2/EMSCOMM)

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

1. Local users
2. EMSCOMM

94 This functionality implements FIA_UAU.5.

95 The EMSCOMM user is authenticated in the TOE by a password based challenge-response method. Domain users are authenticated in the U2020 element of the TOE environment, so they are also not considered in this requirement neither by the TOE authentication functionality.

6.1.2. Access control

96 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). The custom user group means that the command groups are directly assigned to the user. 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 cannot be assigned to any role.

2. The TOE divides the system commands to different groups which is called command groups according to different functions. LTE eNodeB creates 23 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.

8. Access control policy can be configured in the TOE in terms of local user management and command group management (FMT_SMF.1).

97 The domain access control policy allows users managed by the U2020 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 MML or BIN interface), the TOE send the used user and password to the U2020 which performs user authentication and return to the user the commands that the user can execute. If the U2020 user belongs to the Administrator group, access to all functionality is always granted. (FDP_ACC.1/Domain, FDP_ACF.1/Domain).

98 The EMSCOMM users are built-in users that are used by the U2020 to operate the TOE. Th ese users have permission to execute all the commands of the TOE and cannot be modified neither deleted. This user can only be implicitly accessed through the MML or BIN interface. (FDP_ACC.1/EMSCOMM, FDP_ACF.1/EMSCOMM).

6.1.3. Auditing

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

100 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.

101 For each of these kinds there exist several files that are rotated in the following way: if total size exceeds the pre-defined volume of the specific log type, the oldest file is deleted and a new one is created. (FAU_STG.3). For security log storage, the capacity limitation is 2M bytes. For operation log storage, the capacity limitation is 11M bytes. Each log file has the size of about 1M bytes. When the capacity is used up, the oldest log file will be deleted.

102 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. The “domain” attribute in log for local user is “local”, for domain user is “EMS”, for EMSCOMM user is “EMSOP”. (FAU_GEN.1)

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

104 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

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

106 Connections to the MML/BIN interface using TLS.

- The TLS connection with the U2020 must include client authentication, this way, a trusted channel is established (FTP_ITC.1)
- The TLS connection must include integrity and confidentiality, this way, a secure channel is established (FCS_COP.1/TLS and FCS_CKM.1/TLS).

107 The TOE includes a FTP client which can establish a secure connection with a FTP server. The connection parameters include the username and password and the IP address of the FTP server, which can be configured. TLS is also used in this connection (FCS_COP.1/TLS and FCS_CKM.1/TLS).

108 The following table shows the TLS cipher suites supported by the TOE:

Cipher suite	TLS1.2
ECDHE_RSA_AES_256_GCM_SHA384	X
DHE_RSA_AES_256_GCM_SHA384	X
RSA_AES_256_GCM_SHA384	X
ECDHE_RSA_AES_128_GCM_SHA256	X
DHE_RSA_AES_128_GCM_SHA256	X
RSA_AES_128_GCM_SHA256	X

Table 12 Supported TLS cipher suites

6.1.5. Backhaul Interface Protection

109 The TOE provides secure communication protocols for the S1 interface (only the segment between eNodeB and security gateway) and X2 interface, using IPSec/IKE. (FCS_COP.1/IPSEC)

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

	IKEv2
RFC Document	RFC 7296
Protocol messages	4 messages for initial exchanges
Authentication type	Digital Signature or Pre-shared key
Key derivation function	PRF_HMAC_SHA1, PRF_AES128_CBC, PRF_HMAC_SHA256, PRF_HMAC_SHA384
SA negotiation	Responder's selection for initiator's proposal
Identity Hiding	Always
Perfect Forward Secrecy	Yes (optional)
Anti-Dos	Yes (optional)
Input of HASH	All messages

Table 13 Supported IKE Protocol functions

111 The TOE supports the following IPsec protocol functions

	IPsec
Protocol	ESP
Encapsulation mode	Tunnel mode
Encryption algorithms	AES-CBC-128, AES-CBC-256, AES-GCM-128, AES-GCM-256
Integrity algorithms	HMAC-SHA-256, HMAC-SHA1
Anti-replay	Yes

Table 14 Supported IPsec Protocol functions

6.1.6. Resource management

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

113 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.

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

115 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.

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

117 The ACL consists of multiple rules. Each VLAN-based rule contains 2 conditions: VLAN range and ACL Action. Each IP-based 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)

118 The ACL rules can be present 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. (FTA_TSE.1/SEP).

119 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. (FTA_TSE.1/Local). Only local users are taken into account in this requirement. The EMSCOMM user is not considered in this requirement. The EMSCOMM user is authenticated in the TOE by a password based challenge-response method. Domain users are authenticated in the U2020 element of the TOE environment, so they are

not considered in this requirement neither by the TOE authentication functionality.

6.1.7. Security function management

120 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). This functionality only applies to the local users. For authentication failure handling values are configurable (FIA_AFL.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 TLS for the communication between U2020 and the TOE.

4. Configuration of IPSec for the communication between eNodeB and IKE Peer.

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

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

7. 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 8 and 32 characters, administrator has the option to enforce the use of specific characters (numeric, alphanumeric low or capital, and special characters).

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

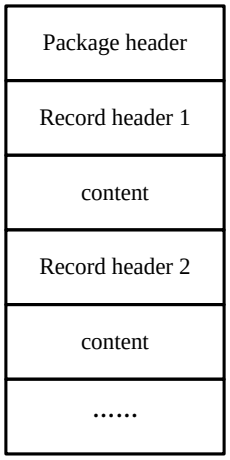
6.1.8. Digital Signature

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

123 The TOE automatically checks the digital signature of the software when the user runs the ACT SOFTWARE command to active the software.

This way exercise the digital signature mechanism implemented in the TOE (FCS_COP.1/Sign).

124 In the following image the CSP structure is depicted:



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

126 VERDES.cms contains the signature of the VERDES.xml file. This way, the TOE will verify the signature stored in VERDES.cms to ensure that the file VERDES. xml has not been tampered. And then hash and CRC value of each of the files will be verified by the TOE using the VERDES. xml file.

127 This way, the integrity chain is guaranteed.

7. Abbreviations, Terminology and References

7.1. Abbreviations

Abbreviations	Full Spelling
ACL	Access Control List
EPS-AKA	Evolved Packet System-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/U2020	Element Management System(U2020)
ETH	Ethernet
FE	Fast Ethernet
FTP	File Transfer Protocol
FTPS	FTP-over-TLS
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
FDD	Frequency Division Duplex

TDD	Time Division Duplex

7.2. References

128 [CC] Common Criteria for Information Technology Security Evaluation. Part 1-3. April 2017. Version 3.1 Revision 5.

129 [CEM] Common Methodology for Information Technology Security Evaluation. April 2017. Version 3.1 Revision 5.