ZTE 5G gNodeB Core Software
Security Target

LEGAL INFORMATION

Revision History

Version	Date	Comment
0.1	2022-11-30	First version
0.2	2023-1-18	Modification
0.3	2023-2-23	Modification
0.4	2023-3-15	Modification
0.5	2023-4-18	Modification
0.6	2023-5-22	Modification
0.7	2023-6-14	Modification
0.8	2023-7-7	Modification
0.9	2023-7-13	Modification
1.0	2023-9-18	Modification
1.1	2023-9-20	Modification
1.2	2023-9-26	Modification
1.3	2023-10-10	Modification
1.4	2023-11-28	Modification
1.5	2023-11-30	Modification
1.6	2023-12-26	Modification
1.7	2024-03-13	Modification
1.8	2024-03-15	Modification
1.9	2024-03-22	Modification
2.0	2024-03-25	Modification
2.1	2024-04-07	Modification

Contents

1 ST Introduction

1.1 ST reference

Title	ZTE 5G gNodeB Core Software Security Target
Version	2.1
Date	Apr 07, 2024
Author	ZTE

1.2 TOE reference

TOE Name	ZTE gNodeB Core Software
TOE version	V5.65.20.10F12
Developer	ZTE

1.3 TOE Overview and usage

The TOE is the core software of ZTE 5G gNodeB base station, which provides the communication with the terminal, the 5GC/Backhaul network, the management interfaces and other security related functionality. The ST describes the security objectives and the security requirements, as well as the necessary functional and assurance measures provided by the TOE.

The TOE is mainly used to provide secure access for terminals and secure data backhaul. In addition, user access control and security log recording are also important parts of the TOE.

The TOE is applicable to network architectures such as NSA and SA. It can be deployed on dedicated hardware V9200.

The ST provides the basis for the TOE according the Common Criteria for Information Technology Security Evaluations(CC)

The following figure shows the position of the TOE in 5G network

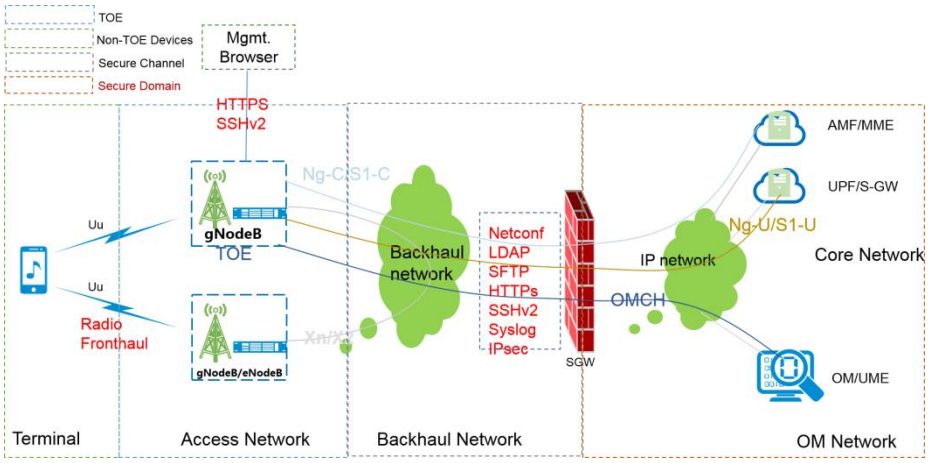

Figure 1: The TOE(core software of ZTE 5G gNodeB) in its environment

1.3.1 Major security features

The major security features of the TOE are:

- Radio Security : UE data and Signaling protection of Uu-U interface;
- Transport Security: Ng/S1, Xn/X2 and OMCH backhaul interface protection. OMCH(operation management channel) is used to provide an O&M management channel between the gNodeB and the UME.
- Operation and Maintenance management:
  - Identification and Authentication
  - Access Control
  - Communications Security
- Digital signature: for the integrity verification of software during version upgrade phase and secure boot phase;
- Provides logging and auditing of user actions.

1.3.2 Non-TOE Hardware/Software/Firmware

The TOE runs into the BBU V9200 shelf. The following figure shows the structure of the BBU V9200 shelf.

<table>
<tr><td colspan="2">VBP SLOT8</td><td colspan="2">VBP SLOT4</td><td rowspan="4">VF
SLOT14</td></tr>
<tr><td colspan="2">VBP SLOT7</td><td colspan="2">VBP SLOT3</td></tr>
<tr><td colspan="2">VBP SLOT6</td><td colspan="2">VSW/VBP SLOT2</td></tr>
<tr><td>VPD SLOT5</td><td>VEM SLOT13</td><td colspan="2">VSW SLOT1</td></tr>
</table>

The BBU shelf mainly contains the following mandatory boards:

- The 5G virtualized base band unit pool(VBP) is a unit which processes the data from Radio Remote Unit(RRU) /Active Antenna Unit(AAU) and resource scheduling.
- The 5G virtualized switch band(VSW) is the main board of the BBU. It controls and manage the entire Base station system, provides synchronization signals for the base station system and provides the transport interfaces for the transmission.
- The 5G virtualized fan(VF) is the fan unit of BBU, which controls the fan functions, such as the speed ,the temperature monitoring and reporting status of the fun.
- The 5G virtualized power distribution(VPD) supports the power to the whole BBU shelf.
- The 5G virtualized environment monitoring(VEM) is used to support the interface which control and report the environment status, such as the fun controlling module, Humidity module .etc

These hardware devices support the operating environment for the TOE. In addition, the basic software such as operating system is also part of TOE environment.

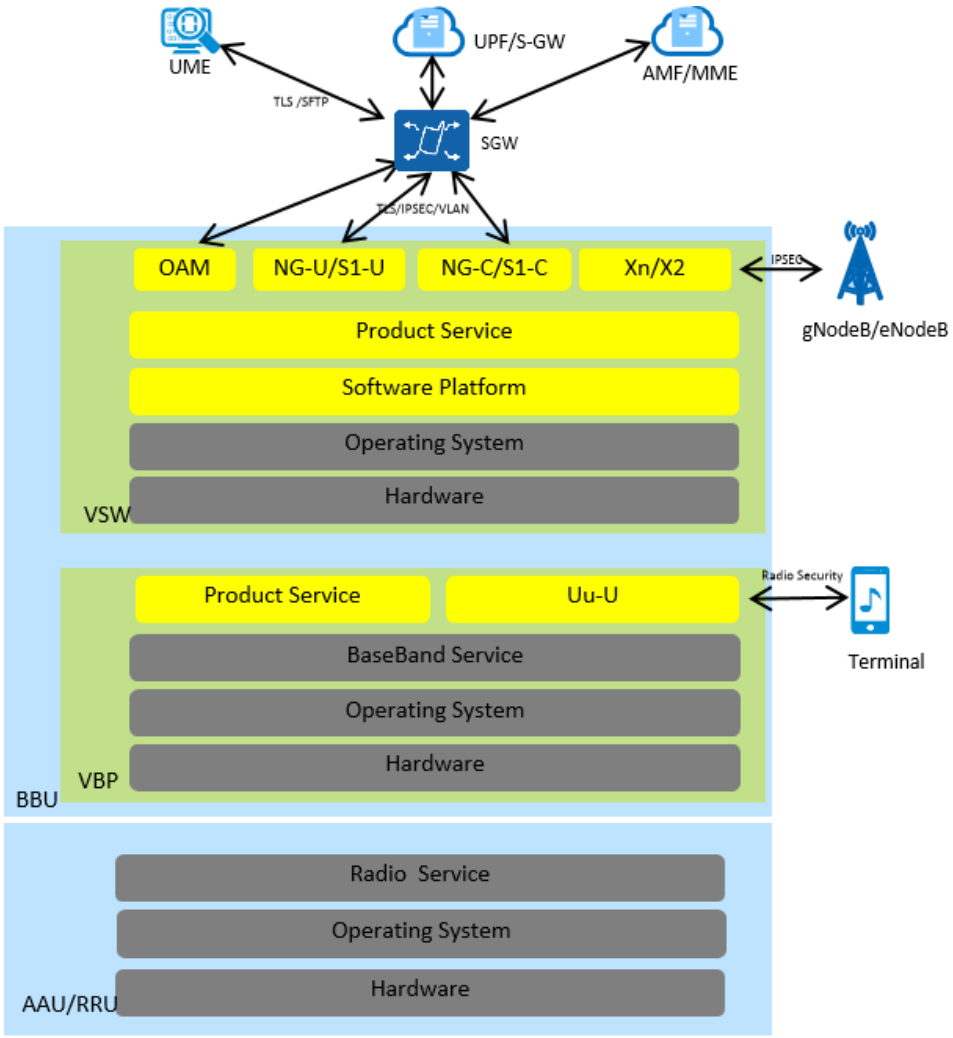

Figure 2 TOE operation environment

As shown in the above diagram, the yellow parts belong to the TOE while others belong to the TOE environment.

The components of the TOE environment are the following:

- RRU: the RRU is the remote radio unit, which processes the weak signals from the antenna system and transmits these processed the signals to the BBU. In addition, the RRU processes the digital signals from the BBU and transmits these the signals through antennas
- AAU: The active antenna system module is a new type of radio frequency module following the RFU and RRU, featured by incorporating functions of RRUs and conventional antennas, the AAU module has multiple transmit and receive signals.
- Hardware: It provides the physical hardware dependent environment for TOE running, including service control board and baseband board. The service control board is used for handling gNode services, mobility management, network resources management, network protocols, and cryptographic engine based on intel snowridge(QAT1.8, firmware is 5.1.0) integrated within intel atom P5942B/P5962B. The baseband board is used

for baseband signal processing. The TOE can be deployed in ZXRAN V9200 with the configuration of VSW series service control board and VBP series baseband board.

- Operating System: the gNodeB's operating system is CGEL(Carrier Grade Embedded Linux), which is an embedded operating system self-developed by ZTE based on public Linux (the Linux version 4.19.82-rt30-CGELV7.03.40B1), to provide process scheduling, memory management, file system, and network resources management, and the security-relevant components of containers and busybox run on top of the kernel. Also, The CRNG and haveged mechanisms are taken by operating system, to ensure that the data available to the read to the /dev/urandom and /dev/random have enough entropy to be used for cryptographic use cases.
- Base Band Service: Processing the data from Radio Remote Unit(RRU) /Active Antenna Unit(AAU) and resource scheduling.
- SGW: Secure Gateway(SGW) supports security tunnel for data transmission locating in the core network,
- UME: Unified Management Expert(UME) is management unit of the gNodeB, and provides configuration management and O&M management functions for gNodeB.
- AMF/MME: It is a unit of 5GC/EPC, which supports User Signaling process, including access control of terminal and pdu session establishment.
- UPF/S-GW: Its role includes acting as the mobility anchor point for the User Plane during handovers between gNodeB/eNodeB as well as data buffering when traffic arrives for a mobile in the 5G Idle state. Other functions performed by the UPF/S-GW include routing, Lawful Interception and billing.
- Terminal: Terminal by air interface data encryption and integrity protection, can share the wireless access through 5G network.

1.4 TOE Description

1.4.1 Physical scope

The release packages consist of software and documents.The 5G gNodeB software package is released in the form of binary compressed file.
The TOE consists of the following:

gNodeB software	**Name and version**
Software	UNI_V5.65.20.10F12.tar
Digital signature	UNI_V5.65.20.10F12.tar.sig.p7b

Document	**Format**
ZXRAN 5G gNodeB Commissioning Guide(Image Burning) R1.6	PDF
ZXRAN 5G gNodeB General Management R1.3	PDF
ZXRAN Base Station Security Hardening R1.9	PDF
ZXRAN 5G gNB Software Acceptance procedure v0.4	PDF

1.4.2 Logical scope

This section defines the logical scope of the TOE. The TOE is pure software. It is the core part of the software that is deployed into a 5G base station.

The architecture of the TOE's system is described in Figure 1. The TOE provides the following security functionalities:

1) Communication security

- **Communication between TOE and UEs**

  The TOE supports the encryption and integrity protection of air interface, which uses the AES,Snow3G and ZUC security algorithms. It ensures the security of user data and signaling.

- **Communication between TOE and another BBU/SGW**

  Ipsec is used in the backhaul interfaces to protect the traffic between the TOE and other network elements such as gNodeB(Xn interface) ,eNodeB(X2 interface) or security gateway(NG,S1 or OMCH interface). Ipsec is used to establish a secure channel between itself and peer entity(security gateway or base station). It mainly provides integrity ,confidentiality and authentication security features.

2) Transport Security (telecom network)

The TOE includes multiple security technologies to ensure transmission security of backhaul networks,such Ipsec,VLAN,and ACL.etc.

- VLANs(Virtual Local Area Networks) are implemented to separate the traffic from different flow planes(control panel,user panel and management panel),which reduce traffic storms and avoid resource overhead.
- ACL(Access Control List) uses the packet filtering technology to read the information in the packet header, such as the source address, destination address, source port, and destination port. Packets are filtered in accordance with the predefined rules to achieve the purpose of access control.

3) User Identification and Authentication

Each user has the information (such as role, password, idle time, account lock, etc.)Users identification and authentication is enforced so users must be authenticated by user name and user password before using or managing the TOE.

During authentication, User session are monitored and passwords are verified to enforce secure authentication. furthermore, the Identification and authentication of the users differ depending on the entity storing the credentials, the following shows two storing credential scenarios.

A. Local user access: The local users are those whose credentials are stored in the TOE. The users access the TOE for executing device management functions and are identified by individual user name and authenticated by passwords. The roles of local user include: Administrator, Maintenance and Ordinary.
B. centralized user access: The centralized users are those whose credentials are stored in the UME (Unified Management Expert), ,

such as the password is stored in the UME. In this case, the users accounts are created and managed by the UME, which means that their information is stored in the UME. When centralized users access to the TOE, TOE will send the username to the UME to query the user information, and the UME will return the role and credential of this user to the TOE by a secure tunnel. Then the TOE implements the authentication with credential return from the UME, and grant the corresponding permissions based on the role of this user.

4) Access Control

Access control is strictly enforced to TOE users based on their role and the access control policy to access objects i.e.user information and setting information.

Based on user's role, user could modify, create or delete objects. User with administrator privilege could operate user's role type.

5) Digital Signature Verification during software upgrade

When the software is upgraded, the TOE uses the digital certificate pre-installed in the factory to decrypt the hash value from the digital signature of the software, and compare it with the hash value of the software by calculating to verify the software consistency.

6) Logging and auditing

User activities on TOE are recorded to provide full accountability of the user actions, and the log trail is protected against unauthorized modification. The TOE provides administrators with the log review capabilities.

2 Conformance Claims

This ST claims to conforms to version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation Part 1-Introduction and general model, Version 3.1 Revision 5, April 2017,CCMB-2017-04-001 [CCp1]
- Common Criteria for Information Technology Security Evaluation Part 2-Security functional components, Version 3.1 Revision 5, April 2017,CCMB-2017-04-002 [CCp2]
- Common Criteria for Information Technology Security Evaluation Part 3-Seucirty assurance components, April 2017,CCMB-2017-04-003 Version 3.1 Revision 5, [CCp3]

The following methodology will be used for the evaluation

- “Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, Version 3.1, Revision 5, April 2017,CCMB-2017-04-004 [CEMe].

This Security Target claims conformance to the assurance package EAL 4 augmented. The augmentation to EAL4 is ALC_FLR.2.

This Security Target claims conformance to no Protection Profile.

3 Security Problem Definition

This section describes the assets, thread agents and threads to the TOE.

3.1 Assets

A.USER_DATA	User data from a user device that is transmitted by the TOE.
A.TSF_DATA	TSF data stored and managed by the BBU and that is used to enforce the security mechanism, such as the stored user passwords, the user attributes, or the encryption keys for the trusted channels.
A.ADMIN_ACCESS	Configuration information which represents privilege of administrator.
A.TSF_ACTIVITY_LOGS	User and administrator log records generated by the TSF.

3.2 Threat agents

TA.REMOTE	A attacker with access to the backhaul Network that is connected to the TOE and/or with access to the air network between UE and RRU/AAU. This agent does not have authorized access to the UME or the BBU.
TA.USER	An attacker with authorised access to the BBU, but without any administrative rights.

3.3 Threats

T.COMMUNICATION_CH	**TA.REMOTE** may be able to disclose or modify **A.USER_DATA** or **A.TSF_DATA** data while being transmitted through secure networks.
T.UNAUTHENTICATED_USER	**TA.REMOTE** may be able to bypass the user authentication and access the TOE and administrator configuration (**A.ADMIN_ACCESS**) on the TOE and modify A.TSF_DATA .
T.UNAUTHORIZED_ADMIN	**TA.USER** may be able to bypass the access control policy of the TOE, access to administrator configuration (**A.ADMIN_ACCESS**) and then modify A.TSF_DATA.
T.UNDETECTED_ACTIVITY	**TA.REMOTE** or **TA.USER** may be able to attempt or perform abusive actions on the TOE without administrator awareness (**A.TSF_ACTIVITY_LOGS**).

3.4 Assumptions

A.PHYSICAL_PROTECTION	5G gNodeB equipment are placed in a safe and controllable places. This equipment is maintained and operated only by authorized

	personnel.
A.ADMINISTRATORS	The personnel working as authorized administrators are trustworthy and trained for the TOE administration.
A.NETWORKSEGREGATION	It is assumed that the management network, the telecom network and the signal network are separated between each other
A.SECUREPKI	There is a well-managed and protected public key infrastructure. The certificate used by the TOE and its clients are managed by PKI.
A.TRUSTEDITPRODUCTS	It is assumed that： 1. The UME and CN NEs shall be deployed in the operator's core equipment room. And the SGW need to be deployed to ensure the security of the traffic entering the room. 2. Only authorized personnel can enter the computer room, and registration is required for entering and exiting the equipment room 3. Physical security measures such as door access control and monitoring are required in the core equipment room.
A.RELIABLETIMESTAMPS	It is assumed that the TOE can get reliable time stamps from the operational environments.

4 Security Objectives

The security objectives describe how the threats described in the previous section will be addressed. It is divided into:

- The Security Objectives for the TOE, describing what the TOE will do to address the threats
- The Security Objectives for the Operational Environment, describing what other entities must do to address the threats

A rationale that the combination of all of these security objectives indeed addresses the threats may be found in section 7.1 of this Security Target.

4.1 Security objectives for the TOE

O.SECURE_COMMUNICATION The TOE shall provide secure communication with external entities including::

1. User Equipments(UE)
2. Another BBU
3. Secure Gateway (SGW)
4. User Management Expert (UME)

O.USER_AUTHENTICATION The TOE shall enforce the user authentication on all user access to the gNodeB, the identification and authentication mechanism shall be implemented in the following users : local user and centralized user.

O.ACCESS_CONTROL The TOE shall implement a flexible role-based access control mechanism. Each role allows a user to access certain objects, and the TOE shall ensure that users can only access to objects when they have a role that allows them to access.

O.DIGITALSIGNATURE The TOE must provide functionality to verify the integrity of the received software packages and patches.

O.AUDITING The TOE shall enforce logging of user actions and provide auditing capabilities to the administrator role.

4.2 Security objectives for the Operational Environment

OE.PHYSICAL_PROTECTION BBU and UME server hardware equipment shall be placed in a secured and controllable space. These equipment shall be maintained and operated only by authorized personnel.

OE.ADMINISTRATORS The personnel working as authorized administrators shall be trustworthy and thoroughly trained for the TOE administration and will follow the TOE's user guidance.

OE.NETWORKSEGREGATION	The TOE environment shall ensure that management network and signal network and telecom network are separated from each other.
OE.SECUREPKI	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.
OE.TRUSTEDITPRODUCTS	1. The UME and CN NEs shall be deployed in the operator's core equipment room. And the SGW need to be deployed to ensure the security of the traffic entering the room. 2. Only authorized personnel can enter the computer room, and registration is required for entering and exiting the equipment room 3. Physical security measures such as door access control and monitoring are required in the core equipment room.
OE.RELIABLETIMESTAMPS	The operational environment shall provide reliable time stamps.

5 Security Requirements

5.1 Extended components definition

There are no extended components defined.

5.2 Definitions

The following terms are used in the security requirements:

5.2.1 Subject

- **S.BBU-user:** the external users accessing to the TOE that are connected through the local network.

5.2.2 Objects

O.User: the entity in TOE represents user account. Each user account has the following information:

- **O.User.username**: User unique identifier;
- **O.User.password**: the user password;
- **O.User.rolesList:** is the list of roles of the user;
- **O.User.rule**: is the security rule of the user;
- **O.User.isLocked**: this indicates if the user account is locked or not. Only not **locked users are allowed to login;**

O.Rule: this object includes all information of the security rule, including:

- **O.Rule.passwordExpirationDate:** is the expiration date of user password if used;
- **O.Rule.passwordHistoryNumber: t**he history number of the last passwords. When set, the user cannot use the passwords in this password history for when changing the password.
- **O.Rule.authenticationAttempts:** is the maximum authentication attempts allowed for the user before locking its account.
- **O.Rule.lockedPeriod:** is the period of time that the user account will remain locked;

O.Setting: this object includes all information of the security common setting, including:

- **O.Setting.idleTimeout**: is the amount of time that the user can remain idle before it is logged out.

5.2.3 Operations

Create, modify, delete, read

*5.2.4 **User group/role***

Roles: the role information including:

- **Role.type**: it can be one of the following:

- Administrator - super root user, which is not restricted by password expiration, and has totally permissions to all the configuration parameters.
- Maintenance – Users that have read, write, and execute permissions to all configuration parameters but the configuration parameters under security management (SecM) node, and have no any permissions to configurations under SecM node.
- Ordinary – Users that have no any permissions to the configuration parameters under SecM node, and only have read-only permission to the other configuration parameters.

Application note: SecM is the abbreviation for security management, which includes the security configuration management related to authentication, certificate and authorization.

5.2.5 Events

- **OP.lockUnlockUser**: to unlock or lock a user. A locked user is not able to log-in to the UME or gNodeB.
- **OP.userManagement**: to perform user management functions, which include to add, remove users or modify user attributes.
- **OP.RuleManagement**: to perform security rule management functions, which include managements functions include add, remove or modify security rule.
- **OP.idleTimeout: to** set the amount of time that a user can remain idle before it is logged out.
- **OP.authentication:** BBU-users get authenticated by TOE when logging in TOE.

5.2.6 External entities

- **UE:** user equipment used by the subscribers to connect to the gNodeBs using the air interface.
- **Other BBU**: this is another BBU supporting the TOE but performing the same function as the TOE's BBU.
- **Secure gateway (SGW)**: locates in the backhaul network and connect BBUs to other outer NEs,such as UPF,AMF.etc
- **UME**: Unified Management Expert(UME) is management unit of the gNodeB,and provides configuration management and O&M management functions for gNodeB.

5.3 Security Functional Requirements

5.3.1 Security Audit(FAU)

5.3.1.1 FAU_GEN.1 Audit data generation

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the **[not specified]** level of audit; and
c) **[**The following auditable events:
- OP.authentication;
- OP.lockUnlockUser;
- OP.userManagement ;
- OP.idleTimeout**]**

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,**[**none**].**

Application note:
a) Start-up and shutdown of the audit functions is not explicitly logged, however the logging functionality is enabled at start-up and cannot be disabled.
b) The centralized users are managed by UME, so changing password of centralized users will not be logged.

5.3.1.2 FAU_GEN.2 User Identity Association

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

5.3.1.3 FAU_STG.1 Protected audit trail storage

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

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

5.3.1.4 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall **[ignore audited events]** and **[a notification is raised and reported to UME]** if the audit trail is full.

Application note:

Audit records can be exported to a backup server.

The limitation of audit storage is 10MBytes per day.

5.3.2 User Data Protection(FDP)

5.3.2.1 FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the **[**Role-based Access Control Policy**]** on **[**subjects: S.BBU-user, objects: O.user, O.Rule, O.setting and Software upgrade operation**]** and all operations among subjects and objects covered by the SFP

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

5.3.2.2 ***FDP_ACF.1 Security attribute based access control***

FDP_ACF.1.1 The TSF shall enforce the **[**Role-based Access Control Policy**]** to objects based on the following:**[**subjects: all subjects, objects: all objects security attributes: Role.type**]**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[S.BBU-user has the following operations under different Role.types:

Role	operation	Allowed actions
Administrator	modify	O.Setting.idleTimeout, O.Rule.passwordExpirationDate, O.Rule.passwordHistoryNumber, O.Rule.authenticationAttempts, O.Rule.lockedPeriod, O.User.isLocked, O.User.rolesList
	read	all Objects except O.User.password
	create,modify, delete	O.User
	Software upgrade operation	The link between the gNB and the UME is established with the user (administrator permission), software upgrade can be downloaded to TOE, and the TOE performs the software integrity verification.
Maintenance	**No permissions**	No permissions for security configuration parameters uner security management node(SecM).
Ordinary	**No permissions**	No permissions for security configuration parameters uner security managementl node(SecM).

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:**[**

- user account is locked (i.e.O.User.isLocked is True);
- user account has no role assigned (i.e.O.User.rolesList is empty);
- S.BBU-user session has been terminated due to inactivity (O.Setting.idleTimeout);
- user account's password has expired (current time >= O.Rule.passwordExpirationDate);

5.3.2.3 FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1The TSF shall enforce the **[**Role-based Access Control Policy**]** to **[receive]** user data in a manner protected from **[modification]** errors.

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

5.3.3 Identification and Authentication(FIA)

5.3.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **[an administrator configurable positive integer (O.Rule.authenticationAttempts) within 1 and 6 (default 6)],** unsuccessful authentication attempts occur related to **[**OP.authentication**]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **[met]**, the TSF shall **[**lock the S.BBU-user account

- Until is unlocked by the administrator, or
- Until an administrator configurable time (O,Rule.lockedPeriod) has passed, if the account has not been set to permanent locking.**]**

5.3.3.2 FIA_ATD.1 User attribute definition

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

- O.User.username;
- O.User.password;
- O.User.rolesList;
- O.User.isLocked;
- O.Rule.passwordHistoryNumber;
- O.Rule.authenticationAttempts;
- O.Rule.lockedPeriod;**]**

5.3.3.3 FIA_SOS.1 Verification of secrets

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

- The range of the password minimum length is 8~20, and the default recommended value is 12. including four types: number, upper case letter, lower case letter, other characters;
- The new password cannot be the same as one of the last (O.Rule.passwordHistoryNumber) passwords.**]**

Application notes: secrets here refers to O.User.password.

5.3.3.4 FIA_UAU.2 User authentication before any action

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

5.3.3.5 FIA_UID.2 User identification before any action

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

5.3.4 Security Management (FMT)

5.3.4.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **[**Access Control Policy**]** to restrict the ability to **[**Create, Modify, Delete, Read**]** the security attribute **[**

- O.User.username;
- O.User.password;
- O.User.rolesList;
- O.User.isLocked;
- O.Rule.passwordHistoryNumber;
- O.Rule.authenticationAttempts;
- O.Rule.lockedPeriod;**]**

to [Administrator**].**

5.3.4.2 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **[**Access Control Policy**]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **[**Administrator**]** to specify alternative initial values to override the default values when an object or information is created.

5.3.4.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management function:**[**
User Management
Users authorization management
Configuration of SSH/TLS
Configuration of IPSec
Configuration of ACL
Configuration of VLAN
Configuration of Uu-U interface
]

5.3.4.4 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: **[**Administrator, Maintenance, Ordinary**]**

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

5.3.5 TOE access(FTA)

5.3.5.1 FTA_MCS.1 Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The TSF shall Restricts the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of **[10]** sessions per user.
Application note:

For local user, the number of concurrent session per user is configured from 1 to 20, 10 by default.
For centralized user, the number of concurrent session per user is fixed value of 20.

5.3.5.2 FTA_SSL.3 TSF-initiated termination
FTA_SSL.3.1 The TSF shall terminate an interactive session after **[**configured time **].**
Application note: The configured time is set in Setting.idleTimeout.

5.3.6 Trusted Path/Channels(FTP)

5.3.6.1 FTP_ITC.1[BBU-SGW] Inter-TSF trusted Channel

FTP_ITC.1.1[BBU-SGW] 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[BBU-SGW] The TSF shall permit the **[the TSF, another trusted IT product]** to initiate communication via the trusted channel.
Application notes: another trusted IT products here refers to SGW.

FTP_ITC.1.3[BBU-SGW]The TSF shall initiate communication via the trusted channel for **[**transmission of management user data**].**

5.3.6.2 FTP_ITC.1[BBU-BBU] Inter-TSF trusted Channel

FTP_ITC.1.1[BBU-BBU] 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[BBU-BBU] The TSF shall permit the **[the TSF, another trusted IT product]** to initiate communication via the trusted channel.
Application notes: another trusted IT products here refers to another BBU.

FTP_ITC.1.3[BBU-BBU] The TSF shall initiate communication via the trusted channel for **[**transmission of management user data**].**

5.3.6.3 FTP_ITC.1[BBU-UME] Inter-TSF trusted Channel

FTP_ITC.1.1[BBU-UME] 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[BBU-UME] The TSF shall permit the [**the TSF, another trusted IT product]** to initiate communication via the trusted channel.
Application notes: another trusted IT products here refers to UME.

FTP_ITC.1.3[BBU-UME] The TSF shall initiate communication via the trusted channel for **[**transmission of management data**].**

5.3.6.4 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and **[remote]** ***UE*** that are logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **[modification,disclosure].**

FTP_TRP.1.2 The TSF shall permit **[the TSF, remote *UE*]** to initiate communication via the trusted path.
FTP_TRP.1.3 The TSF shall require the use of the trusted path for **[transmission of user data].**

5.3.7 Protection of the TSF(FPT)

5.3.7.1 FPT_TST.1 TSF testing
FPT_TST.1.1 The TSF shall run a suite of self tests **[during initial start-up]** to demonstrate the correct operation of **[the TSF].**

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **[TSF data]**.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of **[TSF]**.

5.4 Security Assurance Requirements

The assurance requirements are EAL4+ ALC_FLR.2 and have been summarized in the following table:

Assurance Class	Assurance Components	
	Identifier	Name
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.4	Production support,acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw reporting procedures
	ALC_LCD.1	Developer defined life-cycle model
	ACL_TAT.1	Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3	Focused vulnerability analysis

5.5 Security Assurance Requirements Rationale

The Security Assurance Requirements for this Security Target are EAL4+ALC_FLR.2. The reasons for this choice are that:

- EAL 4 is deemed to provide a good balance between assurance and costs and is in line with ZTE customer requirements.
- ALC_FLR.2 provides assurance that ZTE has a clear and functioning process of accepting security flaws from users and updating the TOE when required. This is also in line with ZTE customer requirements.

6 TOE Summary Specification

This chapter describes how the TOE implements the security functional requirements defined in chapter 5. The description covers SFRs of gNodeB software unless explicitly stated.

6.1 Secure Communication

The TOE supports encrypted transmission between UE and TOE, another BBU and TOE, SGW and TOE, UME and TOE. It provides secure protocols, such as IPSec, TLS, VLANs, ACL and SFTP, for data transmission.

Recommended security algorithms in different channels

Channel	Security Technology	Algorithms	Key Length(bits)	References
TOE-UE	Radio Security	NEA1-based on SNOW 3G	128	3GPP TS33.501
		NEA2-based on AES-128	128	
		NEA3-based on ZUC	128	
		NIA1-based on Snow3G	128	
		NIA2-based on AES	128	
		NIA3-based on ZUC	128	
TOE-BBU	IPSEC with IKE V2	AES-128 CBC/CTR/GCM	128	3GPP TS33.210
		AES-192 CBC/CTR	192	
		AES-256 CBC/CTR/GCM	256	
		AUTH_HMAC_SHA2_256_128	256	
		AUTH_HMAC_SHA2_512_256	512	
		DH group14/15/18	2048/3072/8192	
		ECDH group19/20	256/384	
		PRF_HMAC_SHA2_256/384/512	256/384/512	
TOE-SGW	IPSEC with IKE V2	AES-128 CBC/CTR	128	3GPP TS33.210
		AES-192 CBC/CTR	192	
		AES-256 CBC/CTR	256	
		AUTH_HMAC_SHA2_256_128	256	
		AUTH_HMAC_SHA2_512_256	512	
		DH group14/15/18	2048/3072/8192	
		ECDH group19/20	256/384	
		PRF_HMAC_SHA2_256/384/512	256/384/512	
	VLAN	None	None	
TOE-UME	TLS	ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Cipher suit	3GPP TS33.210
		DHE_RSA_WITH_AES_128_GCM_SHA256	Cipher suit	
		ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Cipher suit	
		ECDHE_RSA_WITH_AES_256_GCM	Cipher suit	

		_SHA384		
	SFTP based on SSH 2.0	AES-128/192/256 CTR	128/192/256	RFC 4253 RFC 4344 RFC 6668 RFC 8268 RFC 4432 RFC 5656 RFC 8332
		SHA256/384/512	256/384/512	
		DH group14/16/18	2048/4096/8192	
		ECDH group19/20	256/384	

FTP_ITC.1[BBU-SGW], FTP_ITC.1[BBU-BBU]. FTP_ITC.1[BBU-UME], FTP_TRP.1,FMT_SMF.1

6.2 User identification and authentication

The TOE users are required to identify and authenticate themselves before they can perform any action using the TOE.
The following identifies the allowed action for each role in the ToE,

- Administrator - super root user, which is not restricted by password expiration. except user password, administrator can modify any security parameters.
- Maintenance – Users that have the permissions to perform read, write, and execute operations on all other non-security configuration parameters, and have no permissions for security configurations.
- Ordinary –Users that have no permissions to perform read, modify or create any security configuration parameters, and only have read permissions for non-security parameters.

The TOE maintains user information in order to enforce authentication and access control. The following information is maintained for each user:

- User name and password;
- Password history number;
- user role;
- Locked and unlocked status indicators;
- The security rules of the user.

Moreover, TOE also maintains rule information(O.Rule) including: expiration date, the length of password, allowed authentication time, number of authentication attempts and locked period, the number of password history.etc

User authentication is based on the username and password provided by the users and has a limited number of attempts before the user account is locked. User access can also be restricted based on the user's terminal IP.

Users can be unlocked by the administrator. Users can also wait to be automatically unlocked after a period of time that is configurable by the administrator.

User passwords have to meet following rules to ensure that the passwords cannot be easily guessed or broken by brute force, Passwords that do not meet these rules are rejected by the TOE.

- The range of the password minimum length is 8~20, and the default recommended value is 12. including four types: number, upper case letter, lower case letter, other characters;
- The new password cannot be the same as one of the last (O.Rule.passwordHistoryNumber) passwords.

User concurrent sessions are limited to a maximum 10 for each user by default (with 20 as maximum configurable value). Furthermore, the sessions are automatically terminated after period of inactivity that is configurable by the administrator.

FIA_AFL.1,FIA_ATD.1,FIA_SOS.1,FIA_UAU.2,FIA_UID.2,FTA_MCS.1,FMT_SMF.1 ,**FTA_SSL.3,**

6.3 Access Control

The TOE enforces access control on users based on user roles and access control policy to access objects in TOE.
Access control is implemented as follows:

- To facilitate user authorization and management, the administrator sets users with the same operation permissions into one group. The TOE supports three groups (administrator, maintenance, and ordinary). These groups/roles are only applicable to local users. The groups/roles permissions are limited as following:

Role	operation	Allowed actions
Administrator	modify	O.Setting.idleTimeout, O.Rule.passwordExpirationDate, O.Rule.passwordHistoryNumber, O.Rule.authenticationAttempts, O.Rule.lockedPeriod, O.User.isLocked, O.User.rolesList
	read	all Objects except O.User.password
	create,modify, delete	O.User
	Software upgrade operation	The link between the gNB and the UME is established with the user (administrator permission), software upgrade can be downloaded to TOE, and the TOE performs the software integrity verification.
Maintenance	**No permissions**	No permissions for security configuration parameters uner security management node(SecM).
Ordinary	**No permissions**	No permissions for security

		configuration parameters uner security management node(SecM).

Based on user's role, user could modify, create or delete objects. Additionally, administrator can create and delete user account. Users with maintenance role or ordinary role do not have capabilities to operate objects.

- This access control policy is used to restrict the ability to modify the users relationship.

Security attributes have the following policies.

- The range of the password minimum length can be configured from 8 to 20, and the default value is 12, that means the default minimum password length is 12+x. The password must contain digits, upper-case letters, lower-case letters, and other characters. The password cannot contain the username, three or more than three consecutive same characters.
- The password must have a expiration data, the value can be configured from 0 to 99999 days, and the default value is 99999 days.
- The history password number limitation can be configured from 1 to 50, and the default value is 3.
- The login attempts number can be configured from 1 to 6, and the default value is 6. Once the user enter consecutively wrong password number exceeds the value, the user will be locked, and the locked period can be configured from 2 to 100 min, the default value is 2 min.

FMT_MSA.1,FMT_SMF.1,FMT_MSA.3,FMT_SMR.1,FDP_ACC.2 and FDP_ACF.1

6.4 Audit

The TOE generates audit logs to record the following events:

- User authentication;
- Locking or unlocking a user account;
- Add, remove or modify a user account;
- When a user session is terminated by timeout;

The log records include date and time of event, user identity, and the outcome (success or failure) of the event.

In case of the audit storage exceeds the threshold (10MBytes per day), the new audited events are ignored, meanwhile a notification is generated and reported to the UME.

The gNodeB prevents all users to modify or delete the audit logs files by:

Set the log file permission to 640. Only the administrator user can view and modify the log file.The users in the same group can view but cannot modify the log file.Other users cannot view the log file.

FAU_GEN.1, FAU_GEN.2, FAU_STG.1 and FAU_STG.4

6.5 Digital signature

Digital signature mechanism is taken to ensure the legitimacy and integrity of the software packages.

The TOE automatically checks the digital signature of the software when the user with the administrator role runs the software upgrade (note: the link between the gNB and the UME should be established by using the user with administrator permission for accessing control policy).

- The software is released with the digital signature signed by using SHA256 hash algorithm and RSA2048 (both algorithms can be used a higher level) .
- When the device software is upgraded, the TOE uses the digital certificate installed in the factory to decrypt the hash value from the digital signature of the software.
- The TOE gets another hash value of the software by calculating.
- Compare the two hash values, if they are same, the check passes, otherwise the download fails and the user is prompted that the version file check has failed.

During the startup process, the CPU boot also will verify the integrity of the TOE according to digital signature, using SHA256 hash algorithm and RSA2048 (both algorithms can be used a higher level) public key.

This digital signature verification is implemented in the TOE.
FDP_UIT.1, FPT_TST.1

7 Rationales

7.1 Security Objectives Rationale

Assumptions/Threats	Objectives
T.COMMUNICATION_CH	This thread is directly covered by **O.SECURE_COMMUNICATION** as it enforce to use secure communication channels on all communications between: 1. The subscriber (UE) and the BBU; 2. A BBU and another BBU; 3. A BBU and the trusted gateway of the core network; 4. A BBU and UME.
T.UNAUTHENTICATED_USER	This thread is directly covered by **O.USER_AUTHENTICATION** as it enforces user authentication on BBU components.
T.UNAUTHORIZED_ADMIN	This thread is directly covered by **O.USER_AUTHENTICATION, O.ACCESS_CONTROL** as these enforce user authentication and authorization based on the user's role.
T.UNDETECTED_ACTIVITY	This thread is directly covered by **O.USER_AUTHENTICATION ,O.DIGITALSIGNATURE** and **O.AUDITING** as these enforce user authentication and logging of user actions on the BBU
A.PHYSICAL_PROTECTION	This assumption is upheld by **OE.PHYSICAL_PROTECTION**, which directly covers the assumption.
A.ADMINISTRATORS	This assumption is upheld by **OE.ADMINISTRATORS**, which directly covers the assumption.
A.NETWORKSEGREGATION	This assumption is upheld by **OE.NETWORKSEGREGATION**, which directly covers the assumption.
A.SECUREPKI	This assumption is upheld by **OE.SECUREPKI**, which directly covers the assumption.
A.TRUSTEDITPRODUCTS	This assumption is upheld by **OE.TRUSTEDITPRODUCTS**, which directly covers the assumption.
A.RELIABLETIMESTAMPS	This assumption is upheld by **OE.RELIABLETIMESTAMPS**, which directly covers the assumption.

7.2 Security Functional Requirements Rationale

Security objectives	SFRs addressing the security objectives
O.SECURE_COMMUNICATION	This objective is met by: • Secure communication between the TOE and the UE (**FTP_TRP.1**) • Secure communication between the TOE and the secure gateway (**FTP_ITC.1[BBU-SGW])** • Secure communication between the TOE and another BBU (**FTP_ITC.1[BBU-BBU]**) • Secure communication between the TOE and UME (**FTP_ITC.1[BBU-UME]**)
O.USER_AUTHENTICATION	This objective is met by: • User identification and authentication before any action (**FIA_UID.2,FIA_UAU.2)** • Limited user authentication attempts(**FIA_AFL.1**); • Complex user password (**FIA_SOS.1**); • Limitation of user session (**FTA_SSL.3** and **FTA_MCS.1**);
O.ACCESS_CONTROL	This objective is met by: • User roles and attributes implementation (**FIA_ATD.1 and FMT_SMR.1**); • Enforcing access control based on user roles and attributes (**FDP_ACC.2, FDP_ACF.1, FMT_MSA.1 and FMT_MSA.3,FMT_SMF.1**);
O.DIGITALSIGNATURE	• The objective is met by: • The TOE performs digital signature verification over the software patches during software upgrade (FDP_UIT.1) • The TOE performs digital signature verification over software during start up (**FPT_TST.1**)
O.AUDITING	• This objective is met by: • Audit data generation (**FAU_GEN.1**); • User Identity Association(**FAU_GEN.2**) • Audit data protection (**FAU_STG.1 and FAU_STG.4**);

7.3 Dependencies

SFR	Dependency
FAU_GEN.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.2
FAU_STG.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1
FDP_ACC.2	FDP_ACF.1
FDP_ACF.1	FDP_ACC.2 FMT_MSA.3
FDP_UIT.1	FDP_ACC.2 FTP_ITC.1[BBU-UME]
FIA_AFL.1	FIA_UAU.2
FIA_ATD.1	None.
FIA_SOS.1	None.
FIA_UAU.2	FIA_UID.2
FIA_UID.2	None
FMT_MSA.1	FDP_ACC.2 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	None.
FMT_SMR.1	FIA_UID.2
FTA_MCS.1	FIA_UID.2
FTA_SSL.3	None.
FTP_ITC.1/BBU-SGW	None.
FTP_ITC.1/BBU-BBU	None.
FTP_ITC.1/BBU-UME	None.
FTP_TRP.1	None.
FPT_TST.1	None

FPT_STM.1 is not implemented by the TOE , however we get a reliable time stamps from the TOE operation environments as defined in A.RELIABLESTAMPS.

Abbreviations

AC	Alternating Current
BBU	baseband unit
BPL	Baseband Processing module
CC	Control and Clock module
DC	Direct Current
EMS	Element Management System
EPS	Evolved Packet System
eNode B	Evolved Node B
UME	Unified Management Expert
gNode B	generation Node B
NG-RAN	NewGeneration -Radio Access Network
FA	Fan Array Module
IP	Internet Protocol
IPSEC	Internet Protocol Secure
NR	New Generation
LED	Light Emitting Diode
LTE	Long Term Evolution
L3	Layer 3
MME	Mobility Management Entity
MAC	Media Access Control
NAS	Non-Access Stratum
PDCP	Packet Data Convergence Protocol
PHY	Physical Layer
PM	Power Module
RF	Radio Frequency
RLC	Radio Link Control
RRU	Remote Radio Unit
SA	Site alarm Board
SE	Site alarm Extension Board
S-GW	Serving Gateway
AMF	Access and Mobility Management Function
UPF	User Port Function
SGW	Security gateway
UE	User Equipment
UMTS	Universal Mobile Telecommunications System

A References

[CCp1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, version 3.1 Revision 5, April 2017.

[CCp2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, version 3.1 Revision 5, April 2017.

[CCp3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, version 3.1 Revision 5, April 2017.

[CEMe] Common Methodology for Information Technology Security Evaluation Evaluation methodology, version 3.1 Revision 5, April 2017.

[TS33-501] 3GPP TS33.501 Security architecture and procedures for 5G system