ZTE RAN Solution
Security Target

LEGAL INFORMATION

Revision History

Version	Date	Comment
0.1	Oct 23 2019	First version
0.2	Dec 16 2019	General revision
0.3	Jan 14 2020	General revision applying changes
0.4	Jan 22 2020	General revision applying changes
0.7	July 27 2020	Minor revision applying changes
0.9	August 6 2020	SPD and security objectives added.
0.10	August 10 2020	UME components changed
0.11	August 14 2020	Update UME components
0.12	August 17 2020	Fix SFR operations
0.13	August 19, 2020	Fix minor issues
0.14	August 21, 2020	Minor fixes and an application note added to FTP_ITC.1/BBU-UE.
0.15	August 27, 2020	Change UME version and minor fix in SFR operations.
0.16	September 1, 2020	Accepted changes
0.17	September 29, 2020	Section 6.2 updated
0.18	October 10, 2020	FTA_MCS.1/BBU and TSS updated
0.19	October 22, 2020	FTA_MCS.1/BBU Basic limitation on multiple concurrent sessions updated
0.20	December 17, 2020	Updated after evaluator’s feedback.
0.21	January 19, 2021	FAU_STG.4/BBU added to Security Functional Requirements Rationale and the dependencies table.
0.22	February 4, 2021	Fixed versions of the acceptance procedure documents [UG-BBU-ACP] and [UG-UME-ACP].

Contents

1 ST Introduction

1.1 ST reference

Title	ZTE RAN Solution Security Target
Version	0.22
Date	February 04, 2021
Author	ZTE

1.2 TOE reference

TOE Name	ZTE RAN	
TOE version	V3.00.30.20P10	
TOE Components	baseband unit (BBU)	ZXRAN V9200
	remote RF unit (RRU)	ZXRAN R9105
		ZXSDR R8998
		ZXSDR R8862
		ZXSDR R8852
		ZXRAN R8894
		ZXRAN R8854
		ZXRAN R9212
		ZXRAN R9214
		ZXRAN R9222
	Active Antenna Unit (AAU)	ZXRAN A9611
		ZXRAN A9815
		ZXRAN A9631
		ZXRAN A9622
	Unified Management Expert (UME), V16.20.30	
Developer	ZTE	

1.3 TOE Overview and usage

The TOE is a New Generation Radio Access Network (NG-RAN) system solution for NR (new radio) network plus an UME. The solution interfaces with User Equipment (UE) and implements such functions as radio resource management, data stream IP header compression and encryption, attach progress selection, user plane data routing, data scheduling and transmission, and mobility management. The UME is used to manage the system via web interface.

The TOE consists of three parts; a baseband unit (BBU), a remote RF unit (RRU) or an active antenna unit (AAU) and a unified management expert (UME):

- BBU is the device processing the analog to digital conversion of the signal;
- RRU is the remote radio unit transceiver;
- AAU incorporates a radio frequency processing module and antenna;

- UME is a unified intelligent operation and maintenance system for RAN.

UME provides the intelligent operation and maintenance management of network and the on-demand deployment and the gray-scale based upgrade of system.

The TOE is connected by three networks:

- Core network: This is the internal network of the provider, and is considered secure in this evaluation.
- A backhaul network: This is an external network and is considered insecure in this evaluation.
- An IP Management network: This is the internal network of the provider and is considered secure in this evaluation.

The TOE and these networks are shown in Figure 1.

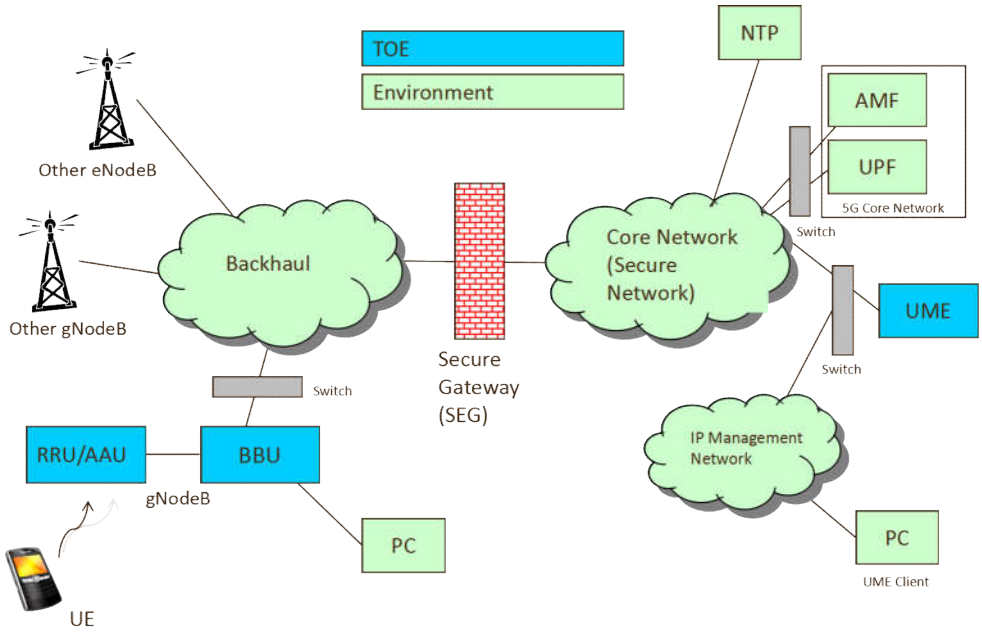


Figure 1: The TOE in its environment

The RAN which is equivalent to gNodeB has the following general functionalities:

- Radio resource management: radio bearer control, radio admission control;
- Access mobility management;
- IP header compression and user data stream encapsulation;
- Paging message scheduling and transmission;
- Broadcast message scheduling and transmission;

1.3.1 Major security features

The major security features of the TOE are:

- Secure management and usage of the TOE, to ensure that only properly authorized staff can manage and/or use the TOE;
- Provides secure interaction between various parts of the TOE and between the TOE and various machines in the environment, so that user data and/or management commands cannot be read or modified in between;
- Provides logging and auditing of user actions.

1.3.2 Non-TOE Hardware/Software/Firmware

The additional systems required by the TOE are:

- L3 Switches providing filtering services to the UME Server and BBU part of the TOE;
- Secure Gateway: The RAN connects to a secure gateway (SEG) using IPSec. The SEG then connects to a secure network (Core) where AMF/UPF/UME connects to;
- UME server: the UME application requires a platform to run consisting on the physical hardware and firmware, the operating system.
- AMF function providing:
    - Allocating paging message to RAN;
    - Security control;
    - Idle state mobility control;
    - UPF bearer control;
    - NAS signaling encryption and integrity protection.
- UPF function providing:
    - Supporting UE's mobility switching user plane data;
    - Downlink packet data buffer and paging support in NG-RAN idle mode.

1.4 TOE Description

1.4.1 Physical scope

The TOE consists of the following:

BBU	**Name and version**
Hardware	V9200
Software	NR: V3.00.30.20P10

RRU	**Name and version**
Hardware	R9105, R9212, R8998, R8894, R8854, R9222 or R9214 R8862 or R8852
Software	V3.00.30.20P10

AAU	**Name and version**
Hardware	A9611, A9815, A9631 or A9622
Software	V3.00.30.20P10

UME	Name and version
Software	UME Server version ElasticNet UME V16.20.30
	SSH Server(Apache SSHD v2.1.0)
	SFTP server(apache-sshd-core v2.2.0)
	LDAP server(ApacheDS 2.0.0-M24)

The TOE hardware parts are delivered by courier, while software parts are either installed in the hardware or installed by ZTE engineers. The following documents are delivered by the ZTE engineers to the customer during the TOE installation:

Document	Version	Format
[UG-BBU-ACP] Acceptance procedure	0.4	PDF
[UG-BBU-CONF] RAN Configuration Management	1.3	PDF
[UG-BBU-HW-DES] ZXRAN V9200 Radio Access Network Product Description	2.0	PDF
[UG-BBU-HW-INS] ZXRAN V9200 Radio Access Network Hardware Installation	2.0	PDF
[UG-BBU-OPE] RAN Element Management	1.0	PDF
[UG-BBU-SW-INS] ZXRAN Base Station Commissioning Guide (Image Burning)	1.2	PDF
[UG-UME-ACP] Acceptance procedure	0.3	PDF
[UG-UME-INS] UME Installation and Deployment Guide	1.3	PDF
[UG-UME-LE] Security Log Events	1.0	PDF
[UG-UME-MML] UME Command List	1.0	PDF
[UG-UME-OPE-LOG] ElasticNet UME Log Management Operation Guide	R1.0	PDF
[UG-UME-OPE-OAOG] ElasticNet UME Open API Service Operation Guide	R1.0	PDF
[UG-UME-OPE-SMOG] ElasticNet UME Security Management Operation Guide	R1.0	PDF
[UG-UME-PRE] UME Software Integrity Protection Evidence description	1.0	PDF
[UG-UME-SPM] Security Parameter Manual	1.0	PDF
[UG-UME-UPG] UME Upgrade Guide	1.12	PDF
ZXRAN A9622E S35 5G Hardware Installation	1.0	PDF
ZXRAN A9631 S26 5G Active Antenna Unit Hardware Installation Guide	1.0	PDF
ZXRAN A9815 5G Active Antenna Unit Hardware Installation	1.0	PDF
ZXRAN A9611 S35 5G Active Antenna Unit Hardware Installation	1.0	PDF
ZXRAN R9105 S26 5G Remote Radio Unit Hardware Installation	1.0	PDF
ZXRAN R9105 S35 5G Remote Radio Unit Hardware Installation	1.0	PDF
ZXRAN R9212E Macro Radio Remote Unit Hardware Installation Guide	1.0	PDF
ZXRAN R9214E Macro Radio Remote Unit Hardware Installation	1.0	PDF
ZXRAN R9222 Macro Radio Remote Unit Hardware Installation Guide	1.0	PDF
ZXSDR R8862A Macro Remote Radio Unit Hardware Installation	1.0	PDF
ZXSDR R8998E S2600 TDD Multi-Path Remote Radio Unit Hardware	1.0	PDF

Installation		
ZXSDR R8998E S3700 TDD Multi-Path Remote Radio Unit Hardware Installation	1.0	PDF
ZXSDR R8852E Macro Remote Radio Unit Hardware Installation	1.0	PDF
ZXSDR R8854E Macro Radio Remote Unit Hardware Installation	1.0	PDF
ZXSDR R8894E Macro Radio Remote Unit Hardware Installation	1.0	PDF
ZXSDR R8894E Macro Radio Remote Unit Hardware Installation	1.0	PDF

1.4.2 Logical scope

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

- Users identification and authentication a is enforced so users must be authenticated by password before using or managing the TOE. User session are monitored and passwords are verified to enforce secure authentication;
- Access control is strictly enforced to TOE users based on their role and the access control policy;
- User management functionalities are provided to control the users and their attributes (role, password, idle time, account lock, etc.);
- TOE communications provide identification of its end-points and are protected against modification or disclosure. This protection includes the communication between TOE parts (UME, BBU-SEG, BBU-BBU) and communication between the TOE and external entities (BBU-UE);
- User activities on UME 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 conforms to:

- CC, version 3.1R5, as defined by [CCp1], [CCp2], [CCp3] and [CEMe].
- CC Part 2 as CC Part 2 conformant
- CC Part 3 as CC Part 3 conformant

This ST conforms to no Protection Profile.
This ST conforms to EAL 3+ALC_FLR.2, and to no other packages.

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 UME and 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. This data shall only be modified by users with **A.ADMIN_ACCESS**

A.ADMIN_ACCESS Administrative access to the UME and to the BBU.

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 UME or 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 unsecure networks.

T.UNAUTHENTICATED_USER **TA.REMOTE** may be able to bypass the user authentication and to access the UME or the BBU and perform administrative actions (**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 UME or the BBU and perform administrative actions (**A.ADMIN_ACCESS**) without administrator rights and modify A.TSF_DATA.

T.UNDETECTED_ACTIVITY **TA.REMOTE** or **TA.USER** may be able to attempt or perform abusive actions on the UME or the BBU without

administrator awareness (**A.TSF_ACTIVITY_LOGS**).

3.4 Assumptions

A.TIME	The environment will provide a reliable timestamp for the TOE.
A.UME_TRUSTED_NETWORK	The UME is deployed in a controlled environment; at the operator's equipment room in a trusted network. The UME is segregated from the core network and IP management network so only authorized network traffic is allowed.
A.PHYSICAL_PROTECTION	BBU and UME server hardware equipment are placed in a safe and controllable space. These 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.UME_PLATFORM	The underlying hardware, firmware, operating system an d other non-TOE software of the UME works correctly.
A.UME_CLIENT	The administrator uses a secure remote management terminal for remote access to the TOE. The client is up to date regarding security upgrades and cryptographic support.

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_COMUNICATION

The TOE shall provide the means to establish the following secure communication channels 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. The UME and the UME Client.

O.USER_AUTHENTICATION

The TOE shall enforce the user authentication on all user access to the BBU and UME.

O.ACCESS_CONTROL

The TOE shall implement a flexible role-based authorization framework. Each role allows a user to perform certain actions, and the TOE shall ensure that users can only perform actions when they have a role that allows them to perform such action.

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.TIME

The TOE environment shall provide reliable time via NTP service.

OE.UME_TRUSTED_NETWORK

The network segment used by the UME shall be secure and provide segregation from other networks via trusted gateway. The secure gateway (SEG) shall be able to provide secure communication with the BBU.

OE.PHYSICAL_PROTECTION

BBU and UME server hardware equipment shall be placed in a safe 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.UME_PLATFORM	The underlying hardware, firmware, operating system an d other non-TOE software of the UME shall work correctly.
OE.UME_CLIENT	The UME administrator shall use a secure remote management terminal for remote access to the TOE.- The client shall be up to date regarding security upgrades and cryptographic support.

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 Subjects:

- **S.UME-**user**:** the users with access to the UME and that are responsible for the TOE management and that are connected through the IP Management network;
- **S.BBU-**user**:** the users with access to the BBU and that are responsible for the BBU management and that are connected through the local network.

5.2.2 Operations

- **OP.lockUnlockUser**: to unlock or lock a user. A locked user is not able to log-in to the UME or BBU;
- **OP.lockUnlockRole**: to lock or unlock a role. A locked role prevents users that only have the locked role to operate the UME, excluding the following functions:
    - Change their password;
    - Log out from UME;
    - View UME version information;
    - Set time zone and DST;
    - Change view language.
- **OP.enableDisableUser**: to enable or disable a user account. A disabled user account cannot login to the UME or BBU;
- **OP.userManagement**: to perform user management functions, which include to add, remove users or modify user attributes from UME and BBU;
- **OP.logReview**: to review the logs generated by the UME;
- **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 from the UME or BBU.

5.2.3 Objects

- **O.user**: this object includes all information of the user account. The specific fields can be seen in the following section as these are considered security attributes;
- **O.role**: this object includes all information of the role object. The specific fields can be seen in the following section as these are considered security attributes;

- **O.rule**: this object includes all information of the security rule. The specific fields can be seen in the following section as these are considered security attributes;
- **O.setting**: this object includes all information of the security common settings. The specific fields can be seen in the following section as these are considered security attributes.

5.2.4 Security attributes

- **Rule**
  - **Rule.passwordExpirationDate**: is the expiration date of user password if used;
  - **Rule.passwordHistoryNumber**: the history number of the last passwords. When set, the user cannot use the passwords in this password history for when changing the password.
  - **Rule.allowedIPs**: is the list of the allowed source IPs for the user to log-in. If the log-in is requested from other IPs access is denied;
  - **Rule.allowedWorkSchedule**: is the accepted time schedule for the user to log-in. Outside this timeframe the user is not allowed for UME ;
  - **Rule.authenticationAttempts**: is the maximum authentication attempts allowed for the user before locking its account.
  - **Rule.lockedPeriod**: is the period of time that the user account will remain locked;
- **Setting**
  - **Setting.idleTimeout**: is the amount of time that the user can remain idle before it is logged out from the UME or the BBU.
- **User**
  - **User.username**: User unique identifier;
  - **User.password**: the user password;
  - **User.passwordHistory:** the user password change history;
  - **User.rolesList**: is the list of roles of the user;
  - **User.rule**: is the security rule of the user;
  - **User.isLocked**: this indicates if the user account is locked or not. Only not locked users are allowed to login;
  - **User.isEnable**: this Indicated if the user is enabled and can be used or not. Only enabled users are allowed to login;
- **Roles**
  - **Role.type(UME)**: it can be one of the following:
    - Security Administrator: this role has the right to conduct security data maintenance, but it has no business related privileges;
    - Administrator: this role has complete and unrestricted access to system, except maintenance of the security information;
    - Maintenance: this role has complete access to system and its managed network, except maintenance of the security information and maintenance system;

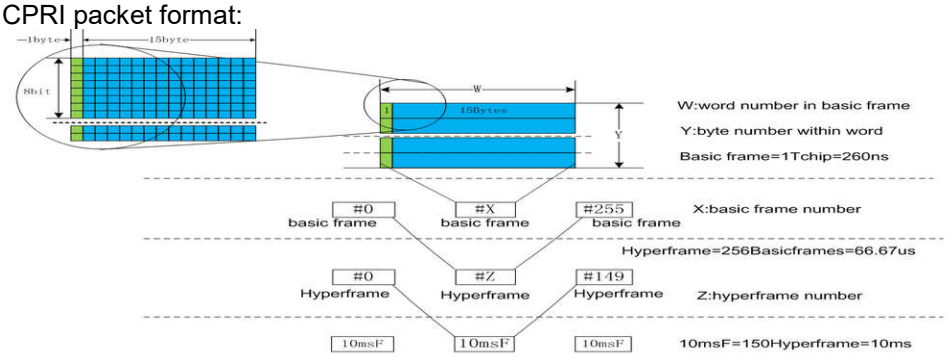
- Operator: this role has the right to view network information and conduct normal maintenance, but it cannot modify system sensitive information;
- Supervisor: this role has the right to view system information.

- **Role.type(BBU)**: it can be one of the following:
  - Administrator - super root user, which is not restricted by password expiration;
  - Maintenance - other user, which cannot create or modify user information and is restricted by password expiration;
  - Ordinary – ordinary user with no read, write, or execute permission for security management node data, and have read-only permission for other nodes such as radio common service, device, transport network, gNode function models.

- **Role.islocked**: this indicates if the role is locked or not. When a role is locked the users with that role cannot operate UME.

5.2.5 BBU And AAU/RRU entity:

The AAU/RRU and the BBU are connected through an optical fiber and communicate through the standard CPRI protocol. The following figure shows the CPRI packet format:



5.2.6 External entities:

- **UE:** user equipment used by the subscribers to connect to the BBUs using the backhaul network.
- **Other BBU**: this is another BBU working in the TOE environment but performing the same function as the TOE's BBU.
- **Secure gateway (SEG)**: is the gateway connecting the UME in the core network to the BBUs.

The following notational conventions are used in the requirements. Operations are indicated in **bold**, except refinements, which are indicated in ***bold italic***. In general

refinements were applied to clarify requirements and/or make them more readable. Iterations were indicated by adding three letters to the component name.

5.3 Security Functional Requirements

The security functional requirements are for UME and BBU. Since AAU/RRU that only enhances 3D beam forming for cubic coverage does not contain the security function, this section does not describe the security function requirements of AAU and RRU.

5.3.1 Security Functional Requirements for the UME

5.3.1.1 FIA_UID.2/UME User identification before any action

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

5.3.1.2 FIA_UAU.2/UME User authentication before any action

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

5.3.1.3 FIA_AFL.1/UME Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **a security administrator configurable positive integer within 3 and 20 (Rule.authenticationAttempts, default 3)** unsuccessful authentication attempts occur related to **S.UME-user authentication**.

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

- **Until is unlocked by the Security administrator, or**
- **Until a security administrator configurable time (Rule.lockedPeriod) have passed, if the account has not been set to permanent locking.**

5.3.1.4 FIA_SOS.1/UME Verification of secrets

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

- **At least 8 characters including four types: number, upper case letter, lower casee letter, other characters;**
- **Cannot be the same as the username, the username in reverse[1] or a common password dictionary word;**
- **The new password cannot be the same as one of the last (Rule.passwordHistoryNumber) passwords set in User.passwordHistory.**

[1] If the username is chang, “gnahc” is not allowed

5.3.1.5 FTA_SSL.3/UME TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session

- **After a period of inactivity that equals the configured time (Setting.idleTimeout);**
- **when one of the user roles in the user's list (User.rolesList) is being locked or being modified while the user is logged in.**

5.3.1.6 FTA_MCS.1/UME Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same **S.UME-user**.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of **1** session per **S.UME-user**.

5.3.1.7 FAU_GEN.1/UME Audit data generation

FAU_GEN.1.1 The UME 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:**
   - **S.UME-user authentication (security log);**
   - **OP.lockUnlockUser (security log);**
   - **OP.enableDisableUser (operation log);**
   - **OP.userManagement (operation log);**
   - **OP.ruleManagement (operation log);**
   - **OP.idleTimeout (operation log).**

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: 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.

5.3.1.8 FAU_SAR.1/UME Audit review

FAU_SAR.1.1 The TSF shall provide **S.UME-user with Administrator or Security Administrator in User.rolesList** with the capability to read **all log records** 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.

5.3.1.9 FAU_STG.1/UME Protected audit trail storage

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

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

5.3.1.10 FAU_STG.4/UME Prevention of audit data loss

FAU_STG.4.1 The TSF shall **overwrite the oldest stored audit records**[2] if the audit trail is full.

Application note: Audit records can be exported to a backup server.

5.3.1.11 FTP_TRP.1/UME-Client Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and **S.UME-user** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **modification and disclosure**.

FTP_TRP.1.2 The TSF shall permit **S.UME-user** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **initial user authentication and all UME management functions defined in FMT_SMF.1/UME**.

5.3.1.12 FIA_ATD.1/UME User attribute definition

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

- **User.username;**
- **User.password;**
- **User.passwordHistory;**
- **User.rolesList;**
- **User.rule;**
- **User.isLocked;**
- **User.isEnable;**

5.3.1.13 FMT_SMR.1/UME Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:

- **Security Administrator**
- **Administrator**
- **Maintenance**
- **Operator**

[2] The operation was completed to “take no other actions”, and this was subsequently refined away to make the sentence more readable.

- **Supervisor**

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

5.3.1.14 FMT_SMF.1/UME Specification of Management Functions

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

Management function	Related to SFR
OP.ruleManagement -> User.Rule.allowedIPs Set wether a user(assigned the rule) can only login from certain IP-addresses, and if so, which IP addresses.	**FDP_ACF.1/UME**
OP.idleTimeout -> Setting.idleTimeout Set the time that users may remain logged in while inactive.	**FTA_SSL.3/UME**
OP.ruleManagement -> User.Rule.allowedWorkSchedule Set whether a user(assigned the rule) is only allowed to work at certain times, and if so, at which times.	**FDP_ACF.1/UME**
OP.ruleManagement -> User.Rule.authenticationAttempts Set the number of allowed unsuccessful authentication attempts	**FIA_AFL.1/UME**
OP.ruleManagement -> User.Rule.lockedPeriod Set the time that an account(assigned the rule) remains locked	**FIA_AFL.1/UME**
OP.lockUnlockUser -> User.isLocked Unlock a user account	**FIA_AFL.1/UME**
OP.ruleManagement -> User.Rule.passwordExpirationDate Set whether a user(assigned the rule) password expires after a certain time, and if so, after how long	**FDP_ACF.1/UME**
OP.ruleManagement -> Rule.passwordHistoryNumber Set the length password history that it is maintained to prevent the users from using the same password. E.g. if set to 3, then the users cannot use the last 3 passwords	**FIA_SOS.1/UME**
OP.userManagement -> User.rolesList Add or remove roles to/from users	**FMT_SMR.1/UME**
OP.userManagement Create, edit and delete user accounts	**FIA_ATD.1/UME** **FIA_SOS.1/UME**
OP.enableDisableUser -> User.isEnable Disable/enable user accounts	**FIA_ATD.1/UME**
OP.lockUnlockRole Lock/unlock roles	**FTA_SSL.3/UME**
OP.logReview Log review	**FAU_SAR.1/UME**

5.3.1.15 FDP_ACC.2/UME Complete access control

FDP_ACC.2.1 The TSF shall enforce the **Role-based Access Control Policy** on

- **Subjects:**
  - **S.UME-user**
- **Objects:**
  - **O.user;**

- **O.role;**
- **O.rule;**
- **O.setting.**

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

5.3.1.16 FDP_ACF.1/UME 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:**
  - **S.UME-user, with security attributes:**
    - **User.rolesList;**
    - **User.rule;**
    - **User.isLocked;**
    - **User.isEnable;**
- **Objects:**
  - **O.user;**
  - **O.role.**
  - **O.rule;**
  - **O.setting.**

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.UME-user is allowed to perform all operations defined in FMT_SMF.1.1/UME, if and only if the user is authenticated and his User.rolesList includes the value: Security Administrator;**
- **S.UME-user is allowed to perform OP.logReview, if the user is authenticated and his User.rolesList includes a role that has log view right.**

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:

- **S.UME-user is locked (User.isLocked is True);**
- **S.UME-user is not enabled (User.isEnable is False);**
- **S.UME-user has no role assigned (User.rolesList is empty);**
- **S.UME-user password has expired (current time >= User.rule.passwordExpirationDate);**
- **S.UME-user source IP is not allowed (not included in User.rule.allowedIPs);**
- **S.UME-user session has been terminated due to:**
  - **Inactivity (Setting.idleTimeout);**
  - **His role is being edited by a security administrator (User.rolesList).**
- **The operation is performed outside the allowed time schedule of S.UME-user (User.rule.allowedWorkSchedule);**
- **Role.type security administrator is locked.**

5.3.1.17 FMT_MSA.1/UME Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **UME Access Control Policy** to restrict the ability to **change_default and modify, delete** the security attributes:

- **Rule.passwordExpirationDate**
- **Rule.passwordHistoryNumber**
- **Rule.allowedIPs**
- **Rule.allowedWorkSchedule**
- **Rule.authenticationAttempts**
- **Rule.lockedPeriod**
- **Setting.idleTimeout**
- **User.username**
- **User.password**
- **User.passwordHistory**
- **User.rolesList**
- **User.rule**
- **User.isLocked**
- **User.isEnable**
- **Role.type**
- **Role.islocked**

to **Security Administrator**.

5.3.1.18 FMT_MSA.3/UME Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **UME 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 **Security Administrator** to specify alternative initial values to override the default values when an object or information is created.

5.3.2 Security Functional Requirements for the BBU

5.3.2.1 FIA_UID.2/BBU User identification before any action

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

5.3.2.2 FIA_UAU.2/BBU User authentication before any action

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

5.3.2.3 FIA_SOS.1/BBU Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that **User.password** meet:

- **The range of the password minimum length is 6~20, 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 (Rule.passwordHistoryNumber) passwords set in User.passwordHistory.**

5.3.2.4 FIA_AFL.1/BBU Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **an administrator configurable positive integer (User.Rule.authenticationAttempts) within 1 and 6 (default 6),** unsuccessful authentication attempts occur related to **S.BBU-user 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 (Rule.lockedPeriod) has passed, if the account has not been set to permanent locking.**

5.3.2.5 FTA_MCS.1/BBU 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 **S.BBU-user**.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of 5 sessions per user.

Application note: The maximum number of concurrent user session is 20.

5.3.2.6 FTA_SSL.3/BBU TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session **after a period of inactivity that equals the configured time (Setting.idleTimeout).**

5.3.2.7 FAU_GEN.1/BBU Audit data generation

FAU_GEN.1.1 The **BBU** 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:**
   - **S.BBU-user authentication (security log);**
   - **OP.lockUnlockUser (security log);**
   - **OP.userManagement (operation log);**
   - **OP.idleTimeout (operation log).**

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: 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.

5.3.2.8 FAU_STG.1/BBU Protected audit trail storage

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

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

5.3.2.9 FAU_STG.4/BBU Prevention of audit data loss

FAU_STG.4.1 The TSF shall **overwrite the oldest stored audit records**[3] if the audit trail is full.

Application note: Audit records can be exported to a backup server.

5.3.2.10 FTP_ITC.1/BBU-SEG Inter-TSF trusted channel

FTP_ITC.1.1 The **BBU** shall provide a communication channel between itself and **SEG** 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 **BBU** shall permit the **BBU and the SEG** to initiate communication via the trusted channel.

FTP_ITC.1.3 The **BBU** shall initiate communication via the trusted channel for **transmission of user data.**

5.3.2.11 FTP_ITC.1/BBU-BBU Inter-TSF trusted channel

FTP_ITC.1.1 The **BBU** shall provide a communication channel between itself and **another BBU** 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 **BBU** shall permit the **BBU and the other BBU** to initiate communication via the trusted channel.

FTP_ITC.1.3 The **BBU** shall initiate communication via the trusted channel for **transmission of user data.**

5.3.2.12 FTP_ITC.1/BBU-UE Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and **UE** that is logically distinct from other communication channels and provides

[3] The operation was completed to “take no other actions”, and this was subsequently refined away to make the sentence more readable.

assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit the **TSF and the UE** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **transmission of user data.**

Application note: This SFR is enforced by default by the BBU. However, the 3GPP specification [TS33-501] requires that the BBU allows non-encrypted connections from the UE.

5.3.2.13 FIA_ATD.1/BBU User attribute definition

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

- **User.username;**
- **User.password;**
- **User.rolesList;**
- **User.isLocked;**
- **User.isEnable;**
- **User.passwordHistory;**
- **User.rule.allowedIPs;**
- **User.rule.passwordHistoryNumber;**
- **User.rule.authenticationAttempts;**
- **User.Rule.lockedPeriod;**

5.3.2.14 FMT_SMR.1/BBU Security role

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.

5.3.2.15 FMT_SMF.1/BBU Specification of Management Functions

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

Management function	**Related to SFR**
OP.ruleManagement -> User.Rule.allowedIPs Set wether a user(assigned the rule) can only login from certain IP-addresses, and if so, which IP addresses.	**FDP_ACF.1/BBU**
OP.idleTimeout -> Setting.idleTimeout Set the time that users may remain logged in while inactive.	**FTA_SSL.3/BBU**
OP.ruleManagement -> User.Rule.passwordExpirationDate Set whether a user(assigned the rule) password expires after a certain time, and if so, after how long	**FDP_ACF.1/BBU**
OP.ruleManagement -> Rule.passwordHistoryNumber	**FIA_SOS.1/BBU**

Set the length password history that it is maintained to prevent the users from using the same password. E.g. if set to 3, then the users cannot use the last 3 passwords.	
OP.ruleManagement -> User.Rule.authenticationAttempts Set the number of allowed unsuccessful authentication attempts	**FIA_AFL.1/BBU**
OP.ruleManagement -> User.Rule.lockedPeriod Set the time that an account(assigned the rule) remains locked	**FIA_AFL.1/BBU**
OP.lockUnlockUser -> User.isLocked Unlock a user account	**FIA_AFL.1/BBU**
OP.userManagement Create, edit and delete user accounts	**FIA_ATD.1/BBU** **FIA_SOS.1/BBU**
OP.enableDisableUser Disable/enable user accounts	**FIA_ATD.1/BBU**
OP.userManagement -> User.rolesList Add or remove roles to/from users	**FMT_SMR.1/BBU**

5.3.2.16 FDP_ACC.2/BBU Complete access control

FDP_ACC.2.1 The TSF shall enforce the **BBU Access Control Policy** on:
Subjects:

- **S.BBU.**

Objects:

- **O.user;**
- **O.role;**
- **O.rule;**
- **O.Setting.**

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.

*5.3.2.17 **FDP_ACF.1/BBU 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:**
  - **S.BBU-user, with security attributes:**
    - **User.rolesList;**
    - **User.isLocked;**
    - **User.isEnable;**
    - **User.rule.passwordExpirationDate;**
    - **Role.type;**
- **Objects:**
  - **O.user;**
  - **O.role.**

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 is allowed to perform all operations defined in FMT_SMF.1.1/BBU if and only if the user is authenticated and his User.rolesList includes the value: Administrator;**

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:

- **S.BBU-user is locked (User.isLocked is True);**
- **S.BBU-user is not enabled (User.isEnable is False)**
- **S.BBU-user has no role assigned (User.rolesList is empty);**
- **S.BBU-user session has been terminated due to inactivity (Setting.idleTimeout);**
- **S.BBU-user source IP is not allowed (not included in User.rule.allowedIPs);**
- **S.BBU-user password has expired (current time >= User.rule.passwordExpirationDate);**
- **Role.type Administrator is locked.**

5.3.2.18 FMT_MSA.1/BBU Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **BBU Access Control Policy** to restrict the ability to **change_default and modify** the security attributes:

- **Rule.passwordExpirationDate**
- **Rule.passwordHistoryNumber**
- **Rule.allowedIPs**
- **Rule.authenticationAttempts**
- **Rule.lockedPeriod**
- **Setting.idleTimeout**
- **User.username**
- **User.password**
- **User.rolesList**
- **User.rule**
- **User.isLocked**
- **User.isEnable**
- **Role.type**
- **Role.islocked**

to **Administrator**.

5.3.2.19 FMT_MSA.3/BBU Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **BBU Access Control Policy** to provide **permissive** 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.

5.4 Security Assurance Requirements

The assurance requirements are EAL3+ 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.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.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.2	Vulnerability analysis

5.5 Security Assurance Requirements Rationale

The Security Assurance Requirements for this Security Target are EAL3+ALC_FLR.2. The reasons for this choice are that:

- EAL 3 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 both UME and BBU SFRs unless explicitly stated.

6.1 User identification and authentication

The TOE users are required to identify and authenticate themselves before they can perform any action using the TOE. 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. Users can be unlocked by the security administrator in the UME and by the administrator in the BBU. Users can also wait to be automatically unlocked after a period of time that is configurable by the security administrator in the UME and by the administrator in the BBU.

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;
- List of user roles;
- User rules, including expiration date, the length of password history, allowed IPs, allowed authentication time, number of authentication attempts and locked period;
- Locked and enabled status indicators.

User concurrent sessions are limited to a maximum 1 for each user in the UME, and 5 for each user of the BBU by default (with 20 as maximum configurable value). Furthermore, the sessions are automatically terminated after period of inactivity that is configurable by the security administrator in the UME and by the administrator in the BBU. A user session is also automatically terminated in the UME when the security administrator is editing the user roles.

User authentication can be restricted based on the user's source IP. The administrator can set an allowed IP (or set of IPs) so the user can only be successfully authenticated by connecting from the allowed IP. The UME security administrator can also restrict the time when a user can be authenticated in the UME by setting an allowed time period on the UME configuration.

User passwords have to meet certain rules to ensure that the passwords cannot be easily guessed or broken by brute force:

- (Only in the UME)At least 8 characters including four types: number, upper case letter, lower case letter, other characters;
- (Only in the BBU)The range of the password minimum length is 6~20, and the default recommended value is 12. including four types: number, upper case letter, lower case letter, other characters;

- (Only in the UME) Cannot be the same as the username, the username in reverse or a common password dictionary word;
- The new password cannot be the same as one of the last (Rule.passwordHistoryNumber) passwords set in User.passwordHistory.

Passwords that do not meet these rules are rejected by the TOE.

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

6.2 Access Control

The TOE enforces access control on users based on user roles. Each user role has an allowed set of allowed actions (including various management actions). A user can have more than one role, so the user access is the combination of all his roles.

The following table identify the allowed action for each role in the UME:

Role	Allowed actions
Security Administrator	Security management operations (as defined in FMT_SMF.1/UME) All user's log review.
Administrator	All(include all user's log review) operations except security management operations.
Maintenance	All (include self log review) except security management operations and system management operations.
Operator	Normal maintenance operations (include self log review) except security management operations.
Supervisor	View operations (include self log review) except security management operations.

The following table identify the allowed action for each role/group in the BBU:

Role/Group	Allowed actions
Administrator	Security management operations (as defined in FMT_SMF.1/BBU)
Maintenance	Read-only permission for security management node data, and read, write, and execute permissions for other node data
Ordinary	Have no read, write, or execute permission for security management node data, and have read-only permission for other nodes

Access control also verifies that user information is correct, such as that the user is enabled and not locked, user is not idle, user's IP is allowed, user's password is not expired and user's role is not locked. The access control on the UME also checks the user's allowed time interval and if the user's role is being edited by the security administrator.

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

6.3 Audit

The TOE generates audit logs to record the following events:

- User authentication;
- Locking or unlocking a user account;
- Enabling or disabling a user account (only UME);
- Add, remove or modify a user account;
- Add, remove or modify a role (only UME);
- Add, remove or modify a user's rule (only UME);
- When a user session is terminated by timeout;

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

The TOE provides the capability to review the logs to the security administrator of the UME.

The audit store is protected against manipulation. Log records cannot be edited and can only be deleted by the administrator of the UME and by the administrator of the BBU if the records are 30 days old or older.

The log records overwrite themselves when the log trail is full in the UME. Nonetheless, the records can be automatically sent to a remote server set on the UME's management network.

FAU_GEN.1, FAU_SAR.1, FAU_STG.1 and FAU_STG.4

6.4 Secure communication

The TOE provides secure interaction between its various parts and between itself and various machines in the environment, so that user data and/or management commands cannot be read or modified in between.

Communication between the UME and the UME Client is protected by HTTPS.

The connection between the BBU and SEG is protected by IPSEC.

The connection between the BBU and another BBU is protected by IPSEC.

The connection between the TOE and UE is protected by Encryption Algorithm.

Table security algorithms in different channels

Channel	Security Technology	Algorithms	Key Length
UME-UME Client	HTTPS	ECDHE-RSA-AES256-GCM-SHA384; DHE-RSA-AES256-GCM-SHA384; ECDHE-RSA-AES128-GCM-SHA256; DHE-RSA-AES128-GCM-SHA256.	
BBU-SEG&BBU-BBU	IPSEC	aes128cbc, aes192cbc, aes256-cbc, 3descbc,	Aes:128,192,256 3des:192
TOE-UE	Radio Security	NULL,Snow3G,AES,ZUC	128bits

FTP_ITC.1 and FTP_TRP.1

7 Rationales

7.1 Security Objectives Rationale

Assumptions/Threats	Objectives
T.COMMUNICATION_CH	This thread is directly covered by **O.SECURE_COMUNICATION** 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. The UME and the UME Client.
T.UNAUTHENTICATED_USER	This thread is directly covered by **O.USER_AUTHENTICATION** as it enforces user authentication on both BBU and UME components.
T.UNAUTHORIZED_ADMIN	This thread is directly covered by **O.USER_AUTHENTICATION** and **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** and **O.AUDITING** as these enforce user authentication and logging of user actions on the BBU and UME.
A.TIME	This assumption is upheld by **OE.TIME**, which directly covers the assumption.
A.UME_TRUSTED_NETWORK	This assumption is upheld by **OE.UME_TRUSTED_NETWORK**, which directly covers the assumption.
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.UME_PLATFORM	This assumption is upheld by **OE.UME_PLATFORM**, which directly covers the assumption.
A.UME_CLIENT	This assumption is upheld by **OE.UME_CLIENT**, which directly covers the assumption.

7.2 Security Functional Requirements Rationale

Security objectives	SFRs addressing the security objectives
O.SECURE_COMUNICATION	This objective is met by: • **FTP_TRP.1/UME-Client** for the secure communication between the UME and the client; • **FTP_ITC.1/BBU-SEG** for the secure communication between the BBU and the secure gateway; • **FTP_ITC.1/BBU-BBU** for the secure communication between the BBU and another BBU; • **FTP_ITC.1/BBU-UE** for the secure communication between the BBU and the UE.
O.USER_AUTHENTICATION	This objective is met by: • User identification and authentication before any action (**FIA_UID.2/UME, FIA_UID.2/BBU, FIA_UAU.2/UME** and **FIA_UAU.2/BBU**); • Limited user authentication attempts (**FIA_AFL.1/UME** and **FIA_AFL.1/BBU**); • Complex user password (**FIA_SOS.1/UME** and **FIA_SOS.1/BBU**); • Limitation of user session (**FTA_SSL.3/UME**, **FTA_SSL.3/BBU, FTA_MCS.1/UME** and **FTA_MCS.1/BBU**); • Supporting user configuration (**FMT_SMF.1/UME** and **FMT_SMF.1/BBU**).
O.ACCESS_CONTROL	This objective is met by: • User roles and attributes implementation (**FIA_ATD.1/UME, FIA_ATD.1/BBU, FMT_SMR.1/UME** and **FMT_SMR.1/UME**); • Enforcing access control based on user roles and attributes (**FDP_ACC.2/UME, FDP_ACC.2/BBU, FDP_ACF.1/UME, FDP_ACF.1/BBU, FMT_MSA.1/UME, FMT_MSA.1/BBU, FMT_MSA.3/UME** and **FMT_MSA.3/BBU**); • Supporting access control configuration (**FMT_SMF.1/UME** and **FMT_SMF.1/BBU**).
O.AUDITING	This objective is met by: • Audit data generation (**FAU_GEN.1/UME** and **FAU_GEN.1/BBU**); • Audit data protection (**FAU_STG.1/UME, FAU_STG.1/BBU, FAU_STG.4/UME, FAU_STG.4/BBU**); • Supporting audit data review (**FAU_SAR.1/UME,**

Security objectives	SFRs addressing the security objectives
	FMT_SMF.1/UME and **FMT_SMF.1/BBU**).

7.3 Dependencies

SFR	Dependency	Coverage
FIA_UID.2/UME	None.	None.
FIA_UAU.2/UME	FIA_UID.1	FIA_UID.2/UME
FIA_AFL.1/UME	FIA_UAU.1	FIA_UAU.1/UME
FIA_SOS.1/UME	None.	None.
FTA_SSL.3/UME	None.	None.
FTA_MCS.1/UME	FIA_UID.1	FIA_UID.2/UME
FAU_GEN.1/UME	FPT_STM.1	N/A See below
FAU_SAR.1/UME	FAU_GEN.1	FAU_GEN.1/UME
FAU_STG.1/UME	FAU_GEN.1	FAU_GEN.1/UME
FAU_STG.4/UME	FAU_GEN.1	FAU_GEN.1/UME
FTP_TRP.1/UME-Client	None.	None.
FIA_ATD.1/UME	None.	None.
FMT_SMF.1/UME	None.	None.
FMT_SMR.1/UME	FIA_UID.1	FIA_UID.2/UME
FDP_ACC.2/UME	FDP_ACF.1	FDP_ACF.1/UME
FDP_ACF.1/UME	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/UME FMT_MSA.3/UME
FMT_MSA.1/UME	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.2/UME FMT_SMR.1/UME FMT_SMF.1/UME
FMT_MSA.3/UME	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/UME FMT_SMR.1/UME
FIA_UID.2/BBU	FIA_UID.1	FIA_UID.2/BBU
FIA_UAU.2/BBU	FIA_UAU.1	FIA_UAU.1/BBU
FIA_SOS.1/BBU	None.	None.
FIA_AFL.1/BBU	FIA_UAU.1	FIA_UAU.1/BBU
FTA_MCS.1/BBU	FIA_UID.1	FIA_UID.2/BBU
FTA_SSL.3/BBU	None.	None.
FAU_GEN.1/BBU	FPT_STM.1	N/A See below
FAU_STG.1/BBU	FAU_GEN.1	FAU_GEN.1/BBU
FAU_STG.4/BBU	FAU_GEN.1	FAU_GEN.1/BBU
FTP_ITC.1/BBU-SEG	None.	None.
FTP_ITC.1/BBU-BBU	None.	None.
FTP_ITC.1/BBU-UE	None.	None.
FIA_ATD.1/BBU	None.	None.
FMT_SMF.1/BBU	None.	None.
FMT_SMR.1/BBU	FIA_UID.1	FIA_UID.2/BBU
FDP_ACC.2/BBU	FDP_ACF.1	FDP_ACF.1/BBU
FDP_ACF.1/BBU	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/BBU FMT_MSA.3/BBU
FMT_MSA.1/BBU	FDP_ACC.1	FDP_ACC.2/BBU

	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1/BBU FMT_SMF.1/BBU
FMT_MSA.3/BBU	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/BBU FMT_SMR.1/BBU

FPT_STM.1 cannot be implemented by the TOE because it does not have the capability to generate reliable time stamps, therefore the time information is provided by a NTP server in the TOE network (OE.TIME).

A 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
NTP	Network Time Protocol
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
SEG	Security gateway
UE	User Equipment
UMTS	Universal Mobile Telecommunications System

B 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