सत्यमेव जयते

Indian Telecom Security Assurance Requirements (ITSAR)

for

5G Aggregated gNB NSA Option-3,7&4

NCCS/ITSAR/Access Equipment/5G Access Equipment/5G Aggregated gNB NSA Option-3,7&4

(No. ITSAR303082306)

NCCS

Securing Networks

Release Date: 26.06.2023 Version: 1.0.0

Date of Enforcement:

Security Assurance Standards Facility (SASF) Division
National Centre for Communication Security (NCCS), Bengaluru
Department of Telecommunications
Ministry of Communications
Government of India

About NCCS

National Centre for communication Security (NCCS), with headquarters at Bengaluru was set up in 2018 with the objective to establish and operationalize a framework of security testing and certification within the country. Security Assurance Standards (SAS) division of NCCS is mandated to prepare Telecom security requirements/standards called Indian Telecom Security Assurance Requirements (ITSAR) that addresses the country specific security needs in telecommunication landscape and notify the same.

Document History

Sr. No.	Title	ITSAR No.	Version	Date of Release	Remark
1.	5G Aggregated gNB NSA Option-3,7&4	ITSAR303082306	1.0.0	26.06.2023	First release

Table of Contents

A) Outline:

The objective of this document is to present a comprehensive, country-specific security requirements for the aggregated gNB/en-gNB/ng-eNB – Network Elements of 5G RAN with Non Standalone option 3, 7 and 4 as defined by 3GPP.

The specifications produced by various regional/international standardization bodies/organizations/ associations like 3GPP, TSDSI along with the country-specific security requirements are the basis for this document.

This document commences with a brief description of 5G RAN with various deployment options, Core architecture and then proceeds to address the common security requirements and specific security requirements of gNB/en-gNB/ng-eNB.

B) Scope:

This document targets on the security requirements of the 5G RAN Network Elements i.e. aggregated gNB/en-gNB/ng-eNB with Non standalone option 3, 7 and 4 as defined by 3GPP.

C) Conventions:

1. Must or shall or required denotes the absolute requirement of a particular clause of ITSAR.
2. Must not or shall not denote absolute prohibition of a particular clause of ITSAR.
3. Should or Recommended denotes that the particular clause of ITSAR may be ignored under justifiable circumstances but after careful examination of its implications.
4. Should not or not Recommended denotes the opposite meaning of (3) above.

Chapter 1 – Overview

Introduction: The fifth generation of mobile technologies - 5G - is expected to connect people, things, data, applications, transport systems and cities in a smart networked communication environment. 5G is standardized by the third Generation Partnership Project (3GPP) and the requirement framework for 5G are specified by ITU under IMT-2020. The usage scenario/use cases identified for 5G are i) enhanced Mobile BroadBand (eMBB) ii) massive Machine Type Communication (mMTC) and iii) Ultra Reliable and Low Latency Communications (URLLC).

5G Architecture: The generic 5G System (5GS) architecture consists of User Equipment, Radio Access Network supporting New Radio (NR) and the cloud-native 5G core networks (5G-CN). 5G base station is called as Next Generation Node B (gNodeB).

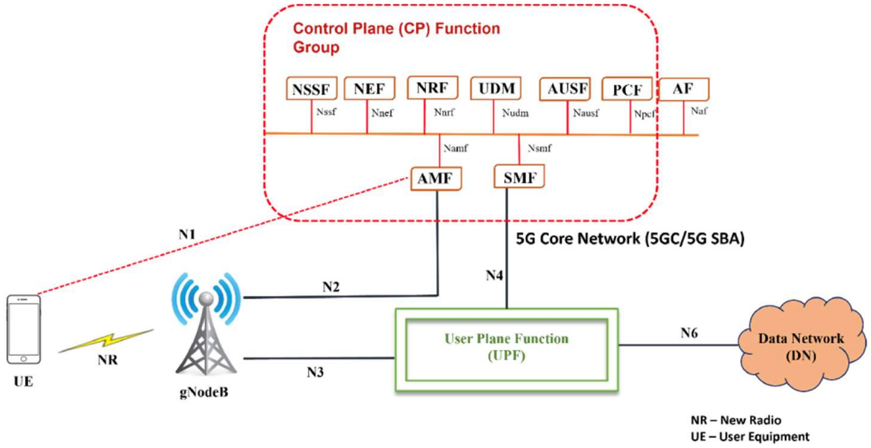

Figure 1: The 5G Generic Architecture

5G RAN Network: RAN (Radio Access Network) is the entry point to the core network for the UE. It handles radio resource allocation and management to UE through Uu interface and connects to Core network via AMF for control plane and UPF for data plane.

gNodeB: The gNB (gNodeB and its variants) in 5G (SA or NSA) network provides connectivity between user equipment (UE) and the core network (i.e. 5GC or EPC as the case may be).

The gNodeB is the functional equivalent of a base station in a traditional cellular network and is mainly responsible for radio communication with UEs in its coverage area/cell. It is also responsible for Radio resource management and control of mobility, connection, signalling and user plane security, QoS flows (an important 5G feature). It contains 3GPP-compliant of independent Network Functions, also referred to as NR RAN protocols namely: PHY, MAC, RLC, PDCP, RRC, SDAP.

5G Core Network: Core network is the central part of mobile network. 5G Core network provides authentication, security, mobility management, session management services and enables the subscribers to avail the services. These functionalities are specified as "network functions". Some of the important core network functions are 1) AMF 2) SMF 3) AuSF 4) UPF 5) AF 6) NEF 7) NRF 8) PCF 9) UDM 10) UDR, etc.

RAN elements and its naming conventions in 5G

The Node B in 5G can be categorized as follows

- gNB/ngNB (Generalised Node B or next-generation Node B) which connects to the 5GC with NG Interface and the UE through NR (New Radio) Uu interface.
- en-gNB (enhanced, generalized NodeB) a variant of the above which connects to the EPC (evolved packet core) through LTE/EUTRA and the UE through NR.
- ng-eNB (Existing LTE evolved NodeB upgraded to support NG Interface to connect to the 5G core and to the UE using LTE/EUTRA.

5G MR-DC, Deployment Options, and related migration paths

5G introduces a new connectivity mode, (viz) MR-DC (Multi Radio Dual Connectivity). The MR (Multi Radio) aspect of NG-RAN enables it to support multi (two) radio access mechanisms. The Dual connectivity (DC) aspect (as according to 3GPP) is a communication mode in which a user equipment (UE) is simultaneously connected to two base stations or nodes using two radio frequency (RF) interfaces. The 5G system allows DC within the native 5G network or relies on MR [Multi Radio] access technologies as defined in Release 16 3GPP 37.340 series

The deployment of 5G does not concomitantly require both the 5G core network (5GC) and the NG-RAN (Next-Generation Radio Access Network). This has led to different deployment options or migration paths towards fully evolved deployment of a 5G network. As a consequence of which, in 5G, network deployment has two models (viz.) SA (Standalone Access) and an NSA (Non-Standalone Access). The diagrams below depict various options possibilities and deployment migration possibilities.

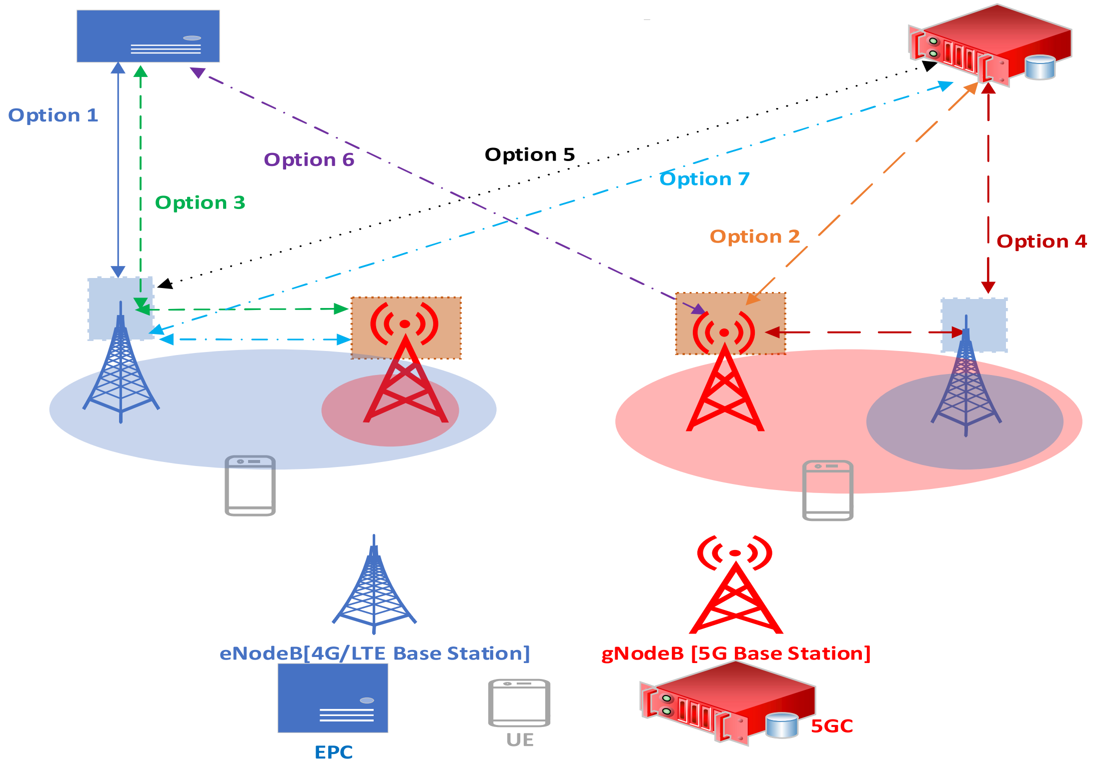

Figure 2: 5G Network System Options

5G RAN Option 2 (SA) Architecture: The '**option 2'** architecture is based upon a gNodeB connected to the 5G Core Network. The gNodeB uses the New Radio (NR) air interface and signalling protocols towards the end-user device. The gNodeB connects to an Access and Mobility Management Function (AMF) for control plane signalling with the 5G Core Network. The gNodeB connects to a User Plane Function (UPF) for the transfer of application data. The gNodeB are inter-connected using the Xn interface. This section also depicts various deployment options of 5G network such as option 3, 4, 7 and its variants.

The following figure illustrates Option 2 (SA) architecture:

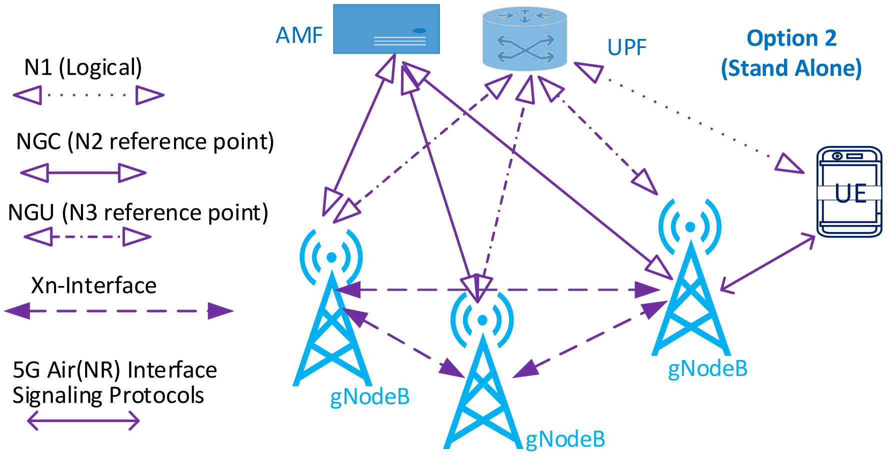

Figure 3: Option 2 Stand Alone Architecture

The following figure illustrates Option 3 (NSA) architecture:

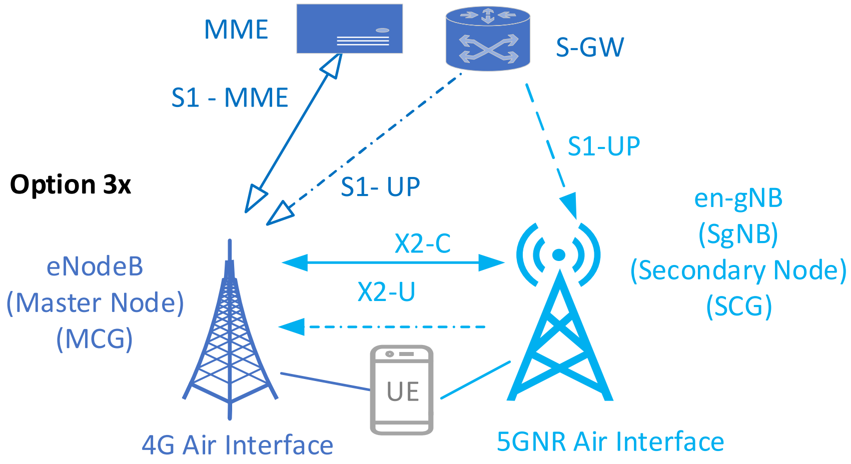

Figure 4: Option 3 Non-Standalone Architecture

The following figure illustrates Option 4 (NSA) architecture:

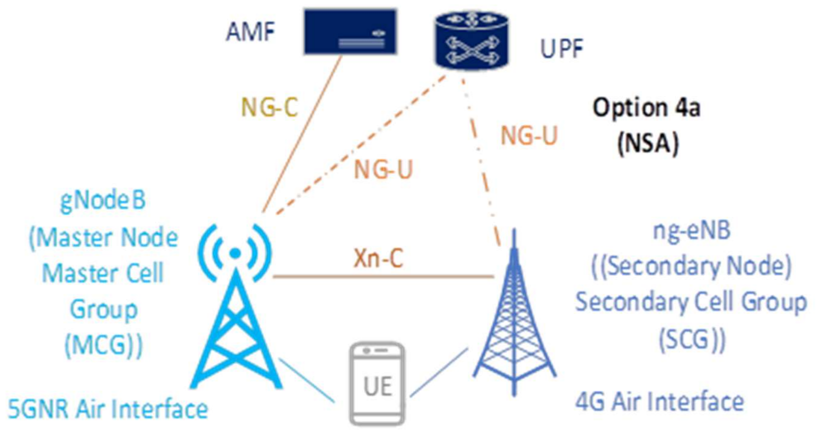

Figure 5: Option 4 Non-Standalone Architecture

The following figure illustrates Option 7 (NSA) architecture:

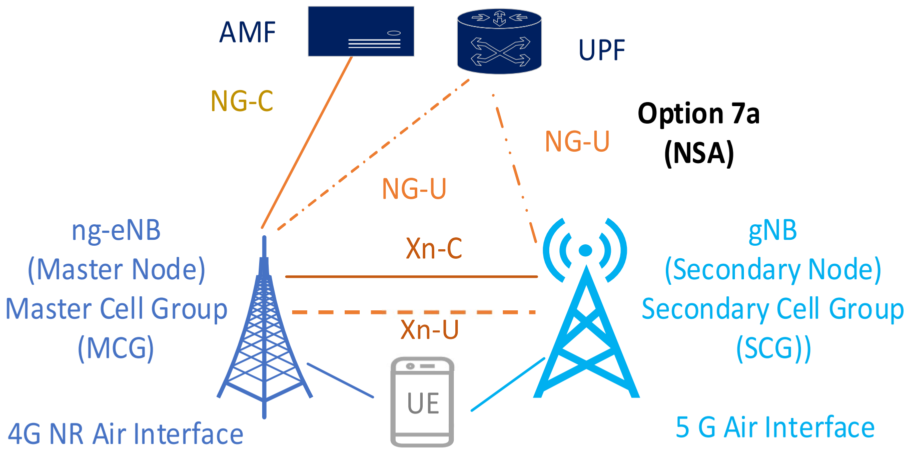

Figure 6: Option 7 Non-Standalone Architecture

The security requirements in this document are defined for various deployment options 3, 7 & 4. Each requirement described with applicable deployment options. Based on the options, gNB, en-gNB and ng-eNB are used interchangeably. Network configuration with respect to NodeBs are provided here for reference.

Option 3: ng-eNB is the master connected to 4GC. en-gNB act as a secondary node.

Option 7: ng-eNB is the master connected to 5GC. en-gNB act as a secondary node.

Option 4: gNB is the master connected to 5GC. ng-eNB act as a secondary node.

Chapter 2 – Common Security Requirements

Section 2.1: Access and Authorization

2.1.1 Management Protocols Mutual Authentication

Requirement:

The gNB/en-gNB/ng-eNB shall support mutual authentication mechanisms, the mutual authentication mechanism can rely on the protocol used for the interface itself or other means.

Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” shall only be used for gNB/en-gNB/ng-eNB management and maintenance.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.4.1]

2.1.2 Management Traffic Protection

Requirement:

gNB/en-gNB/ng-eNB management traffic shall be protected strictly using secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.4]

2.1.3 Role-based access control policy

Requirement:

gNB/en-gNB/ng-eNB shall support Role-Based Access Control (RBAC). A role-based access control system uses a set of controls that determines how users interact with domains and resources.

The RBAC system controls how users or groups of users are allowed access to the various domains and what type of operation they can perform, i.e., the specific operation command or command group (e.g., View, Modify, Execute). gNB/en-gNB/ng-eNB supports RBAC with minimum of 3 user roles, in particular, for OAM privilege management for gNB/en-gNB/ng-eNB Management and Maintenance, including authorization of the operation for configuration data and software via the network product console interface.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117- 16.7.0 V.1.0.0. Section 4.2.3.4.6.2]

2.1.4 User Authentication – Local/Remote

Requirement:

The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the username, enables unambiguous authentication and identification of the authorized user.

Authentication attributes include

- Cryptographic keys
- Token
- Passwords

This means that authentication based on a parameter that can be spoofed is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker.

Minimum two of the above Authentication attributes shall be mandatorily combined for protecting all the accounts from misuse in public network environment. An exception to this requirement is local access and machine accounts where at least one authentication attribute shall be supported.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.2.1]

2.1.5 Remote login restrictions for privileged users

Requirement:

Login to gNB/en-gNB/ng-eNB as root or equivalent highest privileged user shall be limited to the system console only. Root user shall not be allowed to login to gNB/en-gNB/ng-eNB remotely using any application/tool.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.6]

2.1.6 Authorization Policy

Requirement:

The authorizations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform.

Authorizations to a system shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Suitable authorizations shall also be assigned for access to files that are components of the operating system or of applications or that are generated by the same (e.g., configuration and logging files).

Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications should not be executed with administrator or system rights.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.6.1]

2.1.7 Unambiguous identification of the user & group accounts removal

Requirement:

Users shall be identified unambiguously by the gNB/en-gNB/ng-eNB.

gNB/en-gNB/ng-eNB shall support the assignment of individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system.

gNB/en-gNB/ng-eNB shall not enable the use of group accounts or group credentials or sharing of the same account between several users.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Sections 4.2.3.4.1.2]

Section 2.2: Authentication Attribute Management

2.2.1 Authentication Policy

Requirement:

The usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes (e.g., password, certificate) in public network environment shall be prevented. For machine accounts and local access one authentication attribute will be sufficient. System functions comprise, for example network services (like SSH, SFTP, Web services), local access via a management console, local usage of operating system and applications. This requirement shall also be applied to accounts that are only used for communication between systems.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.1.1]

2.2.2 Authentication Support – External

Requirement:

If the gNB/en-gNB/ng-eNB supports external authentication mechanism such as AAA server (for authentication, authorisation and accounting services), then the communication between gNB/en-gNB/ng-eNB and the external authentication entity shall be protected using the authentication and related service protocols built strictly using the Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only.

2.2.3 Protection against brute force and dictionary attacks

Requirement:

A protection against brute force and dictionary attacks that hinder authentication attribute guessing shall be implemented in gNB/en-gNB/ng-eNB.

Brute force and dictionary attacks aim to use automated guessing to ascertain authentication attribute for user and machine accounts.

Various measures or a combination of the following measures can be taken to prevent this:

(i) Using the timer delay (this delay could be the same or increased depending on the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").

(ii) Blocking an account following a specified number of incorrect attempts. However, it has to be taken into account that this solution needs a process for unlocking and an attacker can force this to deactivate accounts and make them unusable.

(iii) Using an authentication attribute blacklist to prevent vulnerable passwords.

(iv) Using CAPTCHA to prevent automated attempts (often used for Web applications).

In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by gNB/en-gNB/ng-eNB. An exception to this requirement is machine accounts.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.3]

2.2.4 Enforce Strong Password

Requirement:

(a) The configuration setting shall be such that a gNB/en-gNB/ng-eNB shall only accept passwords that comply with the following complexity criteria:

(i)Absolute minimum length of 8 characters (shorter lengths shall be rejected by the gNB/en-gNB/ng-eNB). It shall not be possible setting this absolute minimum length to a lower value by configuration.

(ii) Password shall mandatorily comprise all the following four categories of characters:

- at least 1 uppercase character (A-Z)
- at least 1 lowercase character (a-z)
- at least 1 digit (0-9)
- at least 1 special character (e.g., @;!$.)

b) The minimum length of characters in the passwords and the set of allowable special characters shall be configurable by the operator. The special characters may be categorized in sets according to their Unicode category.

c) If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this sub-clause.

d) If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the gNB.

e) When a user is changing a password or entering a new password, gNB/en-gNB/ng-eNB /central system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g., application-level, OS-level, etc.).

Password shall not be stored in clear text in the system; passwords shall be salted and hashed.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section 4.2.3.4.3.1]

2.2.5 Inactive Session timeout

Requirement:

An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period.

gNB/en-gNB/ng-eNB shall monitor inactive sessions of administrative login users and initiate session locking mechanism based on user configurable timers. Unlocking the session shall be permissible only by authentication. If the inactivity period further continues for a defined period, Session /user ID time out must occur after this inactivity.

The timer values can be admin configurable as per requirement, normally recommended to be between 2 to 5 minutes.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.5.2]

2.2.6 Password Changes

Requirement:

If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time. When an external centralized system for user authentication is used it should be possible to implement this function on this system.

Password change shall be enforced after initial login.

gNB/en-gNB/ng-eNB shall enforce password change based on password management policy.

In particular, the system shall enforce password expiry. gNB/en-gNB/ng-eNB shall support a configurable period for expiry of passwords.

Previously used passwords shall not be allowed up to a certain number (Password History).

The number of disallowed previously used passwords shall be:

- Configurable.
- Greater than 0.
- And its minimum value shall be 3. This means that the gNB/en-gNB/ng-eNB shall store at least the three previously set passwords. The maximum number of passwords that the gNB/en-gNB/ng-eNB can store for each user is up to the manufacturer.

When a password is about to expire, a password expiry notification shall be provided to the user.

Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.). An exception to this requirement is machine accounts.

gNB/en-gNB/ng-eNB to have in-built mechanism to support this requirement.

If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password change policies as laid down for the local system in this subclause.

And if a central system is not used for user authentication, the assurance on password changes rules shall be performed on the gNB/en-gNB/ng-eNB.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.2]

2.2.7 Protected Authentication feedback

Requirement:

The Authentication attribute shall not be displayed in such a way that it could be seen and misused by a casual local observer. Typically, the individual characters of the password are replaced by a character such as "*".

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.4]

2.2.8 Removal of predefined or default authentication attributes

Requirement:

Predefined or default authentication attributes shall be deleted or disabled.

Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, OEM or developer of a system. Such authentication attributes shall be changed by automatically forcing a user to change it on first time login to the system or the OEM provides instructions on how to manually change it.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.2.3]

2.2.9 Logout function

Requirement:

The system shall have a function that allows a signed-in user to logout at any time. All processes under the logged-in user ID shall be terminated on logout. The network product shall be able to continue to operate without interactive sessions.

Only for debugging purposes, processes under a logged-in user ID may be allowed to continue to run after detaching the interactive session.

An exception to this requirement is machine accounts.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.5.1]

2.2.10 Policy regarding consecutive failed login attempts

Requirement:

a) The maximum permissible number of consecutive failed user account login attempts should be configurable by the operator. The definition of the default value set at manufacturing time for the maximum number of failed user account login attempts shall be less than or equal to 8. After the maximum permissible number of consecutive failed user account login attempts is exceeded by a user, there shall be a block delay in allowing the user to attempt login again. This block delay and the capability to set the period of the block delay, e.g., double the delay, or 5 minutes delay, or 10 minutes delay, after each login failure should be configurable by the operator. The default value set at manufacturing time for this delay should be greater than or equal to 5 sec.

b) If supported, infinite (permanent) locking of an account that has exceeded the maximum permissible number of consecutive failed user account login attempts should also be possible via configuration, with the exception of administrative accounts, which shall get only temporarily locked.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117- 16.7.0 V.1.0.0. Section 4.2.3.4.5]

Section 2.3: Software Security

2.3.1 Secure Update

Requirement:

For software updates, gNB/en-gNB/ng-eNB shall support software package integrity validation via cryptographic means, e.g., digital signature, code signing certificate (valid and not time expired) and using Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only.

To this end, the gNB/en-gNB/ng-eNB has a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software update is originated from only these sources.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.5]

2.3.2 Secure Upgrade

Requirement:

(i) gNB/en-gNB/ng-eNB Software package integrity shall be validated in the installation /upgrade stage.

(ii) gNB/en-gNB/ng-eNB shall support software package integrity validation via cryptographic means, e.g., digital signature, code signing certificate (valid and not time expired), and using Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only. To this end, the gNB/en-gNB/ng-eNB has a list of public keys or certificates of authorized software sources and uses the keys to verify that the software update originated from only these sources.

(iii) Tampered software shall not be executed or installed if the integrity check fails.

(iv) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade and modify the list mentioned in (ii) above.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.5]

2.3.3 Source code security assurance

Requirement:

a) OEM shall follow best security practices including secure coding for software development. Source code shall be made available either at TSTL premises or at the mutually agreed location for source code review by the designated TSTL. It may be supported by furnishing the Software Test Document (STD).

b) Also, OEM shall submit the undertaking as below:

(i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the gNB/en-gNB/ng-eNB Software which includes OEM developed code, third party software and opensource code libraries used/embedded in the gNB/en-gNB/ng-eNB.

(ii) gNB/en-gNB/ng-eNB software shall be free from CWE top 25 and OWASP top10 security weaknesses on the date of offer of product to designated TTSL for testing. For other security weaknesses, OEM shall give mitigation plan.

(iii) The binaries for gNB/en-gNB/ng-eNB and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

2.3.4 Known Malware and backdoor Check

Requirement:

OEM shall submit an undertaking stating that gNB/en-gNB/ng-eNB is free from all known malware and backdoors as on the date of offer of gNB/en-gNB/ng-eNB to designated TSTL for testing and shall submit their internal Malware Test Document (MTD) of the gNB/en-gNB/ng-eNB to the designated TSTL.

2.3.5 No unused software

Requirement:

Software components or parts of software which are not needed for operation or functionality of the gNB/en-gNB/ng-eNB shall not be present.

Orphaned software components /packages shall not be present in gNB/en-gNB/ng-eNB.

OEM shall provide the list of software that are necessary for gNB/en-gNB/ng-eNB operation.

In addition, OEM shall furnish an undertaking as “gNB/en-gNB/ng-eNB does not contain Software that is not used in the functionality of gNB/en-gNB/ng-eNB”

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117 -16.7.0 V.1.0.0. Section 4.3.2.3]

2.3.6 Unnecessary Services Removal

Requirement:

gNB/en-gNB/ng-eNB shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. By default, all other ports and services will be permanently disabled. gNB/en-gNB/ng-eNB Shall not support following services

- FTP
- TFTP
- Telnet
- rlogin, RCP, RSH
- HTTP
- SNMPv1 and v2
- SSHv1
- TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- BOOTP server
- Discovery protocols (CDP, LLDP)
- IP Identification Service (Identd)
- PAD
- MOP

Any other protocols, services that are vulnerable are also to be permanently disabled.

Full documentation of required protocols and services (communication matrix) of the gNB/en-gNB/ng-eNB and their purpose needs to be provided by the OEM as prerequisite for the test case.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.1]

2.3.7 Restricting System Boot Source

Requirement:

The gNB/en-gNB/ng-eNB can boot only from the memory devices intended for this purpose.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section- 4.2.3.3.2]

2.3.8 Secure Time Synchronization

Requirement:

gNB/en-gNB/ng-eNB shall use reliable time and date information provided through NTP/PTP server. gNB/en-gNB/ng-eNB shall establish secure communication channel with the NTP/PTP server.

gNB/en-gNB/ng-eNB shall establish secure communication channel strictly using Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” with NTP/PTP server.

gNB/en-gNB/ng-eNB shall generate audit logs for all changes to time settings.

2.3.9 Restricted reachability of services

Requirement:

The gNB/en-gNB/ng-eNB shall restrict the reachability of services such that they can be reached only on interfaces meant for the purpose. On interfaces where services are active, the reachability should be limited to legitimate communication peers.

Administrative services (e.g. SSH, HTTPS, RDP) shall be restricted to interfaces in the management plane for separation of management traffic from user traffic.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section 4.3.2.2]

2.3.10 Self Testing

Requirement:
gNB/en-gNB/ng-eNB shall perform self-tests (integrity of the firmware and software as well as correct operation of cryptographic Module as per security requirement area of “self-test” of FIPS-140-3 or Later version, etc.) to identify failures in its security Mechanisms during i) power on ii) at the time of restart; and optionally when Administrator Instructs.

Section 2.4: System Secure Execution Environment

2.4.1 No unused functions

Requirement:

Unused functions i.e., the software and hardware functions which are not needed for operation or functionality of the gNB/en-gNB/ng-eNB shall be deactivated in the gNB/en-gNB/ng-eNB’s software and/or hardware.

The list of hardware and software functions installed in the system shall match with the ones that have been mentioned and deemed necessary for the operation of the gNB/en-gNB/ng-eNB.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.4]

2.4.2 No unsupported components

Requirement:

OEM to ensure that the gNB/en-gNB/ng-eNB shall not contain software and hardware components that are no longer supported by them or their third Parties including the opensource communities, such as components that have reached end-of-life or end-of-support. An undertaking in this regard shall be given by OEM.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.5]

2.4.3 Avoidance of Unspecified mode of Access

Requirement:

gNB/en-gNB/ng-eNB shall not contain any wireless access mechanism which is unspecified or not declared.

An undertaking shall be given by the OEM as follows:

“The gNB/en-gNB/ng-eNB does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel”

Section 2.5: User Audit

2.5.1 Audit trail storage and protection

Requirement:

The security event log shall be access controlled (file access rights) such that only privilege users including the administrator have access to read the log files. The only allowed operations on security event log are archiving/saving and viewing.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.3]

2.5.2 Audit Event Generation

Requirement:

The gNB/en-gNB/ng-eNB shall log all important Security events with unique System Reference details as given in the Table below.

gNB/en-gNB/ng-eNB shall record within each audit record at least information pertaining to Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

Additional audit record information, depending on the audit event, shall also be provided as given in the Table below:

Event Types (Mandatory or optional)	**Description**	**Event data to be logged**
Incorrect login attempts (Mandatory)	Records any user incorrect login attempts to the gNB/en-gNB/ng-eNB.	Username
		Source (IP address) if remote access
		Outcome of event (Success or failure)
		Timestamp
Administrator access (Mandatory)	Records any access attempts to accounts that have system privileges.	Username,
		Timestamp,
		Length of session

		Outcome of event (Success or failure)
		Source (IP address) if remote access
Account administration (Mandatory)	Records all account administration activity, i.e., configure, delete, copy, enable, and disable.	Administrator username,
		Administered account,
		Activity performed (configure, delete, enable and disable)
		Outcome of event (Success or failure)
		Timestamp
Resource Usage (Mandatory)	Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period have exceeded their defined thresholds.	Value exceeded,
		Value reached
		(Here suitable threshold values shall be defined depending on the individual system.)
		Outcome of event (Threshold Exceeded)
		Timestamp
Configuration change (Mandatory)	Changes to configuration of the network device	Change made
		Timestamp
		Outcome of event (Success or failure)
		Username
Reboot/shutdown/crash (Mandatory)	This event records any action on the network device/gNB/en-gNB/ng-eNB that forces a reboot or shutdown OR where the network device/gNB/en-gNB/ng-eNB has crashed.	Action performed (boot, reboot, shutdown, etc.)
		Username (for intentional actions)
		Outcome of event (Success or failure)
		Timestamp
Interface status change (Mandatory)	Change to the status of interfaces on the network device/gNB/en-gNB/ng-eNB (e.g., shutdown)	Interface name and type
		Status (shutdown, down missing link, etc.)
		Outcome of event (Success or failure)
		Timestamp
Change of group membership or accounts (Optional)	Any change of group membership for accounts	Administrator username,
		Administered account,
		Activity performed (group added or removed)
		Outcome of event (Success or failure)
		Timestamp.
		Administrator username

Resetting Passwords (Optional)	Resetting of user account passwords by the Administrator	Administered account
		Activity performed (configure, delete, enable and disable)
		Outcome of event (Success or failure)
		Timestamp
Services (Optional)	Starting and Stopping of Services (if applicable)	Service identity
		Activity performed (start, stop, etc.)
		Timestamp
		Outcome of event (Success or failure)
X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
		Reason for failure
		Subject identity
		Type of event
Secure Update (Optional)	Attempt to initiate manual update, initiation of update, completion of update	User identity
		Timestamp
		Outcome of event (Success or failure)
		Activity performed
Time change (Mandatory)	Change in time settings	Old value of time
		New value of time
		Timestamp
		origin of attempt to change time (e.g., IP address)
		Subject identity
		Outcome of event (Success or failure)
		User identity
Session unlocking/ termination (Optional)	Any attempts at unlocking of an interactive session, termination of a remote session by the session locking mechanism, termination of an interactive session.	User identity (wherever applicable)
		Timestamp
		Outcome of event (Success or failure)
		Subject identity
		Activity performed
		Type of event
Trusted Communication paths with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorised remote administrators (Optional)	Initiation, Termination and Failure of trusted Communication paths	Timestamp
		Initiator identity (as applicable)
		Target identity (as applicable)
		User identity (in case of Remote administrator access)
		Type of event
		Outcome of event (Success or failure, as applicable)

Audit data changes (Optional)	Changes to audit data including deletion of audit data	Timestamp
		Type of event (audit data deletion, audit data modification)
		Outcome of event (Success or failure)
		Subject identity
		User identity
		origin of attempt to change time (e.g., IP address)
		Details of data deleted or modified
User Login (Mandatory)	All use of Identification and authentication mechanisms.	User identity
		Origin of attempt
		(IP address)
		Outcome of event (Success or failure)
		Timestamp

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.1]

2.5.3 Secure Log Export

Requirement:

(i) (a) The gNB/en-gNB/ng-eNB shall support forwarding of security event logging data to an external system by push or pull mechanism.

(b) Log functions should support secure uploading of log files to a central location or to a system external for the gNB/en-gNB/ng-eNB.

(ii) gNB/en-gNB/ng-eNB shall be able to store the generated audit data itself may be with limitations.

(iii) gNB/en-gNB/ng-eNB shall alert administrator when its security log buffer reaches configured threshold limit.

(iv) In the absence of external system (due to loss of connectivity or due to node failure or due to any other reasons), gNB/en-gNB/ng-eNB shall have mechanism to store audit data locally. gNB/en-gNB/ng-eNB shall have sufficient memory to store at least five days logs allocated for this purpose. OEM shall submit justification document for sufficiency of local storage requirement.

(v) Secure Log export shall comply the secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.2]

Section 2.6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirements:

gNB/en-gNB/ng-eNB shall Communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only.

OEM shall submit to TSTL, the list of the connected entities with gNB/en-gNB/ng-eNB and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration, detailed procedure of establishing the communication with each entity and any other details required for verifying this requirement.

2.6.2 Cryptographic Module Security Assurance

Requirement:

Cryptographic module embedded inside the gNB/en-gNB/ng-eNB (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with Level 2 of FIPS 140-3 or later as prescribed by NIST standards.

Till further instructions, this clause will be considered ‘complied’ by submission of an undertaking by the OEM in specified format along with self-certified test reports.

An undertaking is to be submitted by the OEM mentioning that “Cryptographic module embedded inside the gNB/en-gNB/ng-eNB (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with Level 2 of FIPS 140-3 or later as prescribed by NIST standards”.

OEM shall also submit cryptographic module testing document and the detailed self / Lab test report along with test results for scrutiny.

2.6.3 Cryptographic Algorithms implementation Security Assurance

Requirement:

Cryptographic algorithm implemented inside the Crypto module of gNB/en-gNB/ng-eNB shall be in compliance with the respective FIPS standards (for the specific crypto algorithm).

Till further instructions, this clause will be considered ‘complied’ by submission of an undertaking by the OEM in specified format along with self-certified test reports.

An undertaking is to be submitted by the OEM mentioning that “Cryptographic algorithm implemented inside the Crypto module of gNB/en-gNB/ng-eNB is in compliance with the respective FIPS standards (for the specific crypto algorithm embedded inside the gNB)”

OEM shall submit cryptographic algorithm implementation testing document and the detailed self / Lab test report along with test results for scrutiny.

2.6.4 Protecting data and information – Confidential System Internal Data

Requirement:

a) When gNB/en-gNB/ng-eNB is in normal operational mode (i.e., not in maintenance mode) there shall be no system function that reveals confidential system internal data in the clear text to users and administrators.
b) Access to maintenance mode shall be restricted only to authorised privileged user.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.2]

2.6.5 Protecting data and information in storage

Requirement:

a) For sensitive data (persistent or temporary) in storage, read access rights shall be restricted. Sensitive files of gNB/en-gNB/ng-eNB system that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" with appropriate non-repudiation controls.
b) In addition, the following rules apply for:
   (i) Systems that need access to identification and authentication data in the clear/readable form e.g., in order to perform an activity/operation. Such systems shall not store this data in the clear/readable form, but scramble or encrypt it by implementation-specific means.
   (ii) Systems that do not need access to sensitive data in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.
   (iii) Stored files in the gNB/en-gNB/ng-eNB: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section 4.2.3.2.3]

2.6.6 Protection against Copy of Data

Requirement:

a) Without authentication, gNB/en-gNB/ng-eNB shall not create a copy of data in use or data in transit.
b) Protective measures should exist against use of available system functions / software residing in gNB/en-gNB/ng-eNB to create copy of data for illegal transmission.
   The software functions, components in the gNB/en-gNB/ng-eNB for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement**:**

a) gNB/en-gNB/ng-eNB shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.
b) Establishment of outbound overt channels such as, HTTPS, IM, P2P, Email etc. are to be forbidden if they are auto-initiated by / auto-originated from the gNB/en-gNB/ng-eNB.

Session logs shall be generated for establishment of any session initiated by either user or gNB/en-gNB/ng-eNB.

2.6.8 Protection against Data Exfiltration - Covert Channel

Requirement:

a) gNB/en-gNB/ng-eNB shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.
b) Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc. are to be forbidden if they are auto-initiated by / auto-originated from the gNB/en-gNB/ng-eNB.
c) Session logs shall be generated for establishment of any session initiated by either user or gNB/en-gNB/ng-eNB system.

Section 2.7: Network Services

2.7.1 Traffic Filtering – Network Level Requirement

gNB/en-gNB/ng-eNB shall provide a mechanism to filter incoming IP packets on any IP interface.
In particular the gNB/en-gNB/ng-eNB shall provide a mechanism:

(i) To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of the stack ISO/OSI.
(ii) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:
  - Discard/Drop: the matching message is discarded; no subsequent rules are applied, and no answer is sent back.
  - Accept: the matching message is accepted.
  - Account: the matching message is accounted for i.e., a counter for the rule is incremented. This action can be combined with the previous ones.

  This feature is useful to monitor traffic before its blocking.
(iii) To enable/disable for each rule the logging for Dropped packets, i.e., details on messages matching the rule for troubleshooting.
(iv) To filter on the basis of the value(s) of source IP, destination IP and port addresses of protocol header.
(v) To reset the accounting.

(vi) The gNB/en-gNB/ng-eNB shall provide a mechanism to disable/enable each defined rule.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section 4.2.6.2.1]

2.7.2 Traffic Separation

Requirement:

The gNB/en-gNB/ng-eNB shall support the physical or logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains. See RFC 3871 for further information.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.5.1]

2.7.3 Traffic Protection –Anti-Spoofing

Requirement:

gNB/en-gNB/ng-eNB shall not process IP Packets if their source address is not reachable via the incoming interface. Implementation example: Use of "Reverse Path Filter" (RPF) provides this function.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.3.1.1]

2.7.4 GTP-U Filtering

Requirement:

The following capability is conditionally required:

- For each message of a GTP-U-based protocol, it shall be possible to check whether the sender of this message is authorized to send a message pertaining to this protocol.
- At least the following actions should be supported when the check is satisfied:
- Discard: the matching message is discarded.
- Accept: the matching message is accepted.
- Account: the matching message is accounted for, i.e., a counter for the rule is incremented.

This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.

This requirement is conditional in the following sense: It is required that at least one of the following two statements holds:

- gNB/en-gNB/ng-eNB supports the capability described above, and this is stated in the product documentation.

- The gNB's product documentation states that the capability is not supported and that the gNB/en-gNB/ng-eNB needs to be deployed together with a separate entity which provides the capability described above.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.6.2.4]

Section 2.8: Attack Prevention Mechanisms

2.8.1 Network Level and application-level DDoS

Requirement:

gNB/en-gNB/ng-eNB shall have protection mechanism against Network level and Application-level DDoS attacks.

gNB/en-gNB/ng-eNB shall provide security measures to deal with overload situations which may occur as a result of a denial-of-service attack or during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided.

Potential protective measures include but not limited to the following:

- Restricting of available RAM per application
- Restricting of maximum sessions for a Web application
- Defining the maximum size of a dataset
- Restricting CPU resources per process
- Prioritizing processes
- Limiting of amount or size of transactions of a user or from an IP address in a specific time range
- Limiting of amount or size of transactions to an IP address/Port Address in a specific time range

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.1]

2.8.2 Excessive Overload Protection

Requirement:

gNB/en-gNB/ng-eNB shall act in a predictable way if an overload situation cannot be prevented. gNB/en-gNB/ng-eNB shall be built in this way that it can react on an overload situation in a controlled way.

However, it is possible that a situation happens where the security measures are no longer sufficient. In such case it shall be ensured that gNB/en-gNB/ng-eNB cannot reach an undefined and thus potentially insecure, state.

OEM shall provide a technical description of the gNB/en-gNB/ng-eNB's Overload Control mechanisms (especially whether these mechanisms rely on cooperation of other network elements e.g., RAN)

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.3]

2.8.3 Manipulated packets that are sent to an address of the network device shall not lead to an impairment of availability

Requirement:

gNB/en-gNB/ng-eNB shall not be affected in its availability or robustness by incoming packets from other network elements that are manipulated or differing the norm. This means that appropriate packets shall be detected as invalid and be discarded. The process shall not be affecting the performance of the gNB/en-gNB/ng-eNB. This robustness shall be just as effective for a great mass of invalid packets as for individual or a small number of packets.

Examples of such packets are:

- Mass-produced TCP packets with a set SYN flag to produce half-open TCP connections (SYN flooding attack).
- Packets with the same IP sender address and IP recipient address (Land attack).
- Mass-produced ICMP packets with the broadcast address of a network as target address (Smurf attack).
- Fragmented IP packets with overlapping offset fields (Teardrop attack).
- ICMP packets that are larger than the maximum permitted size (65,535 Bytes) of IPv4 packets (Ping-of-death attack).
- Uncorrelated reply to packets (i.e., packets which cannot be correlated to any request).

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.6.2.2]

Section 2.9: Vulnerability Testing Requirements

2.9.1 Fuzzing – Network and Application Level

Requirement:

It shall be ensured that externally reachable services of gNB/en-gNB/ng-eNB are reasonably robust when receiving unexpected input.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 section 4.4.4]

2.9.2 Port Scanning

Requirement:

It shall be ensured that on all network interfaces of gNB/en-gNB/ng-eNB, only documented ports on the transport layer respond to requests from outside the system.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.4.2]

2.9.3 Vulnerability Scanning

Requirement:

The vulnerabilities found during the Vulnerability Scanning/Assessment process shall be remediated as below. For other than critical vulnerabilities, OEM shall provide remediation.

Sl. No.	CVSS Score	Severity	Remediation
1	9.0 – 10.0	Critical	To be patched immediately
2	7.0 – 8.9	High	To be patched within a month
3	4.0 – 6.9	Medium	To be patched within 3 months
4	0.1 – 3.9	Low	To be patched within a year

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 section 4.4.3]

Section 2.10: Operating System

2.10.1 Growing Content Handling

Requirement:

a) Growing or dynamic content shall not influence system functions.

b) A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop gNB/en-gNB/ng-eNB from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.1.1]

2.10.2 Handling of ICMP

Requirement:

Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the gNB/en-gNB/ng-eNB.

gNB/en-gNB/ng-eNB shall not send certain ICMP types by default but it may support the option to enable utilization of these types which are marked as "Optional" in below table:

Type (IPv4)	Type (IPv6)	Description	Send	Respond to
0	128	Echo Reply	Permitted (optional for ng-eNB)	N/A
3	1	Destination Unreachable	Permitted	N/A
8	129	Echo Request	Permitted	Optional
11	3	Time Exceeded	Optional	N/A
12	4	Parameter Problem	Permitted	N/A
N/A	2	Packet too Big	Permitted	N/A
N/A	135	Neighbor Solicitation	Permitted	Permitted
N/A	136	Neighbor Advertisement	Permitted	N/A

gNB/en-gNB/ng-eNB shall not respond to, or process (i.e., do changes to configuration) under any circumstances certain ICMP message types as marked in the below table.

Type (IPv4)	Type (IPv6)	Description	Send	Respond to	Process (i.e., do changes to configuration)
5	137	Redirect	N/A	N/A	Not Permitted
13	N/A	Timestamp	N/A	Not Permitted	N/A
14	N/A	Timestamp Reply	Not Permitted (i.e., as automatic reply to "Timestamp")	N/A	N/A
N/A	133	Router Solicitation	N/A	Not Permitted	Not Permitted
N/A	134	Router Advertisement	N/A	N/A	Permitted (optional for ng-eNB)

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.1.2]

2.10.3 Authenticated Privilege Escalation only

Requirement:

gNB/en-gNB/ng-eNB shall not support a privilege escalation method in interactive sessions (both CLI and GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.2.1]

2.10.4 System account identification

Requirement:

Each system account in gNB/en-gNB/ng-eNB shall have a unique identification with appropriate non-repudiation controls.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.2.2]

2.10.5 OS Hardening - Minimized kernel network functions

Requirement:

Kernel-based network functions not needed for the operation of the network element shall be deactivated. In particular, the following ones shall be disabled by default:

1. IP Packet Forwarding between different interfaces of the network product.

   (Note: The above text does not preclude that IP Packet Forwarding can be enabled in certain deployment scenarios.)
2. Proxy ARP
3. Directed broadcast
4. IPv4 Multicast handling
5. Gratuitous ARP messages

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section - 4.3.3.1.2]

2.10.6 No automatic launch of removable media

Requirement:

gNB/en-gNB/ng-eNB shall not automatically launch any application when a removable media device is connected.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.3]

2.10.7 Protection from buffer overflows

Requirement:

gNB/en-gNB/ng-eNB shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided by OEM.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section - 4.3.3.1.5]

2.10.8 External file system mount restrictions

Requirement:

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in gNB/en-gNB/ng-eNB in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

OS-level restrictions shall apply to normal users against mount / use of removable media devices (e.g., USB drive, CD ROM etc.) for data transfer.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section - 4.3.3.1.6]

2.10.9 File-system Authorization privileges

Requirement:

gNB/en-gNB/ng-eNB shall be designed to ensure that only users that are authorized to modify files, data, directories or file systems have the necessary privileges to do so.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section - 4.3.2.7]

2.10.10 SYN Flood Prevention

Requirement:

gNB/en-gNB/ng-eNB shall support a mechanism to prevent Syn Flood attacks. This feature shall be enabled by default.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.4]

2.10.11 Handling of IP options and extensions

Requirement:

IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g., source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.2.4.1.1.3]

2.10.12 Restrictions on running Scripts / Batch-processes

Requirement:

Scheduled tasks for carrying out the activities such as taking the backups, monitoring disk space and system maintenance activities shall be executed by the privileged user such as administrator only. Similarly, gNB/en-gNB/ng-eNB shall have feature to restrict Scripts / Batch-processes / Macros usage among various users. It shall be possible to administratively configure scheduled tasks usage i.e. Cron-Job usage (permit / deny) among various users like Normal users, privileged users.

2.10.13 Restrictions on Soft-Restart

Requirement:

gNB/en-gNB/ng-eNB shall restrict software-based system restart options usage among various users. The software reset / restart either through command or use of key-combinations like CTRL+ALT+DEL is not available to normal users for prevention of unintended / malicious trigger of system reset / restart.

Section 2.11: Web Servers

This entire section of the security requirements is applicable if the gNB/en-gNB/ng-eNB supports **web management interface.**

2.11.1 HTTPS

Requirement:

The communication between Web client and Web server shall be protected strictly using the Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” only

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.1]

2.11.2 Webserver logging

Requirement:

Access to the gNB/en-gNB/ng-eNB webserver (for both successful as well as failed attempts) shall be logged by gNB/en-gNB/ng-eNB.

The web server log shall contain the following information:

- Access timestamp
- Source (IP address)
- Account (if known)
- Attempted login name (if the associated account does not exist)
- Relevant fields in http request. The URL should be included whenever possible.
- Status code of web server response

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.2]

2.11.3 HTTPS input validation

Requirement:

The gNB/en-gNB/ng-eNB shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.

gNB/en-gNB/ng-eNB shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.4]

2.11.4 No system privileges

Requirement:

No gNB/en-gNB/ng-eNB web server processes shall run with system privileges.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.2]

2.11.5 No unused HTTPS methods

Requirement:

HTTPS methods that are not required for gNB/en-gNB/ng-eNB operation shall be deactivated.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 section 4.3.4.3]

2.11.6 No unused add-ons

Requirement:

All optional add-ons and components of the web server shall be deactivated if they are not required for gNB/en-gNB/ng-eNB operation.

In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.4]

2.11.7 No compiler, interpreter, or shell via CGI or other server-side scripting

Requirement:

If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory or other corresponding scripting directory shall not include compilers or interpreters.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.5]

2.11.8 No CGI or other scripting for uploads

Requirement:

If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.6]

2.11.9 No execution of system commands with SSI

Requirement:

If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.7]

2.11.10 Access rights for web server configuration

Requirement:

Access rights for gNB/en-gNB/ng-eNB web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 section 4.3.4.8]

2.11.11 No default content

Requirement:

Default content that is provided with the standard installation of the gNB/en-gNB/ng-eNB web server shall be removed.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.9]

2.11.12 No directory listings

Requirement:

Directory listings (indexing) / "Directory browsing" shall be deactivated.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.10]

2.11.13 Web server information in HTTPS headers

Requirement:

The HTTPS header shall not include information on the version of the gNB/en-gNB/ng-eNB web server and the modules/add-ons used.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.11]

2.11.14 Web server information in error pages

Requirement:

User-defined error pages and Error messages shall not include version information and other internal information about the gNB/en-gNB/ng-eNB web server, and the modules/add-ons used.

Default error pages of the gNB/en-gNB/ng-eNB web server shall be replaced by error pages defined by the OEM.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.12]

2.11.15 Minimized file type mappings

Requirement:

File type or script-mappings that are not required for gNB/en-gNB/ng-eNB operation shall be deleted.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.13]

2.11.16 Restricted file access

Requirement:

Restrictive access rights shall be assigned to all files which are directly or indirectly reside in the gNB/en-gNB/ng-eNB web server's document directory.

In particular, the gNB/en-gNB/ng-eNB web server shall not be able to access files which are not meant to be delivered.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 section 4.3.4.14]

2.11.17 Execute rights exclusive for CGI/Scripting directory

Requirement:

If CGI or other scripting technology is used, only the CGI/Scripting directory is configured with execute rights. Other directories used or meant for web content do not have execute rights.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.15]

2.11.18 HTTP User session

Requirement:

To protect user sessions, gNB/en-gNB/ng-eNB shall support the following session ID and session cookie requirements:

1. The session ID shall uniquely identify the user and distinguish the session from all other active sessions.

2.The session ID shall be unpredictable.

3.The session ID shall not contain sensitive information in clear text (e.g., account number, social security, etc.).

4.In addition to the Session Idle Timeout, gNB/en-gNB/ng-eNB shall automatically terminate sessions after a configurable maximum lifetime. This maximum lifetime defines the maximum session span. When the maximum lifetime expires, the session shall be closed, the session ID shall be deleted, and the user shall be forced to (re)authenticate in the web application and to establish a new session. The default value for this maximum lifetime shall be set to 8 hours.

5.Session IDs shall be regenerated for each new session (e.g., each time a user logs in).

6.The session ID shall not be reused or renewed in subsequent sessions.

7.The gNB/en-gNB/ng-eNB shall not use persistent cookies to manage sessions but only session cookies. This means that neither the "expire" nor the "max-age" attribute shall be set in the cookies.

8.Where session cookies are used the attribute 'HTTP Only' shall be set to true.

9.Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.

10.Where session cookies are used the 'path' attribute shall be set to ensure that the cookie can only be sent to the specified directory or sub-directory.

11.The gNB/en-gNB/ng-eNB shall not accept session identifiers from GET/POST variables.

12.The gNB/en-gNB/ng-eNB shall be configured to only accept server generated session ID.

[Reference: TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.3]

Section 2.12: Other Security requirements

2.12.1 No System Password Recovery

Requirement:

No provision shall exist for gNB/en-gNB/ng-eNB System / Root password recovery.

2.12.2 Secure System Software Revocation

Requirement:

Once the gNB/en-gNB/ng-eNB software image is legally updated/upgraded with New Software Image, it should not be possible to roll back to a previous software image.

In case roll back is essential, it shall be done only by the administrator with appropriate audit trail log created.

gNB/en-gNB/ng-eNB shall support a well-established control mechanism for rolling back to previous software image.

2.12.3 Software Integrity Check –Installation

Requirement:

gNB/en-gNB/ng-eNB shall validate the software package integrity before the installation/upgrade stage strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

Tampered software shall not be executed or installed if integrity check fails.

2.12.4 Software Integrity Check – Boot

Requirement:

The gNB/en-gNB/ng-eNB shall verify the integrity of a software component by comparing the result of a measurement of the component, typically a standard cryptographic hash generated strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" to the expected reference value.

2.12.5 Unused Physical and Logical Interfaces Disabling

Requirement:

gNB/en-gNB/ng-eNB shall support the mechanism to verify both the physical and logical interfaces exist in the product.

Physical and logical accessible interfaces (except console interface) which are not under use shall be disabled so that they remain inactive even in the event of reboot.

2.12.6 No Default Profile

Requirement:

Predefined or default user accounts (other than Admin/Root) in gNB/en-gNB/ng-eNB shall be deleted or disabled.

Chapter 3: Specific Security Requirements – Option 3 (NR NodeB)

3.1 Integrity protection of RRC-signalling

Requirement:

The en-gNB shall support integrity protection of RRC-signalling over the NG RAN air interface.

[Reference: TEC 25875:2022 - TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

3.2 Integrity protection of user plane data between the en-gNB and the UE

Requirement:

The en-gNB shall support integrity protection of user plane data packets over the NG RAN air interface through eNB.

[Reference: TEC 25875:2022 - TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

3.3 RRC integrity check failure

Requirement:

The RRC integrity checks shall be performed both in the ME and the en-gNB. In case failed integrity check (i.e., faulty or missing MAC-I) is detected after the start of integrity protection, the concerned message shall be discarded. This can happen on the en-gNB side or on the ME side.

[Reference: TEC 25875:2022 - TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section 7.4 and E3.10.1]

3.4 UP integrity check failure

Requirement:

The User Plane integrity check shall be performed both in UE and en-gNB. If the en-gNB or the UE receives a PDCP PDU which fails integrity check with faulty or missing MAC-I after the start of integrity protection, the PDU shall be discarded.

[Reference: TEC 25875:2022 - TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section 7.3 and E3.10.1]

3.5 Ciphering of RRC-signalling

Requirement:

The en-gNB shall support standard ciphering of RRC-signalling over the NG RAN air interface.

Secure cryptographic controls prescribed for AES in Table 1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” or SNOW3G-128 or ZUC-128 shall be used for gNB management and maintenance.

[Reference: TEC 25875:2022 - TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

3.6 Ciphering of user plane data between the en-gNB and the UE

Requirement:

The en-gNB shall provide standard ciphering of user plane data packets between the en-gNB and the UE on NG RAN air interface.

Secure cryptographic controls prescribed for AES in Table 1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” or SNOW3G-128 or ZUC-128 shall be used for en-gNB management and maintenance.

[Reference: TEC 25875:2022 - TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

3.7 Replay protection of user plane data between the en-gNB and the UE

Requirement:

The gNB shall support replay protection of user plane data between the gNB and the UE.

[Reference: TEC 25875:2022 - TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E1.3 and E3.10.1]

3.8 Replay protection of RRC-signalling

Requirement:

The gNB shall support integrity protection and replay protection of RRC-signalling.

[Reference: TEC 25875:2022 - TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E1.3 and E3.10.1]

3.9 Key refresh at the en-gNB [Sen-gNB]

Requirement:

The UE and MeNB shall derive the security key S-KgNB of the target Sen-gNB. KSgNB-UP-enc, KSgNB-RRC-int and KSgNB-RRC-enc are derived from the S-KgNB both at the Sen-gNB side and the UE side.

[Reference: TEC 25875:2022 - TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.4.2]

3.10 AS protection algorithm selection in Dual Connectivity

Requirement:

"When establishing one or more DRBs and/or an SRB for a UE at the Sen-gNB, the MeNB shall send the UE NR security capabilities associated with the UE in the Sen-gNB Addition/Modification procedure. Upon receipt of this message, the Sen-gNB shall identify the needed algorithm(s) with highest priority in the locally configured priority list of algorithms that is also present in the received UE NR security capabilities and include an indicator for the locally identified algorithm(s) in Sen-gNB Addition/Modification Request Acknowledge.

The MeNB shall forward the indication to the UE during the RRCConnectionReconfiguration procedure that establishes the Sen-gNB terminated DRBs and/or SRB in the UE. The UE shall use the indicated encryption algorithms for the Sen-gNB terminated DRBs and/or SRB and the indicated integrity algorithm for the Sen-gNB terminated SRB."

[Reference: TEC 25875:2022 - TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.4.3]

3.11 Key update at the en-gNB on dual connectivity

Requirement:

If the MeNB receives a request for S-KgNB update from the Sen-gNB or decides on its own to perform S-KgNB update, the eNB shall compute a fresh S-KgNB and increment the SCG Counter. Then the MeNB shall perform a Sen-gNB Modification procedure to deliver the fresh S-KgNB to the Sen-gNB. The MeNB shall provide the value of the SCG Counter used in the derivation of the S-KgNB to the UE in an integrity protected RRC procedure. The UE shall derive the S-KgNB. Whenever the UE or Sen-gNB start using a fresh S-KgNB, they shall re-calculate KSgNB-UP-enc, KSgNB-RRC-int and KSgNB-RRC-enc from the fresh S-KgNB.

[Reference: TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.5.2]

3.12 Key update at the en-gNB on dual connectivity when PDCP counter is about to wrap around

Requirement:

The en-gNB shall request the MeNB to update the S-KgNB over the X2-C interface when uplink or downlink PDCP counts are about to wrap around.

[Reference: TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.5.1]

3.13 Control plane data protection over X2-C interface

Requirement:

The transport of control plane data over X2-C interface (between eNB and en-gNB) shall be confidentiality, integrity and replay protected.

[Reference: TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E1.3 and E3.10.1]

3.14 User plane data protection over X2-U interface

Requirement:

The transport of user plane data over X2-U interface (between eNB and en-gNB) shall be confidentiality, integrity and replay protected.

[Reference: TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E1.3 and E3.10.1]

3.15 Bidding down prevention in X2 handover

Requirement:

During X2 handover, the DRB connection between UE and en-gNB/eNB shall be released and the AS security context and en-gNB and UE shall be deleted.

[Reference: TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.6**]**

Chapter 4: Specific Security Requirements – Option 7 (NR NodeB)

4.1 Integrity protection of RRC-signalling

Requirement:

The gNB shall support integrity protection of RRC-signalling over the NG RAN air interface.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.1, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.3, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

4.2 Integrity protection of user plane data between the gNB and the UE

Requirement:

The gNB shall support integrity protection of user plane data packets over the NG RAN air interface.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.2, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.3, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

4.3 RRC integrity check failure

Requirement:

The RRC integrity checks shall be performed both in the ME and the gNB. In case failed integrity check (i.e., faulty or missing MAC-I) is detected after the start of integrity protection, the concerned message shall be discarded. This can happen on the gNB side or on the ME side.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.4, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 6.5.1, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

4.4 UP integrity check failure

Requirement:

The User Plane integrity check shall be performed both in UE and gNB. If the gNB or the UE receives a PDCP PDU which fails integrity check with faulty or missing MAC-I after the start of integrity protection, the PDU shall be discarded.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.5, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 6.6.4, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

4.5 Ciphering of RRC-signalling

Requirement:

"The gNB shall support standard ciphering of RRC-signalling over the NG RAN air interface.

Secure cryptographic controls prescribed for AES in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" or SNOW3G-128 or ZUC-128 shall be used for gNB management and maintenance."

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.6, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.2, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

4.6 Ciphering of user plane data between the gNB and the UE

Requirement:

"The gNB shall provide standard ciphering of user plane data packets between the gNB and the UE on NG RAN air interface.

Secure cryptographic controls prescribed for AES in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" or SNOW3G-128 or ZUC-128 shall be used for gNB management and maintenance."

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.7, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.2, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

4.7 Replay protection of user plane data between the gNB and the UE

Requirement:

The gNB shall support replay protection of user plane data between the gNB and the UE.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.8, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.3, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

4.8 Replay protection of RRC-signalling

Requirement:

The gNB shall support integrity protection and replay protection of RRC-signalling.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.9, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.3, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

4.9 Ciphering of user plane data based on the security policy sent by the SMF

Requirement:

The gNB shall activate ciphering of user plane data based on the security policy sent by the SMF.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.10, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 5.3.2]

4.10 Integrity of user plane data based on the security policy sent by the SMF

Requirement:

The gNB shall provide integrity protection of user plane data based on the security policy sent by the SMF.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 section 4.2.2.1.11, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 5.3.2]

4.11 Key refresh at the gNB [SgNB]

Requirement:

The UE and Mng-eNB shall derive the security key S-KgNB of the target Sen-gNB. KSgNB-UP-enc, KSgNB-RRC-int and KSgNB-RRC-enc are derived from the S-KgNB both at the SgNB side and the UE side.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.13, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 6.9.4.1, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.4.2]

4.12 Bidding down prevention in Xn-handovers

Requirement:

During Xn handover the DRB connection between UE and gNB shall be released and the AS security context at gNB and UE shall be deleted.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.14, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 6.7.3.1, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.6]

4.13 AS protection algorithm selection in SgNB change

Requirement:

"When establishing one or more DRBs and/or an SRB for a UE at the SgNB, the Mng-eNB shall send the UE NR security capabilities associated with the UE in the SgNB Addition/Modification procedure. Upon receipt of this message, the SgNB shall identify the needed algorithm(s) with highest priority in the locally configured priority list of algorithms that is also present in the received UE NR security capabilities and include an indicator for the locally identified algorithm(s) in SgNB Addition/Modification Request Acknowledge.

The Mng-eNB shall forward the indication to the UE during the RRCConnectionReconfiguration procedure that establishes the SgNB terminated DRBs and/or SRB in the UE. The UE shall use the indicated encryption algorithms for the SgNB terminated DRBs and/or SRB and the indicated integrity algorithm for the SgNB terminated SRB."

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.15, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 6.7.3.1 & 6.7.3.2, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.4.3]

4.14 Control plane data & User plane data protection over Xn interface

Requirement:

The transport of control plane data and user plane data over Xn shall be confidentiality, integrity & replay protected.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.17, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 Sections 9.4, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

4.15 Key update at the SgNB on dual connectivity

Requirement:

If the Mng-eNB receives a request for S-KgNB update from the SgNB or decides on its own to perform S-KgNB update, the ng-eNB shall compute a fresh S-KgNB and increment the SCG Counter. Then the Mng-eNB shall perform a SgNB Modification procedure to deliver the fresh S-KgNB to the SgNB. The Mng-eNB shall provide the value of the SCG Counter used in the derivation of the S-KgNB to the UE in an integrity protected RRC procedure. The UE shall derive the S-KgNB. Whenever the UE or SgNB start using a fresh S-KgNB, they shall re-calculate KSgNB-UP-enc, KSgNB-RRC-int and KSgNB-RRC-enc from the fresh S-KgNB.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.18, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 Sections 6.10.2.1, 6.10.2.2.1, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.5.2]

4.16 Key update at the SgNB on dual connectivity when PDCP counter is about to wrap around

Requirement:

The SgNB shall request the Mng-eNB to update the S-KgNB over the X2-C interface when uplink or downlink PDCP counts are about to wrap around.

[Reference: TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.5.1]

Chapter 5: Specific Security Requirements – Option 4 (NR NodeB)

5.1 Integrity protection of RRC-signalling

Requirement:

The gNB shall support integrity protection of RRC-signalling over the NG RAN air interface.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.1, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.3, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

5.2 Integrity protection of user plane data between the gNB and the UE

Requirement:

The gNB shall support integrity protection of user plane data packets over the NG RAN air interface.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.2, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.3, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

5.3 RRC integrity check failure

Requirement:

The RRC integrity checks shall be performed both in the ME and the gNB. In case failed integrity check (i.e., faulty or missing MAC-I) is detected after the start of integrity protection, the concerned message shall be discarded. This can happen on the gNB side or on the ME side.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.4, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 6.5.1, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

5.4 UP integrity check failure

Requirement:

The User Plane integrity check shall be performed both in UE and gNB. If the gNB or the UE receives a PDCP PDU which fails integrity check with faulty or missing MAC-I after the start of integrity protection, the PDU shall be discarded.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.5, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 6.6.4, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

5.5 Ciphering of RRC-signalling

Requirement:

The gNB shall support standard ciphering of RRC-signalling over the NG RAN air interface.

Secure cryptographic controls prescribed for AES in Table 1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” or SNOW3G-128 or ZUC-128 shall be used for gNB management and maintenance.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.6, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.2, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

5.6 Ciphering of user plane data between the gNB and the UE

Requirement:

The gNB shall provide standard ciphering of user plane data packets between the gNB and the UE on NG RAN air interface.

Secure cryptographic controls prescribed for AES in Table 1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” or SNOW3G-128 or ZUC-128 shall be used for gNB management and maintenance.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.7, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.2, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

5.7 Replay protection of user plane data between the gNB and the UE

Requirement:

The gNB shall support replay protection of user plane data between the gNB and the UE.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.8, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.3, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

5.8 Replay protection of RRC-signalling

Requirement:

The gNB shall support integrity protection and replay protection of RRC-signalling.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.9, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.3, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

5.9 Ciphering of user plane data based on the security policy sent by the SMF

Requirement:

The gNB shall activate ciphering of user plane data based on the security policy sent by the SMF.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.10, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 5.3.2]

5.10 Integrity of user plane data based on the security policy sent by the SMF

Requirement:

The gNB shall provide integrity protection of user plane data based on the security policy sent by the SMF.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 section 4.2.2.1.11, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 5.3.2]

5.11 Access Stratum (AS) algorithms selection

Requirement:

The serving network shall select the algorithms to use dependent on the UE security capabilities of the UE, the configured allowed list of security capabilities of the currently serving network entity.

“Each gNB shall be configured via network management with lists of algorithms which are allowed for usage. There shall be one list for integrity algorithms, and one for ciphering algorithms. These lists shall be ordered according to a priority decided by the operator.”

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.12, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 5.11.2]

5.12 Key refresh at the gNB

Requirement:

Key refresh shall be possible for K_{gNB}, $K_{RRC-enc}$, $K_{RRC-int}$, K_{UP-int}, and K_{UP-enc} and shall be initiated by the gNB when a PDCP COUNTs are about to be re-used with the same Radio Bearer identity and with the same K_{gNB}.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.13, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 6.9.4.1, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.4.2]

5.13 Bidding down prevention in Xn-handovers

Requirement:

In the Path-Switch message, the target gNB shall send the UE's 5G security capabilities, UP security policy with corresponding PDU session ID received from the source gNB to the AMF.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.14, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 6.7.3.1, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.6]

5.14 AS protection algorithm selection in gNB change

Requirement:

The target gNB shall select the algorithm with highest priority from the UE's 5G security capabilities according to the locally configured prioritized list of algorithms (this applies for both integrity and ciphering algorithms). The chosen algorithms shall be indicated to the UE in the Handover Command message if the target gNB selects different algorithms compared to the source gNB.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.15, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 6.7.3.1 & 6.7.3.2, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.4.3]

5.15 Control plane data protection over N2 interface

Requirement:

The transport of control plane data over N2 shall be confidentiality, integrity & replay protected.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0. section 4.2.2.1.16, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 Sections 9.2]

5.16 Control plane data & User plane data protection over Xn interface

Requirement:

The transport of control plane data and user plane data over Xn shall be confidentiality, integrity & replay protected.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.17, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 Sections 9.4, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.10.1]

5.17 Key update at the gNB on dual connectivity

Requirement:

When executing the procedure for adding subsequent radio bearer(s) to the same SN (Secondary Node i.e. ng-eNB), the MN (Master Node i.e. gNB) shall, for each new radio bearer, assign a radio bearer identity that has not previously been used since the last K_{SN} change. If the MN cannot allocate an unused radio bearer identity for a new radio bearer in the SN, due to radio bearer identity space exhaustion, the MN shall increment the SN Counter and compute a fresh K_{SN}, and then shall perform a SN Modification procedure to update the K_{SN}.

The SN shall request the Master Node to update the K_{SN} over the Xn-C, when uplink and/or downlink PDCP COUNTs are about to wrap around for any of the SCG DRBs or SCG SRB.

[Reference: TEC 25879:2022 – TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.18, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 Sections 6.10.2.1, 6.10.2.2.1, TEC 25875:2022 – TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.5.2]

5.18 UP security activation in Inactive scenario

Requirement:

If the UP-security activation status can be supported in the target gNB, the target gNB shall use the UP-security activations that the UE used at the last source cell. Otherwise, the target gNB shall respond with an RRC Setup message to establish a new RRC connection with the UE.

[Reference: 3GPP TS 33.511 17.3.0 V1.0.0 section 4.2.2.1.19, TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 6.8.2.1.3]

5.19 Key update at the gNB on dual connectivity when SN counter is about to wrap around

Requirement:

The MN shall refresh the root key of the 5G AS security context associated with the SN Counter before the SN Counter wraps around. When the root key is refreshed, the SN Counter is reset to '0'.

[Reference: TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 6.10.3.1]

5.20 User plane data protection over N3 interface

Requirement:

(i) The transport of user plane data over N3 shall be integrity protected.
(ii) The transport of user plane data over N3 shall be confidentiality protected.
(iii) The transport of user plane data over N3 shall be replay protected.

[Reference: TEC 25878:2022 – TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 9.3]

Annexure-I (Definition)

1. Aggregated gNB means monolithic gNB (NR Node B) which contains DU & CU together.
2. Confidential System Internal Data: it may contain authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e. stack traces in error messages). Such functions could be local or remote OAM CLI/GUI, logging messages, alarms, configuration file exports, etc.
3. DDoS: A distributed denial-of-service attack that renders the victim un-usable by the external environment.
4. Downlink: Unidirectional radio link for the transmission of signals from a RAN access point to a UE. Also, in general the direction from Network to UE.
5. eNodeB: a Base station which connects UE to 4G Core Network.
6. en-gNB: evolved next generation gNB which connects to 5G Core network and 4G core network and eNB in case of dual connectivity.
7. gNodeB: an NR Base Station which connects UE to 5G Core Network.
8. Medium Access Control: A sub-layer of radio interface layer 2 providing unacknowledged data transfer service on logical channels and access to transport channels.
9. Mobility: The ability for the user to communicate whilst moving independent of location.
10. Network Element: A discrete telecommunications entity which can be managed over a specific interface e.g., the gNB.
11. ng-eNB: a base station which connects UE to 4G core network and 5G Core network and gNB in case of dual connectivity.
12. NG-RAN: It is the radio access network introduced for accessing 5G.
13. NG-U interface: New generation user plane interface between eNB and 5G Core network
14. Non-Access Stratum: Protocols between UE and the core network that are not terminated in the RAN.
15. Original Equipment Manufacturer (OEM): manufacturer of communication and its related products under whose brand, the products are sold or proposed to be sold to operators in the country.
16. Protocol: A formal set of procedures that are adopted to ensure communication between two or more functions within the same layer of a hierarchy of functions.
17. Radio link: A “radio link” is a logical association between single User Equipment and a single RAN access point. Its physical realization comprises one or more radio bearer transmissions.
18. Radio Resource Control: A sublayer of radio interface Layer 3 existing in the control plane only which provides information transfer service to the non-access stratum. RRC is responsible for controlling the configuration of radio interface Layers 1 and 2.

19. Remote Access: The access which is not Local access. This includes access from the EMS (Element Management System) network, and access that originates or passes through the internet.
20. RRC Connection: A point-to-point bi-directional connection between RRC peer entities on the UE and the UTRAN sides, respectively. A UE has either zero or one RRC connection.
21. Security: The ability to prevent fraud as well as the protection of information availability, integrity, and confidentiality.
22. Sensitive data: data that may be used for authentication or may help to identify the user, such as user names, passwords, PINs, cryptographic keys, IMSIs, IMEIs, MSISDNs, or IP addresses of the UE, as well as files of a system that are needed for the functionality such as firmware images, patches, drivers or kernel modules.
23. Transmission or Transport is the transfer of information from one entity (transmitter) to another (receiver) via a communication path.
24. Uplink: An “uplink” is a unidirectional radio link for the transmission of signals from a UE to a base station.
25. User Equipment: A device allowing a user access to network services. The interface between the UE and the network is the radio interface. A User Equipment can be subdivided into a number of domains, the domains being separated by reference points.

Annexure-II (Acronyms)

5GC	-	5G Core Network
5GS	-	5G System
AAA	-	Authentication, Authorization and Accounting
AES	-	Advanced Encryption Standards
ARP	-	Address Resolution Protocol/Allocation and Retention Priority
AS	-	Access Stratum
AuSF	-	Authentication Server Function
CLI	-	Command Line Interface
CP	-	Control Plane
DC	-	Dual Connectivity
DDoS	-	Distributed Denial of Service
DL	-	Downlink
DN	-	Data Network
DRB	-	Data Radio Bearer
DTLS	-	Datagram Transport Layer Security
EPC	-	Evolved Packet Core
EPS	-	Evolved Packet System
eNB	-	Evolved Node B (Fourth Generation Base Station)
en-gNB	-	Enhanced 5G Next Generation Base station
gNB	-	5G Next Generation base station
GTP	-	GPRS Tunnelling Protocol
GTP-C	-	GPRS Tunnelling Protocol Control Plane
GTP-U	-	GPRS Tunnelling Protocol User Plane
GUI	-	Graphical User Interface
HTTP	-	Hypertext Transfer Protocol
HTTPS	-	Hypertext Transfer Protocol Secure
ICMP	-	Internet Control Message Protocol
IMS	-	IP Multimedia Subsystem
IP	-	Internet Protocol

ISO-OSI	-	International organization of Standardization – Open System Interconnection
MAC-I	-	Message Authentication Code - Integrity
ME	-	Mobile Equipment
MN	-	Master Node
MeNB	-	Master eNB
Mng-eNB	-	Master ng-eNB
MR	-	Multi Radio
NAS	-	Non-Access Stratum
NEF	-	Network Exposure Function
NF	-	Network Function
NG	-	Next Generation
ng-eNB	-	Next Generation e-NodeB
NG-RAN	-	Next Generation Radio Access Network
NRF	-	Network Repository Function
O&M	-	Operations and Maintenance
OAM	-	Operations, Administration, Maintenance
OS	-	Operating System
PCF	-	Policy Control Function
PDCP	-	Packet Data Convergence Protocol
PDU	-	Protocol Data Unit
PLMN	-	Public Land Mobile Network
QoS	-	Quality of Service
RAM	-	Random Access Memory
RAN	-	Radio Access Network
RAT	-	Radio Access Technology
RFC	-	Request For Comments
RRC	-	Radio Resource Control
SCG	-	Secondary Cell Group
Sen-gNB	-	Secondary en-gNB

SgNB	-	Secondary gNB
SMF	-	Session Management Function
SN	-	Secondary Node
SRB	-	Signalling Radio Bearer
TSTL	-	Telecom Security Testing Laboratory
UDM	-	Unified Data Management
UDR	-	Unified Data Repository
UE	-	User Equipment
UL	-	Uplink
UP	-	User Plane
UPF	-	User Plane Function
URL	-	Uniform Resource Locator
URLLC	-	Ultra Reliable Low Latency Communication
WLAN	-	Wireless Local Area Network

Annexure-III (List of Submissions)

1. Source Code Security Assurance (against test case 2.3.3)
2. Known Malware and backdoor Check (against test case 2.3.4)
3. No unused Software (against test case 2.3.5)
4. Unnecessary Services Removal (against test case 2.3.6)
5. No Unused Functions (against test case 2.4.1)
6. Avoidance of Unspecified mode of Access (against test case 2.4.3)
7. Cryptographic Based Secure Communication (against test case 2.6.1)
8. Cryptographic Module Security Assurance (against test case2.6.2)
9. Cryptographic Algorithms implementation Security Assurance (against test case 2.6.3)

Annexure-IV (References)

1. TEC 25848:2022 - TEC 25848:2022 - TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0: “Catalogue of General Security Assurance Requirements”.
2. TEC 25879:2022 - TSDSI STD T1.3GPP 33.511-16.7.0 V.1.0.0 “Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class”.
3. TEC 25878:2022 - TSDSI STD T1.3GPP 33.501-16.9.0 V.1.0.0 Security architecture and procedures for 5G System”.
4. TEC 25875:2022 - TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 3GPP System Architecture Evolution (SAE); Security architecture

---End of Document---