Indian Telecom Security Assurance Requirements (ITSAR)

भारतीय दूरसंचार सुरक्षा आश्वासन आवश्यकताएँ (भा.दू.सु.आ.आ.)

5G Disaggregated RAN gNodeB (CU, DU & RU)

Draft For Comments (DFC)

ITSAR Number: ITSAR3030924MM
ITSAR Name: NCCS/ITSAR/Access Equipment/5G Access Equipment/5G Disaggregated RAN gNodeB CU-DU-RU

Date of Release: DD.MM.YYYY
Date of Enforcement:

Version: 1.0.0

MTCTE के तहत जारी:
Issued under MTCTE by:

राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)
दूरसंचार विभाग, संचार मंत्रालय
भारत सरकार
सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत

National Centre for Communication Security (NCCS)
Department of Telecommunications
Ministry of Communications
Government of India
City Telephone Exchange, SR Nagar, Bangalore-560027, 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

Sl. No.	Title	ITSAR No.	Version	Date of release	Remarks
1	5G Disaggregated RAN gNodeB (CU, DU & RU)	ITSAR3030924MM	1.0.0	DD.MM.YYYY	First release

Table of Contents

A) Outline

A gNodeB (gNB) is a network element of 5G RAN as defined by 3GPP. Provisioning of a gNB can be either disaggregated or aggregated based on the split functionalities as specified by 3GPP. The objective of this document is to present a comprehensive, country-specific security requirements for a deployment of disaggregated gNB resulting from exercising the suggested and supported functional split options for a gNB (NR Node B) as specified in 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 various functional split options of 5G RAN with emphasis on 3GPP recommended, supported option and then proceeds to address the common security requirements and specific security requirements of disaggregated gNB.

B) Scope

This document targets on the security requirements of the 5G RAN Network Element i.e., dis-aggregated gNB's CU, DU and RU component as defined and explicitly supported by 3GPP. The requirements specified here are binding on network equipment providers OEMs (Original Equipment Manufacturer).

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 clause of ITSAR may be ignored under justifiable circumstances but after careful examination of its implications.
4. Should not or not Recommended denotes that that clause of ITSAR may not be ignored under justifiable circumstances but after careful examination of its implications.
5. gNB shall be referred to as disaggregated gNB wherever applicable.
6. In the case of CSR, the requirements applied to CU, DU and RU unless otherwise stated.
7. The following section may not be applicable to RU or will be adopted as per the OEM guidelines as RU is FPGA based hardware cum software than a conventional server or network products.
    a. Section 2.2.3 (iv), 2.2.7
    b. Section 2.5
    c. Section 2.7.4
    d. Section 2.10.2, 2.10.10
    e. Section 2.11

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 3rd 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).

The 5G deployment scenarios are better understood by a closer study of high-level RAN architectures and network topologies supported by 5G. Disaggregation of the base stations and separation of the control plane (CP) and user plane (UP) entities are the basic design principles of 5G RAN architecture. The basis of this could be tied to the evolving concepts of C-RAN (Cloud RAN). Numerous architectural and deployment schemes that were introduced during the evolution targeting improving the spectral efficiency, latency, and support of advanced interference mitigation techniques. These aspects were studied and trialled by the leading operators. One of the outcomes of this study trials was demarcation of the BBU (Base band unit) into a CU (Central Unit) and DU (Distributed Unit). The aggregated and disaggregated RAN architecture is shown below as per the 3GPP TS 38.401 standard. The scope of the requirements is limited to option 7.2 split as per the 3GPP standards.

In case of option 7.2 split option as per the 3GPP TR 38.816 from Release 15 [20], the RF and the low phy are part of the RU. Upper Phy to RLC is part of the DU and PDCP to RRC in case of control plane, PDCP to SDAP in case of user plane are part of the CU.

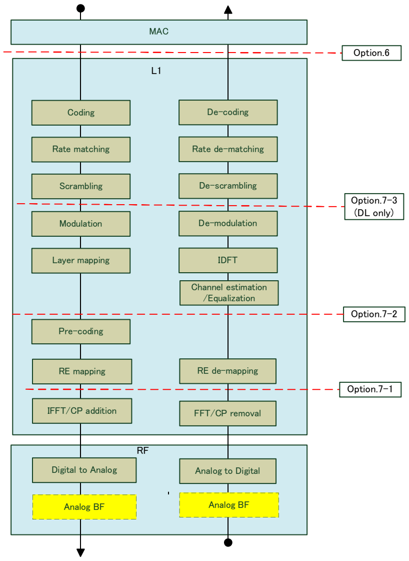

Figure 1: Disaggregated RAN SW Architecture

The transport to connect functional units has a range of names within the industry, such as fronthaul, midhaul, backhaul, x-haul et., The usage of these terms is not consistent among groups and individuals in the industry, so can lead to confusion. Next Generation Mobile Network (NGMN) defines the interfaces of the disaggregated RAN as below figure as per the specification NGMN overview on 5G RAN Functional Decomposition clause 2.2 [10]

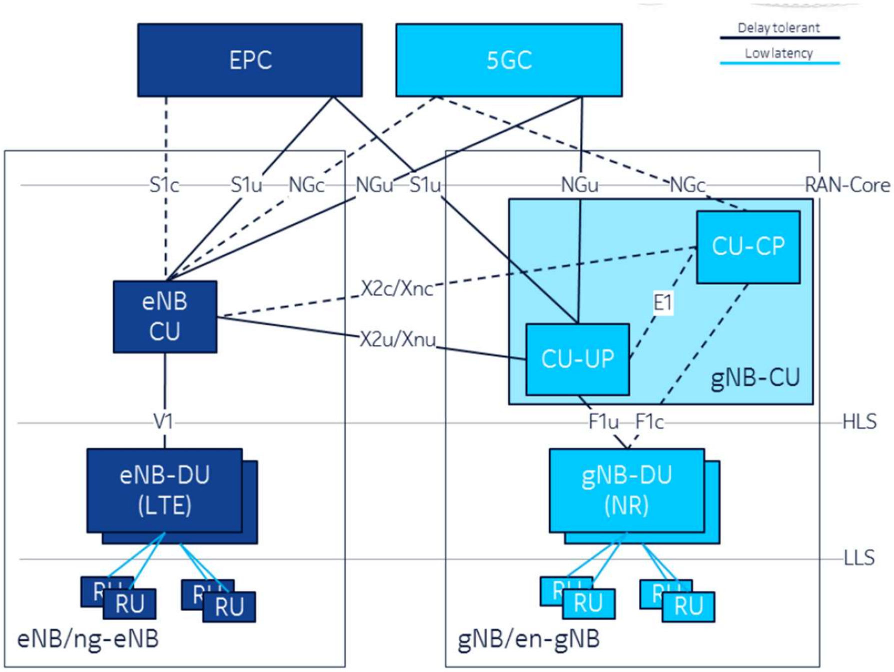

Figure 2: Disaggregated RAN Architecture

Chapter 2: Common Security Requirements

Section 2.1: Access and Authorization

2.1.1 Management Protocols Mutual Authentication

Requirement:

The disaggregated gNB 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 disaggregated gNB management and maintenance.

[Ref [1]: 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:

Disaggregated gNB 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.

[Ref [1]: 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:

Disaggregated gNB 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). Disaggregated gNB supports RBAC with minimum of 3 user roles, in particular, for OAM privilege management for disaggregated gNB Management and Maintenance, including authorization of the operation for configuration data and software via the network product console interface.

[Ref [1] TSDSI STD T1.3GPP 33.117- 16.7.0 V.1.0.0. Section 4.2.3.4.6.2]

Note: The reference to Console interface may not be applicable here for Generalized Virtual Network Product (GVNP) Models of Type 1 & 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. An exception to this requirement is local access and machine accounts where at least one authentication attribute shall be supported.

[Ref [1]: 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 disaggregated gNB as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to disaggregated gNB remotely.

This remote root user access restriction is also applicable to application software's / tools such as TeamViewer, desktop sharing which provide remote access to the disaggregated gNB.

Note: This clause may not be applicable in GVNP Type-1.

[Ref [1]: 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.

[Ref [1]: 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 disaggregated gNB.

Disaggregated gNB 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.

Disaggregated gNB shall not enable the use of group accounts or group credentials or sharing of the same account between several users.

[Ref [1]: 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) 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.

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.1.1]

Note: The reference to 'Local accesses and 'Console' may not be applicable here for GVNP Models of Type 1 & 2.

2.2.2 Authentication Support – External

Requirement:

If the disaggregated gNB supports external authentication mechanism such as AAA server (for authentication, authorisation and accounting services), then the communication between disaggregated gNB 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 disaggregated gNB.

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 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 disaggregated gNB. An exception to this requirement is machine accounts.

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.3]

Note: Sub section (iv) Not applicable to disaggregated RAN RU.

2.2.4 Enforce Strong Password

Requirement:

a) The configuration setting shall be such that a disaggregated gNB 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 disaggregated gNB). 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 disaggregated gNB.

e) When a user is changing a password or entering a new password, disaggregated gNB /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.

[Ref [1]: 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.

Disaggregated gNB 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.

Reauthentication of the OAM user shall be repeated following any period of inactivity lasting 15 minutes or longer.

[Ref [1]: 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.

Disaggregated gNB shall enforce password change based on password management policy.

In particular, the system shall enforce password expiry. Disaggregated gNB 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 disaggregated gNB shall store at least the three previously set passwords. The maximum number of passwords that the disaggregated gNB 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.

Disaggregated gNB 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 disaggregated gNB.

[Ref [1]: 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 "*".

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.4]

Note: This section not applicable to disaggregated RAN RU.

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 1st time login to the system or the OEM provides instructions on how to manually change it.

[Ref [1]: 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.

[Ref [1]: 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, typically 5. 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 shall 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.

[Ref [1]: 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:

(a) Software package integrity shall be validated during the software update stage.

(b) Disaggregated gNB shall support software package integrity validation via cryptographic means, e.g., digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only. To this end, the Disaggregated gNB 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.

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

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

Note: Code signing (valid and not time expired) is also allowed as an option in (b) above.

[Ref [1]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.5]

2.3.2 Secure Upgrade

Requirement:

(i) Disaggregated gNB Software package integrity shall be validated in the installation /upgrade stage.

(ii) Disaggregated gNB 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 SMF 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.

[Ref [1]: 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 disaggregated gNB Software which includes OEM developed code, third party software and opensource code libraries used/embedded in the disaggregated gNB.

(ii) Disaggregated gNB 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 disaggregated gNB and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

[Ref [11]: https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html]

[Ref [12]: https://owasp.org/www-project-top-ten/]

[Ref [13]: https://owasp.org/www-project-api-security/]

2.3.4 Known Malware and backdoor Check

Requirement:

OEM shall submit an undertaking stating that disaggregated gNB is free from all known malware and backdoors as on the date of offer of disaggregated gNB to designated TSTL for testing and shall submit their internal Malware Test Document (MTD) of the disaggregated gNB 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 disaggregated gNB shall not be present/configured.

Orphaned software components /packages shall not be present in disaggregated gNB.

OEM shall provide the list of software that are necessary for disaggregated gNB’s operation.

In addition, OEM shall furnish an undertaking as “disaggregated gNB does not contain Software that is not used in the functionality of disaggregated gNB”

[Ref [1]: 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:

Disaggregated gNB 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. Disaggregated gNB 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 disaggregated gNB and their purpose needs to be provided by the OEM as prerequisite for the test case.

[Ref [1]: 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 disaggregated gNB shall boot only from the memory devices intended for this purpose.

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section- 4.2.3.3.2]

Note: This may not be applicable here for GVNP Models of Type 1 & 2.

2.3.8 Secure Time Synchronization

Requirement:

Disaggregated gNB shall use reliable time and date information provided through NTP/PTP server. Disaggregated gNB shall establish a secure communication channel through standard interface with the Network Time Protocol (NTP) / Precise Time Protocol (PTP) server as per appropriate TEC ER (Essential Requirement) document.

Disaggregated gNB shall establish a 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.

Disaggregated gNB shall generate audit logs for all changes to time settings.

Note: RFC 8915 which proposes Network Time Security (NTS) as an extension field for the NTP version 4 is also permitted.

2.3.9 Restricted reachability of services

Requirement:

The disaggregated gNB 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. This limitation shall be realized on the disaggregated gNB itself (without measures (e.g., firewall) at network side) according to the requirement detailed in section 2.7.1 Traffic Filtering.

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

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section 4.3.2.2]

2.3.10 Self Testing

Requirement:

The Disaggregated gNB's cryptographic module shall perform power-up self-tests and conditional self- tests to ensure that the module is functioning properly. Power-up self-tests shall be performed when the cryptographic module is powered up during System bootup/restart. Conditional self-tests shall be performed when an applicable security function or operation is invoked (i.e. security functions for which self-tests are required). If a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status output interface. The cryptographic module shall not perform any cryptographic operations while in an error state.

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 Disaggregated gNB shall be permanently deactivated. Permanently means that they shall not be reactivated again after the Disaggregated gNB system’s reboot. If unused functions of software cannot be deleted or uninstalled individually as required in clause "2.3.5 No unused software" of the present document, such functions shall be deactivated in the configuration of Disaggregated gNB permanently.

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 Disaggregated gNB.

EXAMPLE: A debugging function in software which can be used for troubleshooting shall not be activated during normal operation of the Disaggregated gNB.

[Ref [1]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.4]

Note: The reference to hardware may not be applicable here for GVNP Models of Type 1 & 2. Applicable only when GVNP Type3 product can be used.

2.4.2 No unsupported components

Requirement:

OEM to ensure that the disaggregated gNB shall not contain software and hardware components that are no longer supported by them or their 3rd 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.

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.5]

Note: The reference to hardware may not be applicable here for GVNP Models of Type 1 & 2. Applicable only when GVNP Type3 product can be used.

2.4.3 Avoidance of Unspecified mode of Access

Requirement:

Disaggregated gNB shall not contain any wireless access mechanism which is unspecified or not declared.

An undertaking shall be given by the OEM as follows:

"The disaggregated gNB does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel."

Section 2.5: User Audit – This section is not applicable to disaggregated RAN RU

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.

[Ref [1]: 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 disaggregated gNB shall log all important Security events with unique System Reference details as given in the Table below.

Disaggregated gNB 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 disaggregated gNB.	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/disaggregated gNB that forces a reboot or shutdown OR where the network device/disaggregated gNB 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/disaggregated gNB (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.
Resetting Passwords (Optional)	Resetting of user account passwords by the Administrator	Administrator username
		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	Changes to audit data including	Timestamp

(Optional)	deletion of audit data	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

[Ref [1]: 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 disaggregated gNB shall support (near real time) forwarding of security event logging data to an external system available in redundant configuration by push or pull mechanism through diverse links.

(b) Log functions should support secure uploading of log files to a central location or to a system external for the disaggregated gNB.

(ii) Disaggregated gNB shall be able to store the generated audit data itself may be with limitations.

(iii) Disaggregated gNB 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), disaggregated gNB shall be able to store the generated audit data locally. The memory for this purpose shall be dimensioned to cater for the continuous storage of two days of audit data. 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.

[Ref [1]: 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:

Disaggregated gNB 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 disaggregated gNB 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 disaggregated gNB (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 FIPS 140-2 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 disaggregated gNB (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 FIPS 140-2 or later as prescribed by NIST standards".

[Ref [17]: ENISA Recommendation "Standardization in support of the cybersecurity certification", Dec 2019]
[Ref [14]: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf]

2.6.3 Cryptographic Algorithms implementation Security Assurance

Requirement:

Cryptographic algorithm implemented inside the Crypto module of disaggregated gNB shall be in compliance with the latest 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 disaggregated gNB is in compliance with the latest FIPS standards (for the specific crypto algorithm embedded inside the disaggregated gNB)"

[Ref [17]: ENISA Recommendation "Standardization in support of the cybersecurity certification", Dec 2019]
[Ref [14]: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf]

2.6.4 Protecting data and information – Confidential System Internal Data

Requirement:

a) When disaggregated gNB 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) Such functions could be, for example, local or remote OAM CLI or GUI, logging messages, alarms, configuration file exports etc. Confidential system internal data contains authentication data (i.e., PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration.
c) Access to maintenance mode shall be restricted only to authorised privileged user.

[Ref [1]: 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 disaggregated gNB 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 disaggregated gNB: 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.

[Ref [1]: 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, disaggregated gNB 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 disaggregated gNB to create copy of data for illegal transmission.
c) The software functions, components in the disaggregated gNB 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) Disaggregated gNB 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 disaggregated gNB.
c) Session logs shall be generated for establishment of any session initiated by either user or disaggregated gNB.

2.6.8 Protection against Data Exfiltration – Covert Channel

Requirement:

a) Disaggregated gNB 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 disaggregated gNB.
c) Session logs shall be generated for establishment of any session initiated by either user or disaggregated gNB system.

Section 2.7: Network Services

2.7.1 Traffic Filtering – Network Level Requirement:

Disaggregated gNB shall provide a mechanism to filter incoming IP packets on any IP interface (Refer to RFC 3871).
In particular the disaggregated gNB 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 disaggregated gNB shall provide a mechanism to disable/enable each defined rule.

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section 4.2.6.2.1]

[Ref [16]: RFC 3871 – Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.2 Traffic Separation

Requirement:

The disaggregated gNB 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.

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.5.1].

[Ref [16]: RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.3 Traffic Protection –Anti-Spoofing:

Requirement:

Disaggregated gNB 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.

[Ref [1]: 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 (Not applicable to disaggregated RAN RU)

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:

- Disaggregated gNB supports the capability described above, and this is stated in the product documentation.
- The disaggregated gNB's product documentation states that the capability is not supported and that the disaggregated gNB needs to be deployed together with a separate entity which provides the capability described above.

[Ref [1]: 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:

Disaggregated gNB shall have protection mechanism against Network level and Application-level DDoS attacks.

Disaggregated gNB 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:

- 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

[Ref [1]: 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:

Disaggregated gNB shall act in a predictable way if an overload situation cannot be prevented. Disaggregated gNB 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 disaggregated gNB cannot reach an undefined and thus potentially insecure, state.

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

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.3]

2.8.3 Interface robustness requirements

Requirement:

Disaggregated gNB 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 disaggregated gNB. 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).

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.6.2.2]

Note: This clause may not be applicable for GVNP Type 1.

Section 2.9: Vulnerability Testing Requirements

2.9.1 Fuzzing – Network and Application Level

Requirement:

It shall be ensured that externally reachable services of disaggregated gNB are reasonably robust when receiving unexpected input.

[Ref [1]: 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 disaggregated gNB, only documented ports on the transport layer respond to requests from outside the system.

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.4.2]

2.9.3 Vulnerability Scanning

Requirement:

The purpose of vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans in place to mitigate them) on the Network Product, both in the OS and in the applications installed, that can be detected by means of automatic testing tools via the Internet Protocol enabled network interfaces.

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

Sr. 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 three months
4	0.1 - 3.9	Low	To be patched within a year

Zero-day vulnerabilities shall be remediated immediately or as soon as possible.

[Ref [1]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.4.3]

[Ref [15]: https://nvd.nist.gov/vuln-metrics/cvss]

[Ref [18]: GSMA NG 133 Cloud Infrastructure Reference Architecture]

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 disaggregated gNB from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided.

[Ref [1]: 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 (Not applicable to disaggregated RAN RU)

Requirement:

Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the disaggregated gNB.

Disaggregated gNB 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	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

Disaggregated gNB 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

[Ref [1]: 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:

Disaggregated gNB 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.

[Ref [1]: 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 disaggregated gNB shall have a unique identification with appropriate non-repudiation controls.

[Ref [1]: 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.
2. Proxy ARP
3. Directed broadcast
4. IPv4 Multicast handling
5. Gratuitous ARP messages

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section - 4.3.3.1.2]

Note: This clause may not be applicable for GVNP Type 1.

2.10.6 No automatic launch of removable media

Requirement:

Disaggregated gNB shall not automatically launch any application when a removable media device is connected.

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.3]

Note: This clause may not be applicable for GVNP Type 1 and 2.

2.10.7 Protection from buffer overflows

Requirement:

Disaggregated gNB 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.

[Ref [1]: 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 disaggregated gNB 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.

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section - 4.3. 3.1.6]

Note: This clause may not be applicable for GVNP Type 1 and 2.

2.10.9 File-system Authorization privileges

Requirement:

Disaggregated gNB 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.

[Ref [1]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section - 4.3.2.7]

2.10.10 SYN Flood Prevention (Not applicable to disaggregated RAN RU)

Requirement:

Disaggregated gNB shall support a mechanism to prevent Syn Flood attacks. This feature shall be enabled by default.

[Ref [1]: 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.

[Ref [1]: 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, disaggregated gNB 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:

Disaggregated gNB 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 disaggregated gNB supports **web management interface.**

Note: This section is not applicable to disaggregated RAN RU.

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.

[Ref [1]: 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 disaggregated gNB webserver (for both successful as well as failed attempts) shall be logged by disaggregated gNB.

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

[Ref [1]: 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 disaggregated gNB shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.

Disaggregated gNB 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.

[Ref [1]: 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 disaggregated gNB web server processes shall run with system privileges.

[Ref [1]: 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 disaggregated gNB operation shall be deactivated.

[Ref [1]: 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 disaggregated gNB operation.

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

[Ref [1]: 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.

[Ref [1]: 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.

[Ref [1]: 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.

[Ref [1]: 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 disaggregated gNB web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges.

[Ref [1]: 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 disaggregated gNB web server shall be removed.

[Ref [1]: 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.

[Ref [1]: 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 disaggregated gNB web server and the modules/add-ons used.

[Ref [1]: 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 disaggregated gNB web server, and the modules/add-ons used.

Default error pages of the disaggregated gNB web server shall be replaced by error pages defined by the OEM.

[Ref [1]: 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 disaggregated gNB operation shall be deleted.

[Ref [1]: 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 disaggregated gNB web server's document directory.

In particular, the disaggregated gNB web server shall not be able to access files which are not meant to be delivered.

[Ref [1]: 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.

[Ref [1]: 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, disaggregated gNB 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, disaggregated gNB 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 disaggregated gNB 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 disaggregated gNB shall not accept session identifiers from GET/POST variables.
12. The disaggregated gNB shall be configured to only accept server generated session ID.

[Ref [1]: 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 Remote Diagnostic Procedure – Verification

Requirement:

If the disaggregated gNB is providing Remote access for troubleshooting purposes/alarm maintenance then it shall be allowed only for authorized users, other than the root user.

All activities performed by the remote user are to be logged with the following parameters:

1. User id
2. Time stamp
3. Interface type
4. Event type (e.g., CRITICAL, MAJOR, MINOR)
5. Command/activity performed and
6. Result type (e.g., SUCCESS, FAILURE).
7. IP Address of remote machine

[Ref [19]: GSMA NG 133: GSM Association Non-confidential Official Document NG.133 - Cloud Infrastructure Reference Architecture managed by OpenStack section 2.2.7.7]

2.12.2 No System Password Recovery

Requirement:

No provision shall exist for disaggregated gNB System / Root password recovery.

2.12.3 Secure System Software Revocation

Requirement:

Once the disaggregated gNB 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 non-repudiation controls.

Disaggregated gNB shall support a well-established control mechanism for rolling back to previous software image.

2.12.4 Software Integrity Check –Installation

Requirement:

Disaggregated gNB 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 ITSAR" only.

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

[Ref [1]: TSDSI STD T1. TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.5]

2.12.5 Software Integrity Check – Boot

Requirement:

The disaggregated gNB 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 ITSAR" to the expected reference value.

Note: This may not be applicable for GVNP Type 1 and Type 2.

2.12.6 Unused Physical and Logical Interfaces Disabling

Requirement:

Disaggregated gNB 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.

Note: This may not be applicable for GVNP Type 1 and Type 2.

2.12.7 Predefined accounts shall be deleted or disabled

Requirement:

Predefined or default user accounts (other than Admin/Root) in disaggregated gNB shall be deleted or disabled.

[Ref [1]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.2.2]

Chapter 3: Disaggregated gNB CU-CP Specific Security Requirements

3.1 Integrity protection of RRC-signaling

Requirement:

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

[Ref [2]: TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.1]

[Ref [3]: TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.3]

3.2 RRC integrity check failure

Requirement:

The RRC integrity checks shall be performed both in the ME and the disaggregated gNB-CU-CP. 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 disaggregated gNB-CU-CP side or on the ME side.

[Ref [2]: TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.4]

[Ref [3] TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 6.5.1]

3.3 Ciphering of RRC-signaling

Requirement:

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

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

[Ref [2]: TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.6]

[Ref [3]: TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.2]

3.4 Replay protection of RRC-signaling

Requirement:

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

[Ref [2]: TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.9]

[Ref [3]: TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.3]

3.5 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 disaggregated gNB-CU-CP 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."

[Ref [2]: TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.12]

[Ref [3]: TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 5.11.2]

3.6 Key refresh at the disaggregated 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 disaggregated gNB-CU-CP when a PDCP COUNTs are about to be re-used with the same Radio Bearer identity and with the same K_{gNB}.

[Ref [2]: TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.13]

[Ref [3]: TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 6.9.4.1]

[Ref [6]: TSDSI STD T1.3GPP 33.401-16.3.0 V1.0.0 section E3.4.2]

3.7 Bidding down prevention in Xn-handovers

Requirement:

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

[Ref [2]: TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.14]

[Ref [3]: TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 6.7.3.1]

3.8 AS protection algorithm selection in disaggregated gNB-CU-CP change

Requirement:

The target disaggregated gNB-CU-CP 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 disaggregated gNB-CU-CP selects different algorithms compared to the source gNB.

[Ref [2]: TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.15]

[Ref [3]: TSDSI STD T1.3GPP 33.501 16.9.0 V1.0.0 section 6.7.3.1 & 6.7.3.2]

3.9 Key update at the disaggregated gNB-CU-CP on dual connectivity

Requirement:

When executing the procedure for adding subsequent radio bearer(s) to the same SN, the MN 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.

[Ref [2]: TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.18]

[Ref [3]: TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 Sections 6.10.2.1, 6.10.2.2.1]

3.10 UP security activation in Inactive scenario

Requirement:

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

[Ref [2]: 3GPP TS 33.511 17.3.0 V1.0.0 section 4.2.2.1.19]

[Ref [3]: TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 6.8.2.1.3]

3.11 Control plane data confidentiality protection over N2/Xn/F1/E1 interface

Requirement:

F1-C interface shall support confidentiality protection, the E1 interface between CU-CP and CU-UP, the transport of control plane data over N2 is confidentiality protected and the transport of control plane data over Xn is confidentiality protected.

[Ref [4]: TSDSI STD T1.3GPP 33.523-18.1.0 V1.0.0 section 5.2.2.1.2]

3.12 Control plane data integrity protection over N2/Xn/F1/E1 interface

Requirement:

F1-C interface shall support integrity and replay protection, the E1 interface between CU-CP and CU-UP, the transport of control plane data over N2 is integrity and replay protected and the transport of control plane data over Xn is integrity and replay protected.

[Ref [4]: TSDSI STD T1.3GPP 33.523-18.1.0 V1.0.0 section 5.2.2.1.3]

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

Requirement:

The disaggregated gNB-CU-CP shall activate the ciphering of user data based on the security policy sent by the SMF.

[Ref [4]: TSDSI STD T1.3GPP 33.523-18.1.0 V1.0.0 section 5.2.2.1.4]

3.14 Integrity protection of user data based on the security policy sent by the SMF

Requirement:

The disaggregated gNB-CU-CP shall activate the integrity protection of user data based on the security policy sent by the SMF.

[Ref [4]: TSDSI STD T1.3GPP 33.523-18.1.0 V1.0.0 section 5.2.2.1.5]

3.15 Mutual authentication between CU-CP and CU-UP over E1 interface.

Requirement:

Mutual authentication shall be supported over the E1interface between the gNB-CU-CP and the gNB-CU-UP using DTLS and/or IKEv2

[Ref [3]: TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 9.8.3]

Chapter 4: Disaggregated gNB-CU-UP Specific Security Requirements

4.1 UP integrity check failure

Requirement:

The User Plan integrity check shall be performed both in UE and disaggregated gNB. If the disaggregated gNB-CU-UP 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.

[Ref [2]: TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.5]

[Ref [3]: TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 6.6.4]

4.2 Replay protection of user plane data between the disaggregated gNB-CU-UP and the UE

Requirement:

The disaggregated gNB-CU-UP shall support replay protection of user plane data between the disaggregated gNB-CU-UP and the UE.

[Ref [2]: TSDSI STD T1. 3GPP TS 33.511 16.7.0 V1.0.0 section 4.2.2.1.8]

[Ref [3]: TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 section 5.3.3]

4.3 Control plane data confidentiality protection over E1 interface

Requirement:

E1 interface between CU-CP and CU-UP shall support confidentiality protection.

[Ref [4]: TSDSI STD T1.3GPP 33.523-18.1.0 V1.0.0 section 6.2.2.1.2]

4.4 Control plane data integrity protection over E1 interface

Requirement:

E1 interface between CU-CP and CU-UP shall support integrity and replay protection.

[Ref [4]: TSDSI STD T1.3GPP 33.523-18.1.0 V1.0.0 section 6.2.2.1.3]

4.5 User plane data confidentiality protection over N3/Xn/F1 interface

Requirement:

The disaggregated gNB-CU-UP shall support confidentiality protection on the disaggregated gNB DU-CU F1-U interface for user plane, the transport of user data over N3 is confidentiality protected and the transport of user plane data over Xn is confidentiality protected.

[Ref [4]: TSDSI STD T1.3GPP 33.523-18.1.0 V1.0.0 section 6.2.2.1.4]

4.6 User plane data integrity protection over N3/Xn/F1 interface

Requirement:

The disaggregated gNB-CU-UP shall support integrity and replay protection on the disaggregated gNB DU-CU F1-U interface for user plane, the transport of user data over N3 is integrity and replay protected and the transport of user plane data over Xn is integrity and replay protected.

[Ref [4]: TSDSI STD T1.3GPP 33.523-18.1.0 V1.0.0 section 6.2.2.1.5]

4.7 Integrity and replay protection of user data between the UE and the disaggregated gNB-CU-UP

Requirement:

The disaggregated gNB-CU-UP shall support integrity and replay protection of user data between the UE and the gNB-CU-UP.

[Ref [4]: TSDSI STD T1.3GPP 33.523-18.1.0 V1.0.0 section 6.2.2.1.6]

4.8 Confidentiality protection of user data between the UE and the gNB-CU-UP

Requirement:

The disaggregated gNB-CU-UP shall support confidentiality protection of user data between the UE and the gNB-CU-UP.

[Ref [4]: TSDSI STD T1.3GPP 33.523-18.1.0 V1.0.0 section 6.2.2.1.7]

Chapter 5: Disaggregated gNB-DU Specific Security Requirements

The disaggregated gNB-DU specific security requirements are derived from 3GPP TS 33.523, TS 33.511, TS 33.501 and TS 38.473. These specific requirements will focus on the F1-C and F1-U interfaces of the disaggregated gNB DU and the interface towards gNB-RU.

5.1 Control plane confidentiality protections over F1-C interface of disaggregated gNB-DU

Requirement:

The disaggregated gNB-DU shall establish confidentiality protection over F1-C interface between disaggregated gNB-DU and disaggregated gNB-CU.

[Ref [8]: TSDSI STD T1. 3GPP TS 38.473 16.14.0 V1.0.0 section 8.2.3]

[Ref [4]: TSDSI STD T1. 3GPP TS 33.523 18.1.0 V1.0.0 section 7.2.2.1.1]

5.2 Control plane integrity protections over F1-C interface of disaggregated gNB-DU

Requirement:

The disaggregated gNB-DU shall establish integrity protection over F1-C interface between disaggregated gNB-DU and disaggregated gNB-CU.

[Ref [8]: TSDSI STD T1. 3GPP TS 38.473 16.14.0 V1.0.0 section 8.2.3]

[Ref [4]: TSDSI STD T1. 3GPP TS 33.523 18.1.0 V1.0.0 section 7.2.2.1.2]

5.3 User data confidentiality protections over F1-U interface of disaggregated gNB-DU

Requirement:

The disaggregated gNB-DU shall establish confidentiality protection over F1-U interface between disaggregated gNB-DU and disaggregated gNB-CU.

[Ref [8]: TSDSI STD T1. 3GPP TS 38.473 16.14.0 V1.0.0 section 8.10.4]

[Ref [4]: TSDSI STD T1. 3GPP TS 33.523 18.1.0 V1.0.0 section 7.2.2.1.3]

5.4 User plane data integrity protections over F1-U interface of disaggregated gNB-DU

Requirement:

The disaggregated gNB-DU shall establish integrity protection over F1-U interface between disaggregated gNB-DU and disaggregated gNB-CU.

[Ref [8]: TSDSI STD T1. 3GPP TS 38.473 16.14.0 V1.0.0 section 8.2.3]

[Ref [4]: TSDSI STD T1. 3GPP TS 33.523 18.1.0 V1.0.0 section 7.2.2.1.4]

5.5 User plane integrity and replay protection over eCPRI interface between disaggregated gNB-DU and disaggregated gNB-RU

Requirement:

The disaggregated gNB-DU shall support integrity and replay protection over eCPRI interface between disaggregated gNB-DU and disaggregated gNB-RU

[Ref [9]: eCPRI Specification V2.0, section 6.8.2.1]

5.6 Control plane integrity and replay protection over eCPRI interface between disaggregated gNB-DU and disaggregated gNB-RU

Requirement:

The disaggregated gNB-DU shall support integrity and replay protection over eCPRI interface between disaggregated gNB-DU and disaggregated gNB-RU

[Ref [9]: eCPRI Specification V2.0, section 6.8.2.2]

5.7 User plane confidentiality protection over eCPRI interface between disaggregated gNB-DU and disaggregated gNB-RU

Requirement:

The disaggregated gNB-DU shall support integrity and replay protection over eCPRI interface between disaggregated gNB-DU and disaggregated gNB-RU

[Ref [9]: eCPRI Specification V2.0, section 6.8.2.1]

5.8 Control plane confidentiality protection over eCPRI interface between disaggregated gNB-DU and disaggregated gNB-RU

Requirement:

The disaggregated gNB-DU shall support integrity and replay protection over eCPRI interface between disaggregated gNB-DU and disaggregated gNB-RU

[Ref [9]: eCPRI Specification V2.0, section 6.8.2.2]

Chapter 6: Disaggregated RAN - RU Specific Security Requirements

The RU specific security requirements are derived from 3GPP TR 33.926 and TS 33.511, and TS 33.501. These specific requirements will focus on the following interfaces of the disaggregated RAN.

- eCPRI interface or F2 interface or Open Fronthaul interface.

6.1 User plane protection over F2 interface between disaggregated RAN RU and DU

Requirement:

The disaggregated RAN RU shall support IPsec protection over eCPRI interface for user plane data over IP and MACsec protection for user plane data over Ethernet

[Ref [9]: eCPRI Specification V2.0, section 6.8.2.1]

6.2 Control and management plane protection over F2 interface between disaggregated RAN RU and DU

Requirement:

For eCPRI, the disaggregated RAN RU shall support TLS, IPSec or MACsec to provide transmission security and access control.

[Ref [9]: eCPRI Specification V2.0, section 6.8.2.2]

6.3 User plane protection over Uu interface between disaggregated RAN RU and UE

Requirement:

The disaggregated RAN RU shall support integrity, confidentiality and replay protection of user plane data over Uu interface between disaggregated RAN RU and UE

6.4 Control plane protection over Uu interface between disaggregated RAN RU and UE

Requirement:

The disaggregated RAN RU shall support integrity, confidentiality and replay protection of control plane data over Uu interface between disaggregated RAN RU and UE.

Annexure-I

Definition

1. DDoS: A distributed denial-of-service attack that renders the victim un-usable by the external environment.
2. 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.
3. eNodeB: a Base station which connects UE to 4G Core Network.
4. en-gNB: evolved next generation gNB which connects to 5G Core network and 4G core network and eNB in case of dual connectivity.
5. E1AP – E1 Application Protocol.
6. F1AP – F1 Application Protocol
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. N2 Interface: The interface between gNB and AMF
11. N3 Interface: The interface between gNB and UPF
12. Network Element: A discrete telecommunications entity which can be managed over a specific interface e.g., the gNB.
13. ng-eNB: a base station which connects UE to 4G core network and 5G Core network and gNB in case of dual connectivity.
14. NG-RAN: It is the radio access network introduced for accessing 5G.
15. NG-RAN-CU: NG-RAN Central Unit responsible for RRC, SDAP, PDCP in disaggregated RAN.
16. NG-RAN-DU: NG-RAN Distributed Unit responsible for RLC and MAC in disaggregated RAN.
17. NG-RAN RU: NG-RAN Radio Unit responsible for Physical layer of disaggregated RAN.
18. NG-U interface: New generation user plane interface between eNB and 5G Core network
19. Non-Access Stratum: Protocols between UE and the core network that are not terminated in the RAN.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.

25. 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.
26. Security: The ability to prevent fraud as well as the protection of information availability, integrity, and confidentiality.
27. Transmission or Transport is the transfer of information from one entity (transmitter) to another (receiver) via a communication path.
28. Uplink: An "uplink" is a unidirectional radio link for the transmission of signals from a UE to a base station.
29. 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.
30. Xn-Interface: The interface between two gNB.

Annexure-II

Acronyms

5GC - 5G Core Network

5GS - 5G System

AAA - Authentication, Authorization and Accounting

AKA - Authentication and Key Agreement

AKA' - AKA Prime

ARP - Address Resolution Protocol/Allocation and Retention Priority

AS - Access Stratum

AuSF - Authentication Server Function

CLI - Command Line Interface

CP - Control Plane

CU – Central Unit

DDoS - Distributed Denial of Service

DL - Downlink

DN - Data Network

DTLS - Datagram Transport Layer Security

DU – Distributed Unit

EAP - Extensible Authentication Protocol

ECS - EDNS Client Subnet

EPC - Evolved Packet Core

EPS - Evolved Packet System

eNB - Evolved Node B (Fourth Generation Base Station)

engNB - Enhanced 5G Next Generation Base station

gNB – Next Generation Node B

gNB-CU – Next Generation Node B Control Unit

gNB-DU – Next Generation Node B Distributed Unit

gNB-RU – Next Generation Node B Radio Unit

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

IAB – Integrated Access and Backhaul

ICMP - Internet Control Message Protocol

IMS - IP Multimedia Subsystem

IP - Internet Protocol

IPSec – IP Security
ISO-OSI - International organization of Standardization – Open System Interconnection
MAC – Medium Access Control
MACSec – MAC Security
NAS - Non-Access Stratum
NEF - Network Exposure Function
NF - Network Function
NG - Next Generation
NG-C – NG-Control Plane
NG-U – NG-User Plane
ng-eNB - Next Generation e-NodeB
NG-RAN - Next Generation Radio Access Network
NGMN – Next Generation Mobile Network.
NRF - Network Repository Function
O&M - Operations and Maintenance
OAM - Operations, Administration, Maintenance
OS - Operating System
PCF - Policy Control Function
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
RRH – Remote Radio Head
RU – Radio Unit
SMF - Session Management Function
TSTL - Telecom Security Testing Laboratory
UDM - Unified Data Management
UDR - Unified Data Repository
UE - User Equipment
UL - UpLink
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. TSDSI STD T1.3GPP 33.117-16.7.0 V1.0.0: “Catalogue of General Security Assurance Requirements”.
2. TSDSI STD T1.3GPP 33.511-16.7.0 V1.0.0 “Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class”.
3. TSDSI STD T1.3GPP 33.501-16.9.0 V1.0.0 Security architecture and procedures for 5G System”.
4. TSDSI STD T1.3GPP 33.523-18.1.0 V1.0.0 Security Assurance Specification (SCAS) split gNB product classes.
5. TSDSI STD T1.3GPP 33.926-16.6.0 V1.0.0 Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes.
6. TSDSI STD T1.3GPP 38.401-16.1.0 V1.0.0 NG-RAN Architecture description
7. TSDSI STD T1.3GPP 38.463-16.15.0 V1.0.0 NG-RAN E1 Application Protocol (E1AP)
8. TSDSI STD T1.3GPP 38.473-16.15.0 V1.0.0 NG-RAN F1 Application Protocol (F1AP)
9. Common Public Radio Interface: eCPRI Specification V2.0
10. NGMN Overview on 5G RAN Functional Decomposition by NGMN alliance.
11. https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html
12. https://owasp.org/www-project-top-ten/
13. https://owasp.org/www-project-api-security/
14. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
15. https://nvd.nist.gov/vuln-metrics/cvss
16. RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure
17. ENISA Recommendation “Standardization in support of the cybersecurity certification”, Dec 2019
18. GSMA NG 133 Cloud Infrastructure Reference Architecture
19. GSMA NG 133: GSM Association Non-confidential Official Document NG.133 - Cloud Infrastructure Reference Architecture managed by OpenStack section 2.2.7.7
20. 3GPP TR 38.816-15.0.0 Study on CU-DU lower layer split for NR.

-End of Document-