Indian Telecom Security Assurance Requirements (ITSAR)

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

Group-II Devices
Common Security Requirements ITSAR

ITSAR Number: ITSAR702022601
ITSAR Name: NCCS/ITSAR/Standards Applicable for Group of Equipment/CSR Group of Devices/Group-II Devices-V1.0.0

Date of Release: 29.01.2026 Version: 1.0.0
Date of Enforcement:

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

Sr. No.	Title	ITSAR No.	Version	Date of Release	Remark
1.	Group-II Devices Common Security Requirements ITSAR	ITSAR702022601	1.0.0		First release

Table of Contents

A) Outline

This Indian Telecom Security Assurance Requirement (ITSAR) document specifies Common Security Requirements for Group-II devices as mentioned in ***office memorandum regarding "Expanding the scope of CSR Testing"*** Ltr No. NCCS/SAS/6-1/2024-25/ dated at Bengaluru,2nd January, 2025.
As per the above referred OM, Group II contains ITSARs of 5G Aggregated gNB NSA Option-3,7&4, 5G Aggregated gNB SA Option-2 and 4G Network Access element eNodeB. This document begins with an overview of Grouping, including its scope and objectives, and then proceeds to outline the Common Security Requirements of the ITSARs applicable to Group II devices.

B) Scope

This document defines Common Security Requirements for Indian Telecom Security Assurance Requirements (ITSARs) of Group II devices (5G Aggregated gNB NSA Option-3,7&4, 5G Aggregated gNB SA Option-2 and 4G Network Access element eNodeB).It serves as the basis for designating Telecom Security Testing Labs (TSTLs) for testing the Common Security Requirements of these devices and security certification of these devices till TSTL capable of testing SSR is available.

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 a 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.

D) Applicability of the clauses

If a requirement explicitly specifies the applicability of a particular device, it applies and is tested only on that device; otherwise, it applies to and is tested on any one or all Group II devices.

Chapter 1: Introduction

The ITSARs are consisting of Common Security Requirements (CSR) and Specific Security Requirements (SSR). The CSR clauses are common across most of the ITSARs. SSR clauses are specific to the 5G Network Access element and 4G Network Access element. However, the testing infrastructure requirement, skill set requirement may vary from device to device or from group of devices to group of devices.

In an endeavor to mandate testing CSR clauses of a group of devices and designate the TSTL for testing CSR clauses of a group of devices ***"Grouping of devices"*** is done.

Chapter 2 of this ITSAR outlines the Common Security Requirements applicable for designating the TSTLs for CSR testing of Group II device ITSARs.

Chapter 2: Common Security Requirements

Section 2.1: Access and Authorization

2.1.1 Management Protocols Mutual Authentication

Requirement:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

The Group II devices 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 Group II devices 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]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

The protocols used for Group II devices management and maintenance shall support mutual authentication mechanisms only i.e. there is mutual authentication of entities for management interfaces on the Group II devices. Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 "shall only be used for the Group II device management and maintenance.

OEM /TSP shall disable permanently the supported Weaker algorithms other than specified in ITSAR Cryptographic control lists document

Note: Any management protocol such as HTTPS Over TLS 1.2 (up to date patched) or latest, IP Sec VPN are permitted

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.4.1]

2.1.2 Management Traffic Protection

Requirement:

The Group II devices 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.

Applicable to 4G eNodeB only: OEM /TSP shall disable permanently the supported Weaker algorithms other than specified in ITSAR Cryptographic control lists document

[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:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

The Group II device 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). The Group II device supports RBAC with minimum of 3 user roles, in particular, for OAM privilege management for the Group II device 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]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

The Group II device shall support Role Based Access Control (RBAC). A role-based access control system uses a set of controls which 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.
The Group II device supports Role Based Access Control (RBAC) conforming to the globally accepted RBAC standard INCITS 359-2012(R2017), with default support of minimum 3 user roles, in particular, for OAM privilege management, for the Group II device Management and Maintenance, including authorization of the operation for configuration data and software via the Group II device console interface.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 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.

Applicable to 5G gNodeB SA and gNodeB NSA only: 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:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

Login to the Group II device as root or equivalent highest privileged user shall be limited to the system console only. Root user shall not be allowed to login to the Group II device 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]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

Login to the Group II device as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to the Group II device remotely i.e. remote login access for root/admin/highest privileged users, by default shall be disabled permanently at the time of first installation.

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 Group II device.

[Reference TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.6]

2.1.6 Authorization Policy

Requirement:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

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]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

Only Role based authorization is permitted. Bare minimum RBAC rights are to be assigned for the task to be performed.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.6.1]

2.1.7 Unambiguous identification of the user & group accounts removal

Requirement:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

Users shall be identified unambiguously by the Group II device. The Group II device 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. The Group II device 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]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

Users shall be identified unambiguously by the Group II device. The Group II device shall support assignment of individual accounts IDs per user by default by OS, where a user could be a person, or a machine account, an application, or a system.

The Group II device shall also support assignment of specific ID for individual accounts per user as configured by administrator /root user the Group II device's all inactive users' accounts shall be locked / permanently disabled. The Group II device shall not enable the use of group accounts or group credentials, or sharing of the same account between several users.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Sections 4.2.3.4.1.2]

Section 2.2: Authentication Attribute Management

2.2.1 Authentication Policy

Requirement:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

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 33.117-16.7.0V.1.0.0. Section 4.2.3.4.1.1]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

For local /Remote access, the various user accounts (other than system /admin accounts) on a E-Node –B shall be protected from misuse. To this end, at least one authentication (Cryptographic keys or Token or Passwords) attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user in closed environment Authentication attributes include For Local /Remote access, Minimum two of the Authentication attributes(Cryptographic Keys , Token , Passwords) shall be mandatorily combined to protect user accounts ((other than system /admin accounts) in open environment (internet).

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.1.1]

2.2.2 Authentication Support – External

Requirement:

If the Group II device supports external authentication mechanism such as AAA server (for authentication, authorization and accounting services), then the communication between The Group II device 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.

Applicable to 4G eNodeB only: OEM /TSP shall disable permanently the supported Weaker algorithms other than specified in ITSAR Cryptographic control lists document.

2.2.3 Protection against brute force and dictionary attacks

Requirement:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

A protection against brute force and dictionary attacks that hinder authentication attribute guessing shall be implemented in the Group II device. 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:

a) 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").
b) 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
c) Using an authentication attribute blacklist to prevent vulnerable passwords
d) 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 the Group II device. 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]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

A protection against brute force and dictionary attacks that hinder Authentication Attribute guessing shall be implemented in the Group II device. Brute force and dictionary attacks aim to use automated guessing to ascertain Authentication Attribute for user and machine accounts. Hence, 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.

In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by the Group II device.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 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 Group II device 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 Group II device). 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 Group II device.

e) When a user is changing a password or entering a new password, The Group II device /central system checks and ensures that it meets the password requirements.

Applicable to 5G gNodeB SA, gNodeB NSA only: 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, TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3]

)

2.2.5 Inactive Session timeout

Requirement:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

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. The Group II device 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]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

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 ranging from 2 to 5 minutes.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 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.
The Group II device shall enforce password change based on password management policy.
In particular, the system shall enforce password expiry. The Group II device 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 Group II device shall store at least the three previously set passwords. The maximum number of passwords that the Group II device 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.

Applicable to 4G eNodeB only: The never expiring password option should be disabled permanently. This requirement shall be met either by the Group II device itself or in combination with external authentication system.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.2]

Applicable to 5G gNodeB SA, gNodeB NSA only: Above requirements shall be applicable for all passwords used (e.g. application-level, OS- level, etc.). An exception to this requirement is machine accounts. The Group II device 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 Group II device.

[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 Hiding Password Display/ 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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.4, 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/Change of predefined or default authentication attributes

Requirement:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

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 33.117-16.7.0V.1.0.0. Section 4.2.3.4.2.3]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

Predefined or default authentication attributes shall be deleted or disabled.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.2.3]

2.2.9 Protecting Session - Logout function/Logout function

Requirement:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

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:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

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:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

For software updates, the Group II device 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 Group II device 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]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

The Group II device system software updates shall be carried out strictly using the Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 "only. The Group II device shall allow updates only if code signing certificate is valid and not time expired. Software update integrity shall be verified strictly using the Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 "only.

2.3.2 Secure Upgrade

Requirement:

(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

(i) The Group II device software package integrity shall be validated in the installation /upgrade stage.
(ii) The Group II device 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 Group II device 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]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

(i) The Group II device software package integrity shall be validated in the installation and upgrade stages strictly using the Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 "only.
(ii) The Group II device shall allow upgrades only if code signing certificate is valid and not time expired. To this end, the Group II device shall have a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software upgrade is originated from only these sources.
(iii) Tampered software shall not be executed or installed if integrity check fails.
(iv) The Group II device software upgrades shall be carried out strictly using the Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 "only.
(v) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade, and modify the list mentioned in bullet (i) above.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.3.5]

2.3.3 Source code security assurance

Requirement:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

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 Group II device Software which includes OEM developed code, third party software and opensource code libraries used/embedded in the Group II device.

(ii) The Group II device software shall be free from CWE top 25 and OWASP top10 security weaknesses on the date of offer of product to designated TSTL for testing. For other security weaknesses, OEM shall give mitigation plan.

(iii) The binaries for the Group II device and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

Requirement:

(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

a) Vendor should follow best security practices including secure coding for software development and should be augmented with designated TSTL source code review duly supported by furnishing the Software Test Document (STD) generated while developing the Group II device.

b) Also, Vendor 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 Group II device Software, which includes vendor developed code, third party software and open-source code libraries used/embedded in the Group II device

(ii) The Group II device software is free from all known (Critical, High, Medium based on CVSS) security vulnerabilities, security weaknesses listed in the CVE and CWE databases on the date of product release and Low severity vulnerabilities shall be addressed at the earliest

(iii) The binaries for the Group II device 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 the Group II device is free from all known malware and backdoors as on the date of offer of the Group II device to designated TSTL for testing and shall submit their internal Malware Test Document (MTD) of the Group II device to the designated TSTL.

2.3.5 No unused software / No unused software packages

Requirement:

Software components or parts of software which are not needed for operation

or functionality of the Group II device shall not be present. Orphaned software components /packages shall not be present in the Group II device.

Applicable to 5G gNodeB SA, gNodeB NSA only: OEM shall provide the list of software that are necessary for the Group II device's operation. In addition, OEM shall furnish an undertaking as "The Group II device does not contain Software that is not used in the functionality of the Group II device"

[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 Insecure services/ protocols Removal/ Unnecessary Services Removal

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

The Group II device shall run only those protocol handlers and services which are needed for its operation and which do not have any known security vulnerabilities the Group II device supported those protocol handlers and services which do not have any known security vulnerabilities shall be disabled by default and can be enabled by Operator as per his requirement
In particular, by default the in- secure services (having known vulnerabilities) shall be permanently disabled on the Group II device by the vendor

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.1]
Requirement:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

The Group II device 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. The Group II device 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

Group II device 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 Group II device 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:

The Group II device shall use reliable time and date information provided through NTP/PTP server. The Group II device shall establish secure communication channel with the NTP/PTP server.

The Group II device 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. The Group II device shall generate audit logs for all changes to time settings.

2.3.9 Restricted reachability of services

Requirement:

The Group II device 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.

Applicable to 5G gNodeB SA, gNodeB NSA only: 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.1.0.0Section 4.3.2.2]

2.3.10 Self -Testing/ Avoidance of Unspecified Wireless Access

Requirement:

The Group II device 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 iii) when Administrator Instructs.

(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

An undertaking shall be given by the vendor as follows: "The eNodeB does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel"

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.6.1]

2.3.11 Disable all software- based reset options

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

All the software- based reset operations (eg: Control + ALT +DEL) which forcibly reboots the Group II device system and/or forces the running programs to stop, shall be permanently disabled.

2.3.12 Disable USB stick detection

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

The Group II device system shall restrict users from using USB stick to protect and secure data from stealing.

2.3.13 Lock Down Cron Jobs

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

Cron Jobs for carrying out the tasks such as Scheduling the backups, Monitoring disk space, deleting files and system maintenance activities shall be executed by privileged users such as administrator only.

2.3.14 Change of SSH Port

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

The Group II device's SSH runs services on predefined port on 22. Due to security reasons, to prevent port scanning attacks, This SSH service can run on other port

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 Group II device shall be deactivated in the Group II

device's software and/or hardware.

Applicable to 5G gNodeB SA, gNodeB NSA only: 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 Group II device.

[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 Group II device 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.

Applicable to 5G gNodeB SA, gNodeB NSA only: 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:

(Applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

The Group II device shall not contain any wireless access mechanism which is unspecified or not declared. An undertaking shall be given by the OEM as follows:
"The Group II device 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 using file access rights such that only privilege users including the administrator have access to only read the log files but not allowed to delete or modify the log files.

Applicable to 5G gNodeB SA, gNodeB NSA only: The only allowed operations on security event log are archiving/saving and viewing.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0. V.1.0.0 section 4.2.3.6.3]

2.5.2 Audit Event Generation

Requirement:

The Group II device shall log all important Security events with unique System Reference details as given in the Table below. The Group II device 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:

Sl No	Event Types (Mandatory or optional)	Description	Event data to be logged
1	Incorrect login attempts (Mandatory)	Records any user incorrect login attempts to the Group II device.	Username
			Source (IP address) if remote access
			Outcome of event (Success or
			failure)
			Timestamp
2	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
3	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
4	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
5	Configuration change (Mandatory)	Changes to configuration of the network device	Change made
			Timestamp
			Outcome of event (Success or failure)
			Username
6	Reboot/shutdown/crash (Mandatory)	This event records any action on the network device/The Group II device that forces a reboot or shutdown OR	Action performed (boot, reboot, shutdown, etc.)
			Username (for intentional actions)
			Outcome of event (Success or failure)

		where the network device/The Group II device has	Timestamp
7	Interface status change (Mandatory)	Change to the status of interfaces on the network device/The Group II device (e.g., shutdown)	Interface name and type
			Status (shutdown, down missing link, etc.)
			Outcome of event (Success or failure)
			Timestamp
8	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.
9	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
10	Services (Optional)	Starting and Stopping of Services (if applicable)	Service identity
			Activity performed (start, stop, etc.)
			Timestamp
			Outcome of event (Success or failure)
11	X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
			Reason for failure
			Subject identity
			Type of event
12	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
13	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
14	Session unlocking/ termination (Optional)	Any attempts at unlocking of an interactive session,	User identity (wherever applicable)
			Timestamp
			Outcome of event (Success or failure)

		termination of a remote session by the session locking mechanism,	Subject identity
			Activity performed
			Type of event
15	Trusted Communication paths with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorized 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)
16	Audit data changes (Mandatory)	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
17	User Login (Mandatory)	All use of Identification and authentication mechanisms.	User identity
			Origin of attempt
			(IP address)
			Outcome of event (Success or failure)
			Timestamp
18	access to personal data (Mandatory) *(Applicable to 4G eNodeB only)*	All use of identification and authentication mechanism	user identity
			origin of attempt (e.g.IP address)
			Timestamp
			Personal data in encrypted text (Optional)
			outcome of event (Success or failure)
19	All activities of the remote user other than Root User (Mandatory) *(Applicable to 4G eNodeB only)*	Records all the activities performed by the remote user on the DUT	Username
			Source (IP address)
			Outcome of event (Success or failure)
			interface type
			Event level (e.g. CRITICAL, MAJOR, MINOR)
			Command/activity performed
			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:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

i. (a)The Group II device 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 Group II device.

ii. The Group II device shall be able to store the generated audit data itself may be with limitations.

iii. The Group II device 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), The Group II device shall have mechanism to store audit data locally. The Group II device 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]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

I. (a) The Group II device shall support forward 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 in a real time for the Group II device. The communication mechanism between the Group II device and the external log server/system should strictly use the secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 "only.

II. The Group II device shall be able to store generated audit data itself, may be with limitations.

III. The Group II device shall alert administrator when its security log buffer reaches configured threshold limit in absence of external system

IV. In the absence of External system, the Group II device shall stop its services when its own security event log buffer is full.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.6.2]

Section 2.6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirements:

The Group II device 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 the Group II device 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 Group II device (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 the security level 2 and above of NIST standard FIPS 140-2 or later.

Vendor shall also submit cryptographic Module testing document and the test results to designated TSTL for scrutiny.

Applicable to 5G gNodeB SA, gNodeB NSA only: 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 Group II device (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 and above of FIPS 140-3 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:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

Cryptographic algorithm implemented inside the Crypto module of the Group II device 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 the Group II device is in compliance with the respective FIPS standards (for the specific crypto algorithm embedded inside the Group II device)"

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

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

Cryptographic algorithms embedded in the crypto module of the Group II device shall be implemented in compliance with respective FIPS standards (for the specific crypto algorithm) Vendor shall also submit cryptographic algorithm implementation testing document and the test results to designated TSTL for scrutiny.

2.6.4 Protecting data and information – Confidential System Internal Data

Requirement:

a) When The Group II device is in normal operational mode (i.e., not in maintenance mode) there shall be no system function that reveals confidential system internal data (eg: PINs, cryptographic keys, passwords, cookies) in the clear text to users and administrators.
b) Access to maintenance mode shall be restricted only to authorized 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 the Group II device 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 Group II device: 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, the Group II device 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 the Group II device to create copy of data for illegal transmission.

The software functions, components in the Group II device 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) The Group II device 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 Group II device.

Applicable to 5G gNodeB SA, gNodeB NSA only: Session logs shall be generated for establishment of any session initiated by either user or Group II device.

2.6.8 Protection against Data Exfiltration - Covert Channel

Requirement:

a) The Group II device 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 Group II device.
c) Session logs shall be generated for establishment of any session initiated by either user or the Group II device system.

Section 2.7: Network Services

2.7.1 Traffic Filtering – Network Level

Requirement:

The Group II device shall provide a mechanism to filter incoming IP packets on any IP

interface. In particular the Group II device 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) *Applicable to 5G gNodeB SA, gNodeB NSA only:* To reset the accounting.

(vi) The Group II device 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:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

The Group II device 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].

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

The Group II device shall support physical and/or logical separation of Operation & Maintenance traffic and control plane traffic complying with the clause 2.3.5 in section 3 of RFC 3871.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.5.1].

2.7.3 Traffic Protection –Anti-Spoofing

Requirement:

The Group II device 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:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

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:

- The Group II device supports the capability described above, and this is stated in the product documentation.
- The Group II device's product documentation states that the capability is not supported and that the Group II device 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:

a) The Group II device shall have protection mechanism against Network level and Application-level DDoS attacks.
b) The Group II device 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:

The Group II device shall act in a predictable way if an overload situation cannot be prevented. The Group II device 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 the Group II device cannot reach an undefined and thus potentially insecure, state.
OEM shall provide a technical description of the Group II device's Overload Control mechanisms (especially whether these mechanisms rely on cooperation of other network elements e.g., RAN)
Applicable to 4G eNodeB only: In an extreme case , a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.

[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:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

The Group II device 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 Group II device. 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:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

It shall be ensured that externally reachable services of the Group II device 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]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

The Group II device shall respond with error messages, anomalous responses, Crash responses when receiving unexpected input request /Malformed input requests.

Vendor should document the list of Protocol stacks supported by Group II device for all traffic planes (Management, Control, Data plane and Service /Application plane).

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.4.4]

2.9.2 Port Scanning

Requirement:

It shall be ensured that on all network interfaces of the Group II device, only documented ports on the transport layer respond to requests from outside the system.

Applicable to 4G eNodeB only: Any attempt to scan the network interface shall lead to triggering of logging of the event with an appropriate parameters like Date & Time stamp, Source IP address, destination IP address etc. The test for this requirement can be verified using a suitable port scanning tool.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.4.2]

2.9.3 Vulnerability Scanning

Requirement:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

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

remediation plan.

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 three 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]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

It shall be ensured that there no known vulnerabilities exist in the Group II device at time of product release. The purpose of vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans are in place to mitigate them) on the Group II device, that can be detected by means of automatic testing tools via the Internet Protocol enabled network interfaces. The test for this requirement can be verified using a suitable Vulnerability scanning tool.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 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 the Group II device from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided.
c) *Applicable to 4G eNodeB only:* Despite the preventive measures, if the said scenario occurs, it shall lead to an event and the event get logged with appropriate message parameters.

[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 Group II device.

The Group II device 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

The Group II device 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

[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:

The Group II device 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 the Group II device 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 Group II devices

Requirement:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

Kernel-based Group II devices that are 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]

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

Appropriate OS hardening procedures including security measures required to ensure the kernel security and miniaturization etc. shall be implemented in Group II devices. Kernel based Group II devices not needed for the operation of the Group II devices shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.]

2.10.6 No automatic launch of removable media

Requirement:

The Group II device 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:

The Group II device shall support mechanisms for buffer overflow protection.

Applicable to 5G gNodeB SA, gNodeB NSA only: 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 the Group II device in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

Applicable to 5G gNodeB SA, gNodeB NSA only: 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:

The Group II device 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:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

The Group II device 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:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

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:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

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, the Group II device 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:
(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

The Group II device 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 Group II device 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.

Applicable to 4G eNodeB only: OEM /TSP shall disable permanently the supported Weaker algorithms other than specified in ITSAR Cryptographic control lists document

[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 Group II device webserver (for both successful as well as failed attempts) shall be logged by the Group II device. 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 wheneverpossible.
- 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 Group II device shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks. The Group II device 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:

The Group II device web server processes shall not 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 the Group II device 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 the Group II device 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 the Group II device 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 Group II device 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 Group II device 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 Group II device web server, and the modules/add-ons used. Default error pages of the Group II device 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 the Group II device 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 Group II device web server's document directory. In particular, the Group II device 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:

(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

To protect user sessions, the Group II device 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, the Group II device 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 Group II device 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 Group II device shall not accept session identifiers from GET/POST variables.
12. The Group II device 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:

(applicable to 5G gNodeB SA, gNodeB NSA only; to be tested on any one of 5G gNodeB SA, gNodeB NSA of Group II)

No provision shall exist for the Group II device System / Root password recovery.

2.12.2 No Password Reset

Requirement:

(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

The Group II device system password reset shall be carried out strictly with appropriate authentication and access control only. In case any unauthorized attempt to reset the Group II Device's system password is successful, then the entire configuration of the Group II device shall be irretrievably deleted.

2.12.3 Secure System Software Revocation

Requirement:

Once the Group II device 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. The Group II device shall support a well-established control mechanism for rolling back to previous software image.

Applicable to 4G eNodeB only: In case roll back is essential, it shall be done only by the administrator with appropriate non-repudiation controls

2.12.4 Software Integrity Check –Installation

Requirement:

The Group II device 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.

2.12.5 Software Integrity Check – Boot

Requirement:
The Group II device 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.

Applicable to 4G eNodeB only: The Group II device shall support the possibility to verify software image integrity at boot time, detecting, for example, software image tampering and/or unauthorized software image updates.

2.12.6 Unused Physical and Logical Interfaces Disabling

Requirement:

The Group II device 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.

2.12.7 No Default Profile

Requirement:

Predefined or default user accounts (other than Admin/Root) in the Group II device shall be deleted or disabled.

2.12.8 Security Algorithm Modification

Requirement:
(applicable to 4G eNodeB only; to be tested only on 4G eNodeB of Group II)

It shall not be possible to modify security algorithms supported by the Group II device through unauthorized access, e.g. to perform a downgrade attack by deceiving the nodes to use a weaker algorithm. The modified list of Security algorithms supported by the Group II device shall strictly fall under the list of crypto controls prescribed in Table1 of the document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0

Annexure-I

Definitions

1. **5G Non-Access Stratum:** Protocols between UE and the core network that are not terminated in the RAN.
2. **Aggregated gNB** means monolithic gNB (NR Node B) which contains DU & CU together.
3. **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.
4. **DDoS:** A distributed denial-of-service attack that renders the victim un-usable by the external environment.
5. **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.
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. **eNodeB:** a Base station which connects UE to 4G Core Network.
8. **gNodeB:** an NR Base Station which connects UE to 5G Core Network.
9. **gNodeB:** an NR Base Station which connects UE to 5G Core Network.
10. **Medium Access Control:** A sub-layer of radio interface layer 2 providing unacknowledged data transfer service on logical channels and access to transport channels.
11. **Mobility:** The ability for the user to communicate whilst moving independent of location.
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-U interface:** New generation user plane interface between eNB and 5G Core network
16. **Non-Access Stratum:** Protocols between UE and the core network that are not terminated in the RAN.
17. **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.
18. **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.
19. **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.
20. **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.

21. **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.
22. **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.
23. **Security:** The ability to prevent fraud as well as the protection of information availability, integrity, and confidentiality.
24. **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.
25. **Transmission or Transport** is the transfer of information from one entity (transmitter) to another (receiver) via a communication path.
26. **Uplink:** An "uplink" is a unidirectional radio link for the transmission of signals from a UE to a base station.
27. **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
ACL	Access Control Lists
AES	Advanced Encryption Standards
AKA	Authentication and Key Agreement
AKA'	AKA Prime
ARP	Address Resolution Protocol/Allocation and Retention Priority
AS	Access Stratum
AuSF	Authentication Server Function
CERT	Computer emergency response teams
CLI	Command Line Interface
CP	Control Plane
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DC	Dual Connectivity
DDoS	Distributed Denial of Service
DL	Downlink
DN	Data Network
DOT	Department of Telecommunications
DRB	Data Radio Bearer
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
ECDSA	Elliptical curved Digital Signature Algorithm
ECS	EDNS Client Subnet
EMS	Element management System
eNB	Evolved Node B (Fourth Generation Base Station)
en-gNB	Enhanced 5G Next Generation Base station
EPC	Evolved Packet Core
EPS	Evolved Packet System
FIPS	Federal Information Processing Standards
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
IPSec VPN	Internet Protocol Security Virtual Private Network
ISO-OSI	International organization of Standardization – Open System Interconnection
ITSAR	Indian Telecom Security Assurance Requirements
MAC-I	Message Authentication Code - Integrity

MC/DC	Modified Condition / Decision Coverage
MD5	Message Digest Algorithm
ME	Mobile Equipment
MeNB	Master eNB
MISRA	Motor Industry Software Reliability Association
MN	Master Node
Mng-eNB	Master ng-eNB
MR	Multi Radio
NAS	Non-Access Stratum
NCCS	National Centre for Communication Security
NEF	Network Exposure Function
NF	Network Function
NG	Next Generation
ng-eNB	Next Generation e-NodeB
NG-RAN	Next Generation Radio Access Network
NIST	National Institute of Standards and Technology
NMS	Network management System
NRF	Network Repository Function
NTP	Network Time Protocol
O&M	Operations and Maintenance
OAM	Operations, Administration, Maintenance
OMC	Operation and maintenance Console
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
RSA	Rivest, Shamir, and Adelman
SASF	Security Assurance Standards Facility
SCG	Secondary Cell Group
Sen-gNB	Secondary en-gNB
SgNB	Secondary gNB
SHA	Secure hash Algorithm
SMF	Session Management Function
SN	Secondary Node
SNMP	Simple Network Management Protocol
SRB	Signalling Radio Bearer
SSH	Secure Shell
TLS	Transport Layer Security
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

List of undertakings to be furnished by the OEM for Group II devices Security testing 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/ No unused Software Packages (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. No unsupported Components (against test case 2.4.2)
7. Avoidance of Unspecified Modes of Access (against test case 2.4.3)
8. Cryptographic Based Secure Communication (against test case 2.6.1)
9. Cryptographic Module Security Assurance (against test case 2.6.2)
10. Cryptographic Algorithms implementation Security Assurance (against test case 2.6.3)

Annexure-IV

References

1. 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.