Indian Telecommunication Security Assurance Requirements (ITSAR)

For

eNodeB (4G Network Access element)

Release Date :

Version : 1.0.0

Enforcement Date :

Security Assurance Standards Facility
National Centre For Communication Security
Department of Telecommunications, Bengaluru-560027

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.

Scope

eNodeB is an access network element in 4G cellular network , which provides connectivity between Mobile equipment and the core network.

The present document contains Indian Telecom Security Assurance Requirements (ITSAR) specific to eNodeB (an access network element in a LTE Network Architecture) with a dedicated hardware and dedicated software which includes Operating System as well as application software i.e ENodeB deployed in Non–virtualised environment.

Table of Contents

Section 1: Access and Authorization

1.1 Management Protocols Mutual Authentication

Requirement:
The protocols used for ENodeB management and maintenance shall support mutual authentication mechanisms only i.e there is mutual authentication of entities for management interfaces on the eNodeB.

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 eNodeB 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]

1.2 .Management Traffic Protection

Requirement:
eNodeB management traffic shall be protected strictly using Secure cryptographic controls prescribed in Table1 of the document " Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 " only.

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.4]

1.3. Role-Based access control

Requirement:
eNodeB 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.
eNodeB 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 eNodeB Management and Maintenance, including authorization of the operation for configuration data and software via the eNodeB console interface.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.6.2]

1.4 User Authentication – Local/Remote

Requirement:

The various user accounts (other than system /admin accounts) on a system shall be protected from misuse. To this end, at least one authentication 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
- 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 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 4.2.3.4.2.1]

1.5 Remote login restrictions for privileged users

Requirement:

Login to eNodeB as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to eNodeB 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 eNodeB.

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

1.6.Authorization Policy

Requirement:

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]

1.7 Unambiguous identification of the user & group accounts removal

Requirement:

Users shall be identified unambiguously by the eNodeB .

eNodeB 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.

eNodeB shall also support assignment of specific ID for individual accounts per user as configured by administrator /root user

eNodeB's all inactive users' accounts shall be locked / permanently disabled.

eNodeB 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: Authentication Attribute Management

2.1 Authentication Policy

Requirement:

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 Authentication Support – External

Requirement

If the eNodeB supports external authentication mechanism such as AAA server (for authentication, authorisation and accounting services) , then the communication between ENodeB 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 document “ Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 “ only.

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

2.3. Protection against brute force and dictionary attacks

Requirement:
A protection against brute force and dictionary attacks that hinder Authentication Attribute guessing shall be implemented in eNodeB.
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 a 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 eNodeB.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.3]

2.4. Enforce Strong Password

Requirement:

a) The configuration setting shall be such that eNodeB 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 eNodeB).It shall not be possible setting this absolute minimum length to a lower value by configuration
(ii) Password shall mandatorily comprises 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 subclause.

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

e) When a user is changing a password or entering a new password , eNodeB /central system checks and ensures that it meets the password requirements stated in this requirement.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3)

2.5 Inactive Session Timeout

Requirement:

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

2.6 Password Changes

Requirement:

a) If a password is used as an authentication attribute, then the eNodeB shall offer a function that enables a user to change his password at any time.

b) When an external centralized system for user authentication is used it is possible to redirect or implement this function on this system.

c) Password change shall be enforced after initial (Default) login.

d) eNodeB shall enforce password change based on password management policy. In particular, it shall enforce password expiry.

e) eNodeB shall support a configurable period for expiry of passwords.

f) Previously used passwords shall not be allowed upto a certain number i.e Password History shall be maintained.

g) The number of disallowed previously used passwords shall be:
   - Configurable;

   - And its default minimum value shall be 3. This means that the ENodeB shall store at least the three previously set passwords. The maximum number of passwords that the E-Node-B can store for each user is up to the manufacturer.

h) When a password is about to expire , a password expiry notification shall be provided to the user.
i) The never expiring password option should be disabled permanently.
j) This requirement shall be met either by eNodeB 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]

2.7 Protected Authentication feedback

Requirement:

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.4]

2.8.Removal of predefined or default authentication attributes

Requirement:
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]

Section 3: Software Security

3.1 Secure Update

Requirement:

eNodeB 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.

eNodeB 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

3.2 Secure Upgrade

Requirement:

(i) eNodeB 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) eNodeB shall allow upgrades only if code signing certificate is valid and not time expired. To this end, eNodeB shall have a list of public keys or certificates of authorised 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) eNodeB 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.3.5]

.

3.3 Source code security assurance

Requirement:

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 eNodeB

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 eNodeB Software, which includes vendor developed code, third party software and open source code libraries used/embedded in the eNodeB

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

3.4 Known Malware and backdoor Check

Requirement:

Vendor shall submit an undertaking stating that E- Node – B is free from all known malware and backdoors on the date of product release and shall submit Malware Test Document (MTD) of the eNodeB to the designated TSTL.

3.5.No unused software packages

Requirement:

Software components / packages or parts of software packages which are not needed for operation or functionality of the eNodeB shall not be present.

Orphaned software components /packages shall not be present in eNodeB.

[Reference: TSDSI STD T1.3GPP 33.117 -14.2.0 V.1.0.0. Section 4.3.2.3]

3.6 In secure secure services/ protocols Removal

Requirement:

eNodeB shall run only those protocol handlers and services which are needed for its operation and which do not have any known security vulnerabilities

eNodeB 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 E-Node –B by the vendor

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.1]

3.7 Restricting System Boot Source

Requirement:

eNodeB shall boot only from memory devices intended for this purpose

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.3.2]

3.8 Secure Time Synchronization

Requirement:

eNodeB shall provide reliable time and date information provided manually by itself or through NTP/PTP server.

eNodeB shall establish secure communication channel 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 “ with the NTP/PTP server.

eNodeB shall generate audit logs for all changes to time settings.

3.9 Restricted reachability of services

Requirement:

The eNodeB 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.

[Reference: TSDSI STD T1.3GPP 33.117-1 4.2.0 V.1.0.0 Section 4.3.2.2]

3.10 Avoidance of Unspecified Wireless Access

Requirement:

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]

3.11. Disable all software based reset options

Requirement:

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

3.12. Disable USB stick detection

Requirement:

eNodeB System shall restrict users from using USB stick to protect and secure data from stealing .

3.13. Lock Down Cron Jobs

Requirement:

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.

3.14. Change of SSH Port

Requirement:

E-Node-B'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 4: System Secure Execution Environment

4.1 No unused functions

Requirement:
Unused functions i.e the software and/or hardware functions which are not needed for operation or functionality of the eNodeB shall not be present in the eNodeB software and/or hardware.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.4]

4.2 No unsupported components

Requirement:
Vendor to ensure that the eNodeB shall not contain software and/or hardware components that are no longer supported by Vendor or its 3rd Parties including the open source communities , such as components that have reached end-of-life or end-of-support.
[
Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.3.2.5]

Section 5:User Audit

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.

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

5.2 Audit Event Generation

Requirement:

The eNodeB shall log all important Security events with unique System Reference details as given in the Table below.
eNodeB shall record within each audit record atleast 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 :
Table :

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

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

		Outcome of event (Success or failure)
		• Timestamp.
Resetting Passwords (Optional)	Resetting of user account passwords by the Administrator	• Administrator username,
		• Administered account,
		• Activity performed (configure, delete, enable and disable)
		Outcome of event (Success or failure)
		• Timestamp
Services (Optional)	Starting and Stopping of Services (if applicable)	Service identity
		Activity performed (start, stop, etc.)
		Timestamp
		Outcome of event (Success or failure)
User login (Mandatory)	All use of identification and authentication mechanism	user identity
		origin of attempt (e.g.IP address)
		Timestamp
		outcome of event (Success or failure)
X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
		Reason for failure
		Subject identity
		Type of event
Secure Update (Optional)	attempt to initiate manual update, initiation of update, completion of update	user identity
		Timestamp
		Outcome of event (Success or failure)
		Activity performed
Time change(Mandatory)	Change in time settings	old value of time
		new value of time
		Timestamp
		origin of attempt to change time (e.g.IP address)
		Subject identity
		outcome of event (Success or failure)
		user identity

Session unlocking/ termination (Optional)	Any attempts at unlocking of an interactive session, Termination of a remote session by the session locking mechanism, Termination of an interactive session	user identity (wherever applicable)
		Timestamp
		Outcome of event (Success or failure)
		Subject identity
		Activity performed
		Type of event
Trusted Communication paths(with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorised remote administrators) (Optional)	Initiation, Termination and Failure of trusted Communication paths	Timestamp
		Initiator identity (as applicable)
		Target identity (as applicable)
		User identity (in case of Remote administrator access)
		Type of event
		Outcome of event (Success or failure, as applicable)
access to personal data (Mandatory)	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)
Audit data changes(Optional)	Changes to audit data including deletion of audit data	Timestamp
		Type of event (audit data deletion, audit data modification)
		Outcome of event (Success or failure, as applicable)
		Subject identity
		user identity
		origin of attempt to change time (e.g.IP address)
		Details of data deleted or modified
All activities of the remote user other than Root User (Mandatory)	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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.3.6.1 & Section 4.2.3.2.5]

5.3.Secure Log Export

Requirement:
(I) (a) The eNodeB 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 realtime for the E-Node B . The communication mechanism between the eNodeB 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) ENodeB shall be able to store generated audit data itself, may be with limitations.
(III) eNodeB shall alert administrator when its security log buffer reaches configured threshold limit in absence of external system
(IV) In the absence of External system, eNodeB 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 6: Data Protection

6.1 Cryptographic Based Secure Communication with connecting entities

Requirement :

eNodeB shall Communicate with the connected entities 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.

Vendor shall give to TSTL , the list of the connected entities with ENodeB and the method of communication with each entity with details of interface , Protocol stack implemented , configuration, detailed procedure of establishing the communication by ENodeB with each entity and any other details required for testing this requirement.

6.2. Cryptographic Module Security Assurance

Requirement :

Cryptographic module embedded inside the eNodeB (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.

6.3. Cryptographic Algorithms implementation Security Assurance

Requirement :

Cryptographic algorithms embedded in the crypto module of ENodeB 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.

6.4. Protecting data and information – Confidential System Internal Data

Requirement:

a) When eNodeB 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 to users and administrators.

b) Access to maintenance mode shall be restricted only to authorised privileged user.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.2.2.]

6.5. Protecting data and information in storage

Requirement :

a) For sensitive data (eg: PINs, cryptographic keys, passwords, cookies) in storage (persistent or temporary) , read access rights shall be restricted.
b) Files of eNodeB system that are needed for the functionality shall be protected against manipulation 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 " with appropriate non-repudiation controls.
c) 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 document " Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 " .
(iii)Stored files: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table1 of the document " Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 "only.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.]

6.6 Protection against Copy of Data

Requirement :

a) eNodeB shall not create a copy of data in use and data in transit.
b) Protective measures shall exist against use of available system functions / software residing in eNodeB to create copy of data for illegal transmission.
c) The software functions, components in the eNodeB for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

6.7 Protection against Data Exfiltration - Overt Channel

Requirement:

a) eNodeB shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.
b) . Establishment of outbound overt channels shall not be allowed and not configured to be used in the E-Node –B .

6.8 Protection against Data Exfiltration - Covert Channel

Requirement :

a) eNodeB 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 shall not be allowed if they are initiated/originated automatically from the eNodeB i.e the e NodeB shall not have a session or process established/initiated without a configured user or a system user.
c) Session logs shall be generated for establishment of any session initiated by either user or eNodeB system

Section 7: Network Services

7.1 Traffic Filtering – Network Level

Requirement:

a) eNodeB shall provide a mechanism to filter incoming IP packets on any IP interface

   (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 any portion of the protocol header.

b) The eNodeB shall provide a mechanism to disable/enable each defined rule.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.6.2.1]

7.2 Traffic Separation

Requirement:

eNodeB 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].

7.3. Traffic Protection –Anti-Spoofing

Requirement:

eNodeB shall not process IP packets if their source address is not reachable via the incoming interface. This feature can be implemented in several ways like use of IPsec, TLS , "Reverse Path Filter" (RPF).

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.3.1.1]

Section 8: Attack Prevention Mechanisms

8.1 Network Level and application level DDoS

Requirement:

a) eNodeB shall have protection mechanism against known network level and Application level DDoS attacks.

b) eNodeB shall have 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 an 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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.3.3.1]

8.2.Excessive Overload Protection

Requirement:

eNodeB shall act in a predictable way if an overload situation cannot be prevented. eNodeB 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 cases, it shall be ensured that eNodeB shall not reach an undefined and thus potentially insecure, state. In an extreme case , a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . section 4.2.3.3.3]

Section 9: Vulnerability Testing Requirements

9.1 Fuzzing – Network and Application Level

Requirement:

E-Node –B 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 E-Node –B 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]

9.2 Port Scanning

Requirement:

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

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]

9.3. Vulnerability Scanning

Requirement:

It shall be ensured that there no known vulnerabilities exist in the eNodeB 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 eNodeB, 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 10: Operating System

10.1 Growing Content Handling

Requirement:

a) Growing or dynamic content on eNodeB shall not influence system functions.
b) A file system that reaches its maximum capacity shall not stop eNodeB from operating properly. Suitable counter measures shall be taken to ensure that this scenario is avoided.
c) Despite the preventive measures , if the said scenario occurs , it shall lead to an event and the event gets logged with appropriate message parameters.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.4.1.1.1]

10.2 Handling of ICMP

Requirement:

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

eNodeB 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	129	Echo Reply	Optional (i.e. as automatic reply to "Echo Request")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	128	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	Neighbour Solicitation	Permitted	Permitted
N/A	136	Neighbour Advertisement	Permitted	N/A

eNodeB shall not respond to, or process (i.e. do changes to configuration), under any circumstances certain ICMP message types as marked in 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 request	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	Not Permitted

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.4.1.1.2.]

10.3 Authenticated Privilege Escalation only

Requirement:

eNodeB 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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.4.1.2.1]

10.4. System account identification

Requirement:

Each system account in eNodeB shall have a unique identification with appropriate non-repudiation controls.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.4.2.2]

10.5 OS Hardening

Requirement:
Appropriate OS hardening procedures including security measures required to ensure the kernel security and miniaturization etc. shall be implemented in eNodeB. Kernel based network functions not needed for the operation of the eNodeB shall be deactivated.

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

10.6 No automatic launch of removable media

Requirement:

eNodeB shall not automatically launch any application when removable media device is connected.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.3.3.1.3]

10.7 Protection from buffer overflows

Requirement:

eNodeB shall support mechanisms for buffer overflow protection.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.3.3.1.5]

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 eNodeB in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.6]

10.9 File-system Authorization privileges

Requirement:

eNodeB 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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.7]

Section 11: Web Servers

This entire section of the security requirements is applicable when the eNodeB supports web management interface .

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 document " Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 " only.

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . section 4.2.5.1]

11.2 Webserver logging

Requirement:
Access to the eNodeB webserver (both successful as well as failed attempts) shall be logged by eNodeB.
The web server log shall contain the following information:
- Access timestamp
- Source (IP address)
- Account (if known)
- Attempted login name (if the associated account does not exist)
- Relevant fields in http request. The URL should be included whenever possible.

- Status code of web server response

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0.section 4.2.5.2.1]

11.3 HTTPS input validation

Requirement:

The eNodeB shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.
eNodeB 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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.4]

11.4 No system privileges

Requirement:

eNodeB web server processes shall not run with system privileges.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.2]

11.5 No unused HTTPS methods

Requirement:

HTTPS methods that are not required for the operation of eNodeB shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.3]

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 eNodeB operation.

In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . section 4.3.4.4]

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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0.section 4.3.4.5]

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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.6]

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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.7]

11.10 Access rights for web server configuration

Requirement:
Access rights for eNodeB web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.8]

11.11 No default content
Requirement:
Default content that is provided with the standard installation of the E-Node -B web server shall be removed.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.9]

11.12 No directory listings

Requirement:

Directory listings (indexing) / "Directory browsing" shall be deactivated.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.10]

11.13 Web server information in HTTPS headers

Requirement:

The HTTPS header shall not include information on the version of the eNodeB web server and the modules/add-ons used.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.11]

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 eNodeB web server and the modules/add-ons used.
Default error pages of the eNodeB web server shall be replaced by error pages defined by the vendor.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.12]

11.15 Minimized file type mappings

Requirement:

File type or script-mappings that are not required for E-Node B operation shall be deleted.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.13]

11.16. Restricted file access

Requirement:

Restrictive access rights shall be assigned to all files which are directly or indirectly reside in the eNodeB web server's document directory.

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.14]

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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.15]

Section 12: Other Security requirements

12.1. Remote Diagnostic Procedure – Verification (Dropped)

If the E-Node –B is providing Remote access for troubleshooting purposes/alarm maintenance, then it shall be allowed only for authorized users , other than the root user.

All activities performed by the remote user are to be logged with the following parameters:
1. User id
2. time stamp
3. interface type
4. Event level (e.g. CRITICAL, MAJOR, MINOR)
5. Command/activity performed and
6. Result type (e.g. SUCCESS, FAILURE).

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

12.2 No Password Reset

Requirement:

eNodeB system password reset shall be carried out strictly with appropriate authentication and access control only.

In case any unauthorized attempt to reset the eNodeB's system password is successful, then the entire configuration of the eNodeB shall be irretrievably deleted.

12.3 Secure System Software Revocation

Requirement:

Once the eNodeB's software image is legally updated/ upgraded with New Software Image , it shall not be possible to roll back to a previous software image.
In case roll back is essential, it shall be done only by the administrator with appropriate non-repudiation controls.

In case roll back is essential, it shall be done only by the administrator with appropriate non-repudiation controls.

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

12.4 Software Integrity Check – Installation

Requirement:

eNodeB shall validate the software package integrity before the installation/upgrade stage 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 .

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

12.5 Software Integrity Check – Boot

Requirement:

eNodeB 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 document " Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 " to the expected reference value.

eNodeB shall support the possibility to verify software image integrity at boot time, detecting, for example, software image tampering and/or unauthorized software image updates.

12.6 Unused Physical and Logical Interfaces Disabling

Requirement:

eNodeB shall support the mechanism to verify both the physical and logical interfaces exist in the product.

Physical and logical accessible Interfaces which are not under use shall be disabled.

12.7. No Default Profile

Requirement:

Predefined or default user accounts in eNodeB shall be deleted or disabled

12.8 Security Algorithm Modification

Requirement:

It shall not be possible to modify security algorithms supported by E-Node –B 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 ENodeB 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

Section 13 : eNodeB specific security requirements (3GPP 33.216)

13.1. Control plane data confidentiality protection

Requirement:

The eNodeB shall provide confidentiality protection for control plane packets on the S1/X2 reference points.

[Reference: 3GPP TS 33.216 V16.1.0 (2019-09) Section 4.2.2.1.1]

13.2 . Control plane data integrity protection

Requirement:

The eNodeB shall provide integrity protection for control plane packets on the S1/X2 reference points.

[Reference: 3GPP TS 33.216 V16.1.0 (2019-09) Section 4.2.2.1.2]

13.3. User plane data ciphering and deciphering at eNodeB

Requirement:
The eNodeB shall cipher and decipher user plane packets between the Uu reference point and the S1/X2 reference points
[Reference: 3GPP TS 33.216 V16.1.0 (2019-09) Section 4.2.2.1.3]

13.4. User plane data integrity protection

Requirement:
The eNodeB shall handle integrity protection for user plane packets for the S1/X2 reference points.
[Reference: 3GPP TS 33.216 V16.1.0 (2019-09) Section 4.2.2.1.4]

13.5. AS algorithms selection

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

"Each eNodeB shall be configured via network management with lists of algorithms which are allowed for usage. There shall be one list for integrity algorithms, and one list for ciphering algorithms. These lists shall be ordered according to a priority decided by the operator.
[Reference: 3GPP TS 33.216 V16.1.0 (2019-09) Section 4.2.2.1.5]

13.6. Verify RRC integrity protection

Requirement **:**
The supervision of failed RRC integrity checks shall be performed in the eNodeB. In case of failed integrity check (i.e. faulty or missing MAC-I) is detected after the start of integrity protection, the concerned message shall be discarded.
[Reference: 3GPP TS 33.216 V16.1.0 (2019-09) Section 4.2.2.1.6]

13.7. The selection of EIA0

Requirement :

EIA0 is only allowed for unauthenticated emergency calls
[Reference: 3GPP TS 33.216 V16.1.0 (2019-09) Section 4.2.2.1.7]

13.8. Key refresh at eNodeB

Requirement :
Key refresh shall be possible for K_{eNodeB}, $K_{RRC\text{-}enc}$, $K_{RRC\text{-}int}$, $K_{UP\text{-}int}$, and $K_{UP\text{-}enc}$ and shall be initiated by the eNodeB when a PDCP COUNTs is about to be re-used with the same Radio Bearer identity and with the same K_{eN}.

[Reference: 3GPP TS 33.216 V16.1.0 (2019-09) Section 4.2.2.1.8]

13.9. AS Security Mode Command Procedure

Requirement :
The eNodeB shall protect the SECURITY MODE COMMAND message with the integrity algorithm, which has the highest priority according to the ordered lists.
[Reference: 3GPP TS 33.216 V16.1.0 (2019-09) Section 4.2.2.1.9]

13.10. Bidding down prevention in X2-handovers

Requirement:

In the path-switch message, the target eNodeB shall send the UE EPS security capabilities received from the source eNodeB to the MME.
[Reference: 3GPP TS 33.216 V16.1.0 (2019-09) Section 4.2.2.1.10]

13.11. AS protection algorithm selection in eNodeB change

Requirement:
The target eNodeB shall select the algorithm with highest priority from the UE EPS security capabilities according to the prioritized locally configured list of algorithms (this applies for both integrity and ciphering algorithms). The chosen algorithms shall be indicated to the UE in the handover command if the target eNodeB selects different algorithms compared to the source eNodeB.
[Reference: 3GPP TS 33.216 V16.1.0 (2019-09) Section 4.2.2.1.11]

13.12. RRC and UP downlink ciphering at the eNodeB

Requirement:

The eNodeB shall start RRC and UP downlink ciphering after sending the AS security mode command message.

[Reference: 3GPP TS 33.216 V16.1.0 (2019-09) Section 4.2.2.1.12]

ABBREVIATIONS

AES	Advanced Encryption Standard
AAA Server	Authentication, Authorization, and Accounting Server
ACL	Access Control Lists
AES	Advanced Encryption Standard
CERT	Computer emergency response teams
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DDOS	Distributed Denial of Service
NE	Network Element
EMS	Element management System
FIPS	Federal Information Processing Standards
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IPSec VPN	Internet Protocol Security Virtual Private Network
MC/DC	Modified Condition / Decision Coverage
MD5	Message Digest Algorithm
MISRA	Motor Industry Software Reliability Association
NIST	National Institute of Standards and Technology
NMS	Network management System
NTP	Network Time Protocol
OMC	Operation and maintenance Console
OS	Operating System
DOT	Department of Telecommunications
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
ECDSA	Elliptical curved Digital Signature Algorithm
HTTPS	Hypertext Transfer Protocol Secure
IPSec	Internet Protocol Security
ITSAR	Indian Telecom Security Assurance Requirements
NCCS	National Centre For Communication Security
RSA	Rivest, Shamir, and Adelman
SASF	Security Assurance Standards Facility
SHA	Secure hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TLS	Transport Layer Security