Indian Telecom Security Assurance Requirements (ITSAR)

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

Group-I Devices
Common Security Requirements ITSAR

ITSAR Number: ITSAR702012504
ITSAR Name: NCCS/ITSAR/Standards Applicable for Group of Equipment/CSR Group of Devices/Group-I Devices-V1.0.0

Date of Release: 21.04.2025 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-I Devices Common Security Requirements ITSAR	**ITSAR702012504**	1.0.0	21.04.2025	First release

Table of Contents

A) Outline

This Indian Telecom Security Assurance Requirement (ITSAR) document specifies Common Security Requirements for Group-I 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 I contains ITSARs of twenty-three 5G network functions viz., the network function AMF (Access and Mobility Management Function), AUSF (Authentication Server Function), NWDAF (Network Data Analytics Function), NEF (Network Exposure Function), NRF (Network Repository Function), N3IWF (Non-3GPP Interworking Function), SEPP (Security Edge Protection Proxy), SCP (Service Communication Proxy), SMF (Session Management Function), UDM (Unified Data Management), UPF (User Plane Function), BSF (Binding Support Function), CHF (Charging Function), LMF-GMLC (Location Management Function/Geographic Mobile Location Center), SMSF (Short Message Service Function), UDR (Unified Data Repository), UDSF (User Data Storage Function), EIR (Equipment Identity Register), NSACF (Network Slice Admission Control Function), UCMF (Unified Charging Management Function), AF (Application Function), NSSF (Network Slice Selection Function) and PCF (Policy Control Function).

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 I devices.

B) Scope

This document defines Common Security Requirements for Indian Telecom Security Assurance Requirements (ITSARs) of Group I devices (Twenty Three Network functions -AMF, AUSF, NWDAF, NEF, NRF, N3IWF, SEPP, SCP, SMF, UDM, UPF, BSF, CHF, LMF-GMLC, SMSF,UDR,UDSF, EIR, NSACF, UCMF,AF, NSSF and PCF).

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 to 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 I 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 functions. 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 endeavour 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 I device ITSARs.

Chapter- 2 Common Security Requirements

Section 2.1 Access and Authorization

2.1.1. Management Protocols Mutual Authentication/Authentication for Product Management and Maintenance interfaces

Requirement:

The Group I device management 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 Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" shall only be used for the network function management and maintenance.

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

2.1.2. Management Traffic Protection

Requirement:

The network function management traffic shall be protected strictly using secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Ref: 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:

The network function 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 network function supports RBAC with minimum of 3 user roles for OAM privilege management for the network function Management and Maintenance, including authorization of the operation for configuration data and software via the network product console interface.

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

Note: The reference to Console interface may not be applicable here for GVNP Models of Type 1& 2

2.1.4. User Authentication – Local/Remote

Requirement:

The various user and machine accounts on a system shall be protected from misuse. To

this end, an authentication attribute is typically used, which, when combined with the username, enables unambiguous authentication and identification of the authorized user.

Authentication attributes include
- Cryptographic keys
- Token
- Passwords

This means that authentication based on a parameter that can be spoofed is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker. Minimum two of the above Authentication attributes shall be mandatorily combined for protecting all the accounts from misuse. An exception to this requirement is local access and machine accounts where at least one authentication attribute shall be supported.

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

Note: Local interface may not be applicable here for GVNP Models of Type 1& 2

2.1.5. Remote login restrictions for privileged users

Requirement:

Direct Login to the network function 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 network function remotely.
This remote root user access restriction is also applicable to application software's / tools such as TeamViewer, desktop sharing which provide remote access to the network function.

This clause may not be applicable to GVNP Type-1

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

2.1.6. Authorization Policy

Requirement:

The authorizations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform.
Authorizations to a system shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Suitable authorizations shall also be assigned for access to files that are components of the operating system or of applications or that are generated by the same (e.g. configuration and logging files). Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications should not be executed with administrator or system rights.

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

2.1.7. Unambiguous identification of the user & group accounts removal

Requirement:

Users shall be identified unambiguously by the network function.
The network function 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 network function shall not enable the use of group accounts or group credentials, or sharing of the same account between several users.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.1.2]

Section 2.2 Authentication Attribute Management

2.2.1. Authentication Policy

Requirement:

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

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

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

2.2.2. Authentication Support – External

Requirement:

If the network function supports external authentication mechanism such as AAA server (for authentication, authorization and accounting services), then the communication between The network function and the external authentication entity shall be protected using the authentication and related service protocols built strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

2.2.3. Protection against brute force and dictionary attacks

Requirement:

A protection against brute force and dictionary attacks that hinder authentication attribute guessing shall be implemented in the network function.
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 network function. An exception to this requirement is machine accounts.

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

2.2.4. Enforce Strong Password

Requirement:

a) The configuration setting shall be such that the network function 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 network function). 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 network function.
e) When a user is changing a password or entering a new password, The network function /central system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.).

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

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

2.2.5. Inactive Session timeout

Requirement:

An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period.
The network function 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 set between 2 to 5 minutes.

[Ref: 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 network functions PCF, UDR, NSACF, EIR, UCMF, CHF, LMF-GMLC, SMSF, BSF, UDSF only; to be tested on any one of these network functions: PCF, UDR, NSACF, EIR, UCMF, CHF, LMF-GMLC, SMSF, BSF, UDSF network functions of Group I)

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.
Group I devices shall monitor inactive sessions of administrative login users and initiate session locking mechanism based on pre-configured timers. Unlocking the session shall be permissible only by user authentication. If the inactivity period further continues for a defined period, session /user ID timeout must occur after this inactivity.
Reauthentication of the OAM user shall be repeated following any period of inactivity lasting 15 minutes or longer.

[Ref :TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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 network function shall enforce password change based on password management policy.
In particular, the system shall enforce password expiry. The network function shall support a configurable period for expiry of passwords.
Previously used passwords shall not be allowed upto 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 network function shall store at least the three previously set passwords. The maximum number of passwords that the network function can store for each user is up to the manufacturer.

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

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

The network function 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 network function.

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

2.2.7. Protected Authentication feedback

Requirement:

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

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

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

2.2.8. Removal of predefined or default authentication attributes

Requirement:

Predefined or default authentication attributes shall be deleted or disabled (or changed). Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, OEM or developer of a system. Such authentication attributes shall be changed by automatically forcing a user to change it on 1st time login to the system or the OEM provides instructions on how to manually change it.

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

2.2.9. Logout function

Requirement:

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

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

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

2.2.10. Policy regarding consecutive failed login attempts

Requirement:

a) The maximum permissible number of consecutive failed user account login attempts should be configurable by the operator. The definition of the default value set at manufacturing time for the maximum number of failed user account login attempts shall be less than or equal to 8, typically 5. After the maximum permissible number of consecutive failed user account login attempts is exceeded by a user, there shall be a block delay in allowing the user to attempt login again. This block delay and the capability to set the period of the block delay, e.g., double the delay, or 5 minutes delay, or 10 minutes delay, after each login failure should be configurable by the operator. The default value set at manufacturing time for this delay shall be greater than or equal to 5 sec.
b) If supported, infinite (permanent) locking of an account that has exceeded the maximum permissible number of consecutive failed user account login attempts should also be possible via configuration, with the exception of administrative accounts, which shall get only temporarily locked.

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

2.2.11. Suspend accounts on non-use

(applicable to network functions BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF, AF, PCF only; to be tested on any one of these network functions: BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF, AF, PCF network functions of Group I)

Requirement:

It shall be possible for the system to automatically suspend an account after 'X' days without a valid login.
Note: X may be specified by operator. It can be implemented centrally also.

[Ref: CIS Password Policy Guide]

Section 2.3 Software Security

2.3.1. Secure Update

Requirement:

a) Software package integrity shall be validated during software update stage.
b) The network function shall support software package integrity validation via cryptographic means, e.g. digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only. To this end, the network product 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.
c) Tampered software shall not be executed or installed if integrity check fails.
d) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software update, and modify the list mentioned in bullet b.

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

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

2.3.2. Secure Upgrade

Requirement:

a) Software package integrity shall be validated during software upgrade stage.
b) The network function shall support software package integrity validation via cryptographic means, e.g. digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only. To this end, the network product 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.
c) Tampered software shall not be executed or installed if integrity check fails.
d) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade, and modify the list mentioned in bullet b.

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

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

2.3.3. Source code security assurance

Requirement:

a) OEM shall follow best security practices including secure coding for software development. Source code shall be made available either at TSTL premises or at the mutually agreed location for source code review by the designated TSTL. It may be supported by furnishing the Software Test Document (STD).
b) Also, OEM shall submit the undertaking as below:
   (i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the network function Software which includes OEM developed code, third party software and opensource code libraries used/embedded in the network function.
   (ii) The network function software shall be free from CWE top 25, OWASP top 10 security vulnerabilities and OWASP top 10 API Security vulnerabilities as on the date of latest release of product or three months prior to the date of offer of product for testing, whichever is latest. For security weaknesses, vulnerabilities identified or discovered during the interim period, OEM shall give mitigation plan.
   (iii) The binaries for the network function and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

[Ref : https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html]
[Ref : https://owasp.org/www-project-top-ten/]
[Ref : https://owasp.org/www-project-api-security/]

2.3.4. Known Malware and backdoor Check

Requirement:

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

2.3.5. No unused software

Requirement:

Software components or parts of software which are not needed for operation or functionality of the network function shall not be present.
Orphaned software components /packages shall not be present in the network function.
OEM shall provide the list of software that are necessary for the network function's operation.
In addition, OEM shall furnish an undertaking as "The network function does not contain Software that is not used in the functionality of the network function."

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

2.3.6. Unnecessary Services Removal

Requirement:

The network function 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 network function 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 network function and their purpose needs to be provided by the OEM as prerequisite for the test case.

[Ref: 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 network function can boot only from the memory devices intended for this purpose.

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

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

2.3.8. Secure Time Synchronization

Requirement:

The network function shall establish secure communication channel with the NTP/PTP server.
The network function shall establish secure communication channel strictly using Secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" with NTP/PTP server.
The network function shall generate audit logs for all changes to time settings.

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

[Ref : RFC 8915 - Network Time Security for the Network Time Protocol (NTP).]

2.3.9. Restricted reachability of services

Requirement:

The network function shall restrict the reachability of services such that they can be reached only on interfaces meant for the purpose. On interfaces where services are active, the reachability should be limited to legitimate communication peers.

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

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

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

2.3.10. Self-Testing

Requirement:

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

In case cryptographic module remains in error state, the network functions shall not carry out any operations.

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 network function shall be deactivated in the network function's software and/or hardware.

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

The list of hardware and software functions installed in the system shall match with the ones that have been mentioned and deemed necessary for the operation of the network function.

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

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

Note: The reference to hardware may not be applicable here for GVNP Models of Type 1& 2.

2.4.2. No unsupported components

Requirement:

OEM to ensure that the network function shall not contain software and hardware components that are no longer supported by them or their 3rd Parties including the opensource communities, such as components that have reached end-of-life or end-of-support. An undertaking in this regard shall be given by OEM.

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

Note: The reference to hardware may not be applicable here for GVNP Models of Type 1& 2.

2.4.3. Avoidance of Unspecified mode of Access

Requirement:

The network function shall not contain any wireless access mechanism which is unspecified or not declared. An undertaking shall be given by the OEM as follows:

"The network function 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 accessing controlled (file access rights) so only privileged users have access to the log files.

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

2.5.2. Audit Event Generation

Requirement:

The network function shall log all important Security events with unique System Reference details as given in the Table below:

The network function 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:

S. no	Event Type or (Mandatory optional)	Description	Event data to be logged
1	Incorrect login attempts (Mandatory)	Records any user incorrect login attempts to the network function.	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,	Administrator username
			Administered account
			Activity performed (configure, delete, enable and disable)

		copy, 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 network function that forces a reboot or shutdown OR where the network device/The network function has crashed.	Action performed (boot, reboot, shutdown, etc.)
			Username (for intentional actions)
			Outcome of event (Success or failure)
			Timestamp
7	Interface status change (Mandatory)	Change to the status of interfaces on the network device/The network function (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			Service identity

	Services (Optional)	Starting and Stopping of Services (if applicable)	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, 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
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			Timestamp

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

[Ref: 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:

a) The network function shall support forwarding of security event logging data to an external system available in redundant configuration by push or pull mechanism through diverse links.
b) Log functions should support secure uploading of log files to a central location or to a system external for the network function.
c) The network function shall be able to store the generated audit data locally. The memory for this purpose shall be dimensioned to cater for the continuous storage of two days of audit data. OEM shall submit justification document for sufficiency of local storage requirement.
d) Secure Log export shall comply the secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

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

2.5.4. Logging access to personal data

Requirement:

In some cases, access to personal data in a clear text might be required. If such access is required, access to this data shall be logged, and the log shall contain who accessed what data without revealing personal data in clear text. When for practical purposes, such logging is not available, a coarser grain logging is allowed. In some cases, the personal data stored in the log files may allow the direct identification of a subscriber. In such cases, the revealed personal information may not expose the subscriber to any kind of privacy violation.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.5]

Section 2.6 Data Protection

2.6.1. Cryptographic Based Secure Communication

Requirement:

The network function shall Communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table 1 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 network function and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration, detailed procedure of establishing 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 network function (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards.

Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format.

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

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

2.6.3. Cryptographic Algorithms implementation Security Assurance

Requirement:

Cryptographic algorithm implemented inside the Crypto module of the network function 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.

An undertaking is to be submitted by the OEM mentioning that "Cryptographic algorithms implemented inside the Crypto module of the network function is in compliance with the respective FIPS standards (for the specific crypto algorithm embedded inside the network function)."

2.6.4. Protecting data and information – Confidential System Internal Data

Requirement:

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

[Ref: 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 network function system that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table 1 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 authentication. 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 Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.
    (iii) Stored files in the network function: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Ref: 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 & authorization and except for specified purposes, the network function shall not support copying of control plane and user plane data.
b) Protective measures should exist against use of available system functions / software

residing in the network function to create copy of control plane and user plane data for illegal transmission.

2.6.7. Protection against Data Exfiltration - Overt Channel

Requirement**:**

a) The network function shall have mechanisms to prevent data exfiltration attacks for theft of control plane and user plane 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 network function.
c) Session logs shall be generated for establishment of any session initiated by either user or the network function.

2.6.8. Protection against Data Exfiltration - Covert Channel

Requirement:

a) The network function shall have mechanisms to prevent data exfiltration attacks for theft of control plane and user plane 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 network function.
c) Session logs shall be generated for establishment of any session initiated by either user or the network function system.

2.6.9. System robustness against unexpected input

(applicable to network functions BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF only; to be tested on any one of these network functions: BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF network functions of Group I)

Requirement:

During transmission of data to a system it is necessary to validate input to network function before processing. This includes all data which is sent to the system. Examples of this are user input, inputs from network function's NF consumers - UDM, PCF and NEF, values in arrays and content in protocols. The following typical implementation error shall be avoided:

a) No validation on the lengths of transferred data
b) Incorrect assumptions about data formats
c) No validation that received data complies with the specification
d) Insufficient handling of protocol errors in received data
e) Insufficient restriction on recursion when parsing complex data formats
f) White listing or escaping for inputs outside the values margin

[Ref : TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. section 4.2.3.3.4]

2.6.10. Security of backup data

(applicable to network functions BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF only; to be tested on any one of these network functions: BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF network functions of Group I)

Requirement:

The network function shall support secure mechanisms for taking backup of sensitive data, configuration, and log files. An effective backup strategy shall be in place and documented.

[Ref : "Security Guidance for 5G Cloud Infrastructure Part III: Data Protection" by NSA & CISA]

2.6.11. Secure deletion of sensitive data

(applicable to network functions BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF only; to be tested on any one of these network functions: BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF network functions of Group I)

Requirement:

The network function shall support secure deletion of sensitive data by authorized user in such a manner that it cannot be recovered through any forensic means.

Section 2.7 Network Services

2.7.1. Traffic Filtering – Network Level Requirement

Requirement:

The network function shall provide a mechanism to filter incoming IP packets on any IP interface (Refer to RFC 3871). In particular the network function shall provide a mechanism:

a) To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of the stack ISO/OSI.
b) 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.
c) To enable/disable for each rule the logging for Dropped packets, i.e. details on messages matching the rule for troubleshooting.
d) To filter on the basis of the value(s) of source IP, destination IP and port addresses of protocol header.
e) To reset the accounting.
f) The network function shall provide a mechanism to disable/enable each defined rule.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.6.2.1, RFC 3871 – Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.2. Traffic Separation

Requirement:

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

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.5.1 RFC 3871 – Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure].

2.7.3. Traffic Protection –Anti-Spoofing

Requirement:

The network function shall not process IP Packets if their source address is not reachable via the incoming interface. Implementation example: Use of "Reverse Path Filter" (RPF) provides this function.

[Ref: 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-C Filtering (when 5GC is interworking with EPC)

(applicable to network functions AMF, AuSF, NWDAF, NEF, NRF, N3IWF, SEPP, SCP, SMF, UDM, UPF, CHF only; to be tested on any of these network functions: AMF, AuSF, NWDAF, NEF, NRF, N3IWF, SEPP, SCP, SMF, UDM, UPF, CHF network functions of Group I)

Requirement:

The following capability is conditionally required:

- For each message of a GTP-C-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 network function supports the capability described above, and this is stated in the product documentation.
- The network function's documentation states that the capability is not supported and that the network function needs to be deployed together with a separate entity that

provides the capability described above.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.6.2.3]

2.7.5. GTP-U Filtering

(applicable to network function UPF only; to be tested only on UPF network function of Group I)

Requirement:

The following capability is conditionally required:
For each message of a GTP-U-based protocol, it shall be possible to check whether the sender of this message is authorized to send a message pertaining to this protocol.
At least the following actions should be supported when the check is satisfied:

- Discard: the matching message is discarded.
- Accept: the matching message is accepted.
- Account: the matching message is accounted for, i.e., a counter for the rule is incremented.

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

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

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

[Ref: 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:

The network function shall have protection mechanism against Network level and Application-level DDoS attacks.

The network function 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.

For example, potential protective measures may include:

- Restricting of available RAM per application
- Restricting of maximum sessions for a Web application
- Defining the maximum size of a dataset

- Restricting CPU resources per process
- Prioritizing processes
- Limiting of amount or size of transactions of a user or from an IP address in a specific time range
- Limiting of amount or size of transactions to an IP address/Port Address in a specific time range

[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 network function shall act in a predictable way if an overload situation cannot be prevented. The network function 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 network function cannot reach an undefined and thus potentially insecure, state.

OEM shall provide a technical description of the network function's Over Load Control mechanisms. (Especially whether these mechanisms rely on cooperation of other network elements e.g. RAN)

Ref: 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 / Interface Robustness Requirements

Requirement:

The network function 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 network function. 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 packets (i.e. packets which cannot be correlated to any request).

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

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

Section 2.9 Vulnerability Testing Requirements

2.9.1. Fuzzing – Network and Application Level

Requirement:

It shall be ensured that externally reachable services of the network function are reasonably robust when receiving unexpected input.

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

2.9.2. Port Scanning

Requirement:

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

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

2.9.3. Vulnerability Scanning

Requirement:

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

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

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

Section 2.10 Operating System

2.10.1. Growing Content Handling

Requirement:

a) Growing or dynamic content shall not influence system functions.
b) A file system that reaches its maximum capacity shall lead to an event getting logged

with appropriate message parameters and shall not stop the network function from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided.

[Ref: 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 network function.
The network function 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	Optional (i.e. as automatic reply to "Echo Request")	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 network function 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	Not Permitted

[Ref: 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 network function shall not support a privilege escalation method in interactive sessions (both CLI and GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication.

[Ref: 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 network function shall have a unique identification.

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

2.10.5. OS Hardening - Minimized kernel network functions

Requirement:

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

(i) IP Packet Forwarding between different interfaces of the network product.
(ii) Proxy Address Resolution Protocol (ARP) (to prevent resource exhaustion attack and man-in-the-middle attacks)
(iii) Directed broadcast (to prevent attacks like Smurf, Denial of Service etc.,)
(iv) IPv4 Multicast handling. In particular all packets with IP source or destination address belonging to the multicast IP ranges (224.0.0.0 through 239.255.255.255) shall be discarded by default and multicast route caching and forwarding shall be disabled to prevent smurf and fraggle attacks. A configuration option shall be available to enable the IPv4 multicast handling if required.
(v) Gratuitous ARP messages (to prevent ARP Cache Poisoning attacks)

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

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

2.10.6. No automatic launch of removable media

Requirement:

The network function shall not automatically launch any application when a removable media device such as Compact Disk (CD), Digital Versatile Disk (DVD), Universal Serial Bus (USB)-Sticks or USB- Storage drive is connected. If the operating system supports an automatic launch, it shall be deactivated unless it is required to support availability requirements.

[Ref: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section – 4.3.3.1.3]
Note: This clause may not be applicable for GVNP Type 1 and 2.

2.10.7. Protection from buffer overflows

Requirement:

The network function shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided by OEM.

[Ref: 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 network function in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems. OS-level restrictions shall apply to normal users against mount / use of removable media devices (e.g. USB drive, CD ROM etc.) for data transfer.

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

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

2.10.9. File-system Authorization privileges

Requirement:

The network function shall be designed to ensure that only users that are authorized to modify files, data, directories or file systems have the necessary privileges to do so.

[Ref: 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:

The network function shall support a mechanism to prevent SYN Flood attacks. This feature shall be enabled by default.

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

2.10.11. Handling of IP options and extensions

Requirement:

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

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

2.10.12. Restrictions on running Scripts / Batch-processes

Requirement:

Scheduled tasks for carrying out the activities such as taking the backups, monitoring disk space and system maintenance activities shall be executed by the privileged user such as administrator only. Similarly, the network function 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:

The network function 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.

Note: Hardware based restart may not be applicable for GVNP Type 1 and 2.

Section 2.11 Web Servers

This entire section of the security requirements is applicable if the network function 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 Table 1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Ref: 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 network function webserver (for both successful as well as failed attempts) shall be logged by the network function.

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

[Ref: 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 network function shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.
The network function shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.

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

2.11.4. No system privileges

Requirement:

No network function web server processes shall run with system privileges.

[Ref: 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 network function operation shall be deactivated.

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

[Ref: 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.

[Ref: 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.

[Ref: 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.

[Ref: 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 network function web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges.

[Ref: 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 network function web server shall be removed.

[Ref: 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.

[Ref: 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 network function web server and the modules/add-ons used.

[Ref: 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 network function web server and the modules/add-ons used.
Default error pages of the network function web server shall be replaced by error pages defined by the OEM.

[Ref: 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 network function operation shall be deleted.

[Ref: 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 network function web server's document directory.
In particular, the network function web server shall not be able to access files which are not meant to be delivered.

[Ref: 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

(applicable to network functions AMF, AuSF, NWDAF, NEF, NRF, N3IWF, SEPP, SCP, SMF, UDM, UPF, AF, LMF-GMLC only; to be tested on any one of these network functions: AMF, AuSF, NWDAF, NEF, NRF, N3IWF, SEPP, SCP, SMF, UDM, UPF, AF, LMF-GMLC network functions of Group I)

Requirement:

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

[Ref: 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

(applicable to network functions AMF, AuSF, NWDAF, NEF, NRF, N3IWF,SEPP, SCP, SMF,

UDM, UPF, BSF, CHF, SMSF, UDR, UDSF, EIR, NSACF,UCMF, AF, NSSF, PCF only; to be tested on any one of these network functions: AMF, AuSF, NWDAF, NEF, NRF, N3IWF,SEPP, SCP, SMF, UDM, UPF, BSF, CHF, SMSF, UDR, UDSF, EIR, NSACF,UCMF, AF, NSSF, PCF network functions of Group I)

Requirement:

To protect user sessions, the network function 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 network function 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
5. 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. 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 network function 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 network function shall not accept session identifiers from GET/POST variables.
12. The network function shall be configured to only accept server generated session ID.

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

Section 2.12 General SBA/SBI Aspects

This general baseline requirements are applicable to all Network Function (NF) within the 5G Core (5GC) utilizing Service-Based Interfaces (SBI), independent of a specific network product class.

2.12.1. No code execution or inclusion of external resources by JSON parsers

Requirement:

Parsers used by Network Functions (NF) shall not execute JavaScript or any other code contained in JSON objects received on Service Based Interfaces (SBI). Further, these parsers shall not include any resources external to the received JSON object itself, such as

files from the NF's filesystem or other resources loaded externally.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.6.2]

2.12.2. Validation of the unique key values in IEs

Requirement:

For data structures where values are accessible using names (sometimes referred to as keys), e.g. a JSON object, the name shall be unique. The occurrence of the same name (or key) twice within such a structure shall be an error and the message shall be rejected.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.6.3]

2.12.3. Validation of the IEs limits

Requirement:

The valid format and range of values for each IE, when applicable, shall be defined unambiguously:

- For each message the number of leaf IEs shall not exceed 16000.
- The maximum size of the JSON body of any HTTP request shall not exceed 16 million bytes.
- The maximum nesting depth of leaves shall not exceed 32.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.6.4]

2.12.4. Protection at the transport layer

(Applicable only to network functions AMF, AUSF, NWDAF, NEF, NRF, SEPP, SCP, SMF, UDM, BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF, AF, NSSF and PCF. to be tested on any one of these network functions AMF, AUSF, NWDAF, NEF, NRF, SEPP, SCP, SMF, UDM, BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF, AF, NSSF and PCF)

Requirement:

NF Service Request and Response procedure shall support mutual authentication between NF consumer and NF producer.

All network functions shall support TLS. Network functions shall support both server-side and client-side certificates.

Authentication between network functions within one PLMN can use the following method:

- If the PLMN uses protection at the transport layer, authentication provided by the transport layer protection solution shall be used for authentication between NFs.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.2.2.2]

2.12.5. Authorization token verification failure handling within one PLMN

(applicable to network functions AMF, AuSF, NWDAF, NEF, NRF,SEPP, SMF, UDM, BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF,UCMF, AF, NSSF, PCF only; to be tested on any one of these network functions: AMF, AuSF, NWDAF, NEF, NRF, SMF, UDM, BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF,UCMF, AF, NSSF, PCF network functions of Group I)

Requirement:

The NF Service producer shall verify the access token as follows:

- The NF Service producer ensures the integrity of the access token by verifying the signature using NRF's public key or checking the MAC value using the shared secret. If integrity check is successful, the NF Service producer shall verify the claims in the access token as follows: - It checks that the audience claim in the access token matches its own identity or the type of NF service producer. If a list of NSSAIs or list of NSI IDs is present, the NF service producer shall check that it serves the corresponding slice(s).
- If an NF Set ID is present, the NF Service Producer shall check the NF Set ID in the claim matches its own NF Set ID.
- If the access token contains "additional scope" information (i.e. allowed resources and allowed actions (service operations) on the resources), it checks that the additional scope matches the requested service operation.
- If scope is present, it checks that the scope matches the requested service operation.
- It checks that the access token has not expired by verifying the expiration time in the access token against the current data/time.

If the verification is successful, the NF Service producer shall execute the requested service and respond back to the NF Service consumer. Otherwise, it shall reply base on the Oauth 2.0 error response defined in RFC 6749. The NF service consumer may store the received token(s). Stored tokens may be re-used for accessing service(s) from producer NF type listed in claims (scope, audience) during their validity time.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.2.2.3.1]

2.12.6. Authorization token verification failure handling in different PLMNs

(applicable to network functions AMF, AuSF, NWDAF, NEF, NRF, SEPP, SMF, UDM, UPF, BSF, CHF, LMF-GMLC, SMSF, NSACF, AF, NSSF, PCF only; to be tested on any one of these network functions: AMF, AuSF, NWDAF, NEF, NRF, SEPP, SMF, UDM, UPF, BSF, CHF, LMF-GMLC, SMSF, NSACF, AF, NSSF, PCF network functions of Group I)

Requirement:

The NF service producer shall check that the home PLMN ID of the audience claimed in the access token matches its own PLMN identity.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.2.2.3.2]

2.12.7. Protection against JSON injection attacks

(applicable to network functions BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF, PCF only; to be tested on any one of these network functions: BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF, PCF network functions of Group I)

Requirement:

NF Service Consumers communicate using JSON on the service-based interfaces with network function. Network function shall never use the eval function to evaluate JSON data to prevent client-side JSON injections. Network function shall sanitize all data before

serializing it to JSON, to prevent server-side JSON injections.

[Ref: ENISA threat landscape for 5g networks, December 2020]

Section 2.13 Other Security requirements

2.13.1. Remote Diagnostic Procedure – Verification

Requirement:

If the network function 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
6. Result type (e.g. SUCCESS, FAILURE).
7. IP Address of remote machine

2.13.2. No System Password Recovery

Requirement:

No provision shall exist for the network function System / Root password recovery.

2.13.3. Secure System Software Revocation

Requirement:

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

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

2.13.4. Software Integrity Check –Installation

Requirement:

The network function shall validate the software package integrity before the installation stage strictly using the Secure cryptographic controls prescribed in Table 1 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.

2.13.5. Software Integrity Check – Boot

Requirement:

The network function 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 Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" to the expected reference value.

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

2.13.6. Unused Physical and Logical Interfaces Disabling

Requirement:

The network function shall support the mechanism to verify both the physical and logical interfaces exist in the product.
Physical and logical accessible interfaces (except console interface) which are not under use shall be disabled so that they remain inactive even in the event of reboot.

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

2.13.7. No Default Profile/ Predefined accounts shall be deleted or disabled

Requirement:
Predefined or default user accounts (other than Admin/Root) in the network function shall be deleted or disabled.

2.13.8. Correct handling of client credentials assertion validation failure

(applicable to network functions BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF only; to be tested on any one of these network functions BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF network functions of Group I)

Requirement:
The verification of the Client credentials assertion shall be performed by the receiving node, i.e., NRF or NF Service Producer in the following way:

a) It validates the signature of the JSON Web Signature (JWS) as described in RFC 7515.
b) If validates the timestamp (iat) and/or the expiration time (exp) as specified in RFC 7519.
    i. If the receiving node is the NF Service Producer, the NF service Producer validates the expiration time and it may validate the timestamp.
c) It checks that the audience claim in the client credentials assertion matches its own type.

It verifies that the NF instance ID in the client credentials assertion matches the NF instance ID in the public key certificate used for signing the assertion.

[Ref : TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.2.2.4.1]
[Ref: RFC 7515 - JSON Web Signature (JWS)]
[Ref : RFC 7519 - JSON Web Token (JWT)]

Note: Not applicable to Release 16 implementation

2.13.9. Isolation of Compromised Element

(applicable to network functions BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF only; to be tested on any one of these network functions: BSF, CHF, LMF-GMLC, SMSF, UDR, UDSF, EIR, NSACF, UCMF network functions of Group I)

Requirement:

In case of any compromise of network function, it shall be possible to isolate the network function at network and/or compute/storage level. Such provisions shall be documented.

[Ref : ENISA SECURITY IN 5G SPECIFICATIONS, Controls in 3GPP Security Specifications (5G SA) FEBRUARY 2021 Section 4.1.3]

Annexure-I

Definitions

1. **AF:** Application Function is the functional element that provides service or application related information to Network Function service consumers.
2. **AUSF:** AUSF is a network function with which SEAF and UDM interact during the authentication of UE.
3. **BSF:** BSF is a network function used for binding an Application Function (AF) request targeting a particular UE to a specific Policy Control Function (PCF) instance .
4. **DDOS:** DDoS is a distributed denial-of-service attack that renders the victim unusable by the external environment.
5. **Integrity:** (in the context of security) The avoidance of unauthorised modification of information.
6. **International Mobile Station Equipment Identity (IMEI):** An "International Mobile Station Equipment Identity" is a unique number which shall be allocated to each individual mobile station equipment in the PLMN and shall be unconditionally implemented by the MS manufacturer.
7. **Intra PLMN handover:** Handover within the same network, i.e. having the same MCC-MNC regardless of radio access system.
8. **Machine Accounts:** These will be used for authentication and authorization from system to system or between applications on a system and cannot be assigned to a single person or a group of persons.
9. **Medium Access Control:** A sub-layer of radio interface layer 2 providing unacknowledged data transfer service on logical channels and access to transport channels.
10. **NEF:** Network Exposure Function, interwork with other network outside 5G.
11. **Network Element:** A discrete telecommunications entity which can be managed over a specific interface e.g. the RNC
12. **Network Function:** A 3GPP adopted or 3GPP defined processing function in a network, which has defined functional be haviour and 3GPP defined interfaces. A network function can be implemented either as a network element on a dedicated hardware, as a software instance running on a dedicated hardware, or as a virtualized function instantiated on an appropriate platform, e.g., on a cloud infrastructure.
13. **NF service operation:** An elementary unit a NF service is composed of.
14. **NF service:** a functionality exposed by a NF through a service-based interface and consumed by other authorized NFs.
15. **NSI:** Network Slice Instance-A set of Network Function instances and the required resources (e.g. compute, storage and networking resources) which form a deployed Network Slice.
16. **NSS:** Network slice Subnet-A representation of the management aspects of a set of Managed Functions and the required resources (e.g. compute, storage and networking resources) -(GSMA 116) Network slices are generally composed of network slice subnets (e.g. RAN network slice subnet, Core network slice subnet and Transport network slice subnet) -(3gpp)

17. **NSSAI:** Network Slice Selection Assistance Information-The NSSAI is a collection of SNSSAIs. An NSSAI may be a Configured NSSAI, a Requested NSSAI or an Allowed NSSAI. There can be at most eight S-NSSAIs in Allowed and Requested NSSAIs sent in signalling messages between the UE and the Network. [1]
18. **NSSF:** Network Slice Selection Function-The selection of the set of Network Slice instances for a UE is triggered by the first contacted the network function in a registration procedure normally by interacting with the NSSF. [1]
19. **NWDAF:** Network Data Analytic Function, provides network analytic information to 5G Core network functions and for Operation, Administration and Management (OAM)
20. **Original Equipment Manufacturer (OEM):** manufacturer of communication and its related products under whose brand, the products are sold or proposed to be sold to operators in the country.
21. **Packet:** An information unit identified by a label at layer 3 of the OSI reference model. A network protocol data unit (NPDU).
22. **Personal data:** any information relating to an identified or identifiable natural person ('data subject'). NOTE: personal data can be gathered from user data and traffic data.
23. **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.
24. **Public land mobile network (PLMN):** A telecommunications network providing mobile cellular services.
25. **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.
26. **Registered PLMN (RPLMN):** This is the PLMN on which the UE has performed a location registration successfully.
27. **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.
28. **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.
29. **SEAF** is an entity which is subsumed by the network function which communicates with UE and AUSF during device authentication.
30. **Security:** The ability to prevent fraud as well as the protection of information availability, integrity, and confidentiality
31. **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.
32. **Service based interface:** It represents how a set of services is provided/exposed by a given NF.
33. **Serving Network:** The serving network provides the user with access to the services of the home environment.

34. **Session:** logical connection between parties involved in a packet switched based communication This term is used for IP connections rather than the term "call" that is normally used for a connection over conventional (circuit switched) systems.
35. **Settlement:** payment of amounts resulting from the accounting process.
36. **Short message (SM):** Information that may be conveyed by means of the Short Message Service.
37. **Software** refers to the programs and data components which are usually stored on erasable media (e.g., disk), that can be dynamically written and modified during execution. Two general categories of software are system software and application software.
38. **Stratum:** Grouping of protocols related to one aspect of the services provided by one or several domains.
39. **Subscriber:** The responsibility for payment of charges incurred by one or more users may be undertaken by another entity designated as a subscriber. This division between use of and payment for services has no impact on standardization.
40. **Transit:** interconnection scenarios in multi operator environments where one or more transit operators are between the originating and terminating operator.
41. **Transmission or Transport** is the transfer of information from one entity (transmitter) to another (receiver) via a communication path.
42. **Uplink:** An "uplink" is a unidirectional radio link for the transmission of signals from a UE to a base station.
43. **User Equipment (UE):** device allowing a user access to network services. For the purpose of 3GPP specifications 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. Currently defined domains are the USIM and ME Domains. The ME Domain can further be subdivided into several components showing the connectivity between multiple functional groups. These groups can be implemented in one or more hardware devices. An example of such connectivity is the TE – MT interface. Further, an occurrence of a User Equipment is an MS for GSM as defined in TS 24.002.

Annexure-II

Acronyms

5GC	-	5G Core Network
AUSF	-	Authentication Server Function
BSF	-	Binding Support Function
CHF	-	Charging Function
CLI	-	Command Line Interface
CVSS	-	Common Vulnerability Scoring System
DDoS	-	Distributed Denial of Service
EPC	-	Evolved Packet Core
GNP	-	Generalized Network Product
GTP-C	-	GPRS Tunnelling Protocol Control Plane
GTP-U	-	GPRS Tunnelling Protocol User Plane
GUI	-	Graphical User Interface
GVNP	-	Generalized Virtual Network Product
HTTP	-	Hypertext Transfer Protocol
HTTPS	-	Hypertext Transfer Protocol Secure
ICMP	-	Internet Control Message Protocol
ISO-OSI	-	International organization of Standardization – Open System Interconnection
JSON	-	JavaScript Object Notation
JWS	-	JSON Web Signature
JWT	-	JSON Web Token
LMF	-	Location Management Function
N3IWF	-	Non-3GPP Interworking Function
NEF	-	Network Exposure Function
NF	-	Network Function
NG	-	Next Generation
NRF	-	Network Repository Function
NSAC	-	Network Slice Admission Control
NWDAF	-	Network Data Analytics Function
OAM	-	Operations Administration Maintenance
OS	-	Operating System
PCF	-	Policy Control Function
PDU	-	Protocol Data Unit
PLMN	-	Public Land Mobile Network
QoS	-	Quality of Service
RAM	-	Random Access Memory
RFC	-	Request For Comments
RRC	-	Radio Resource Control
SBI	-	Service Based Interfaces
SCP	-	Service Communication Proxy

SEPP	-	Security Edge Protection Proxy
SMF	-	Session Management Function
SNPN	-	Stand Alone Non-Public Network
SUPI	-	Subscription Permanent Identifier
TSTL	-	Telecom Security Testing Laboratory
UDM	-	Unified Data Management
UDR	-	Unified Data Repository
UPF	-	User Plane Function
URL	-	Uniform Resource Locator

Annexure-III

List of Submissions

List of undertakings to be furnished by the OEM for Group I 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 (against test case 2.3.5)
4. No unsupported Components (against test case 4.2)
5. Avoidance of Unspecified Wireless Access (against test case 2.4.3)
6. Cryptographic Module Security Assurance (against test case 2.6.2)
7. 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 V1.0.0. / TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. "Catalogue of General Security Assurance Requirements"
2. Security Guidance for 5G Cloud Infrastructure Part III: Data Protection" by NSA & CISA
3. ENISA threat landscape for 5G networks, December 2020
4. RFC 7515 - JSON Web Signature (JWS)
5. RFC 7519 - JSON Web Token (JWT)
6. ENISA security in 5G specifications, Controls in 3GPP Security Specifications (5G SA) February 2021
7. CIS Password Policy Guide
8. ENISA Recommendation "Standardization in support of the cybersecurity certification", Dec 2019]
9. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
10. https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html
11. https://owasp.org/www-project-top-ten/
12. https://owasp.org/www-project-api-security/
13. RFC 3871 – Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure