Indian Telecom Security Assurance Requirements (ITSAR)

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

Lawful Interception (LI) system of 5G

(Draft for Comments)

ITSAR Number: ITSAR10902YYMM
ITSAR Name: NCCS/ITSAR/Core Equipment/Lawful Interception Systems/Lawful Interception System of 5G

Date of Release: DD.MM.YYYY 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. NCCS is mandated to prepare Telecom security requirements/standards called Indian Telecommunication 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.	Lawful Interception (LI) system of 5G	ITSAR10902YYMM	1.0.0	DD.MM.YYYY	First release

Table of Contents

A. Outline

The objective of this document is to present comprehensive, country-specific security requirements for the Lawful Interception System (LI system) in 5G.

The specifications produced by various regional/international standardization bodies/organizations/associations like 3rd Generation Partnership Project (3GPP), International Telecommunication Union - Telecommunications Standardization Sector (ITU-T), International Organization for Standardization (ISO), European Telecommunications Standards Institute (ETSI), Internet Engineering Task Force (IETF), Internet Research Task Force (IRTF), Global System for Mobile communication Association (GSMA), Telecommunications Standards Development Society of India (TSDSI) et. al. along with the country-specific security requirements are the basis for this document. The Telecommunication Engineering Centre (TEC)/ TSDSI references made in this document implies that the respective clause has been adopted as it is or with certain modifications.

This document commences with a brief description of the 5G system architecture, introduction to Lawful Interception (LI) with respect to 5G network and then proceeds to address the common and specific security requirements for LI in 5G.

B. Scope

This document targets on the security requirements of the 5G LI system. This document does not cover the security requirements at the virtualization and infrastructure layers. Remote Access regulations are governed by the Licensing Wing of the Department of Telecommunications (DoT).

C. Conventions

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

Chapter-1 - Overview

1.1 Introduction

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

1.2 5G Architecture

The 5G architecture supports various service deployments by using techniques like Software Defined Networking (SDN) and Network Function Virtualization (NFV). The generic 5G System (5GS) architecture consists of User Equipment (UE), Radio Access Network (RAN), supporting 3GPP (e.g., New Radio (NR) and Evolved Universal Terrestrial Radio Access (E-UTRA)), as well as non-3GPP access (e.g., Wireless Local Area Network (WLAN)) and 5G Core Network. The 5G NR base station is called Next Generation Node B (gNB). The deployment strategies possible are Non-Stand Alone (NSA) and Stand Alone (SA). SA denotes 5G NR RAN connecting to 5G Core Network. In NSA mode, 5G NR RAN (gNBs) gets connected to Fourth Generation (4G)'s Evolved Packet Core (EPC) but uses 4G Long Term Evolution (LTE) eNode as anchor in the control plane.

1.2.1 5G Core Network

Core network is the central part of the mobile network. 5G Core network provides authentication, security, mobility management, session management services and allows the subscribers through access and authorization to avail the services. These functionalities of the 5G core network are supported using 3GPP defined processing functions specified as "network functions". A network function can be realized in different ways, e.g., as a network element on a dedicated hardware, or as a software instance running on a dedicated hardware, or as a virtualized function instantiated on shared (cloud) infrastructure.

The salient features of 5G core network are as follows:

a) Separation of Control Plane and User Plane
b) Service Based Architecture (SBA)
c) Network Slicing support
d) Enable usage of Network Function Virtualization (NFV) and Software Defined Networking (SDN)
e) Access Agnostic
f) Framework for policy control and support of Quality of Service (QoS)

g) Secure exposure of network function capabilities to 3rd party providers
h) Storage of subscription data, subscriber access authentication, authorization and security anchoring
i) Support for "stateless" NFs and storage of their unstructured data in UDSF

In an SBA framework, the individual elements are defined as Network Functions (NFs) instead of Network entities. Through Service Based Interface (SBI), an NF consumes services offered by other NFs. RESTful Application Programming Interfaces (APIs) are used in 5G SBA which use Hypertext Transfer Protocol (HTTP)/2 as the application layer protocol. Service based architecture for the 5G system is shown in Figure 1 including some important core network functions. For the sake of clarity & simplicity, all NFs are not shown.

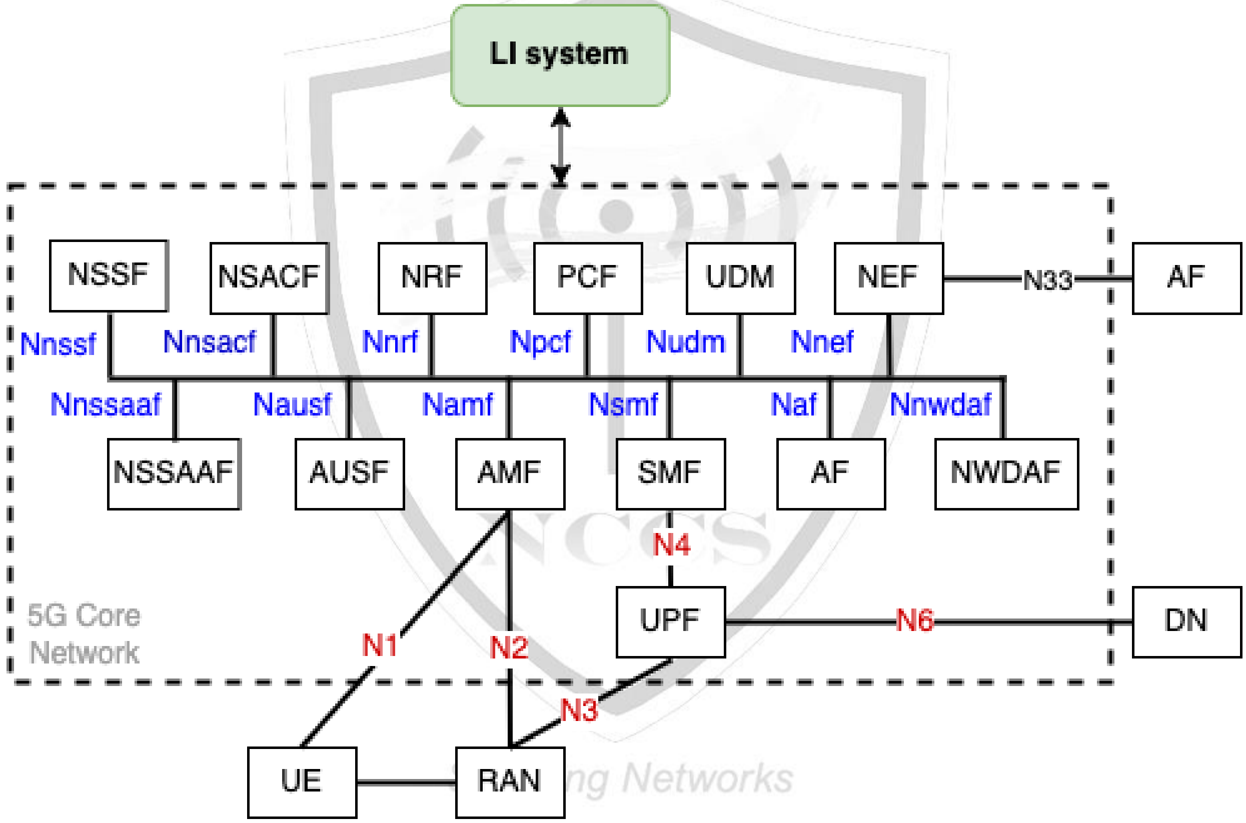

Figure 1: Service based architectural view of 5GS [Adapted from TSDSI STD T1.3GPP 23.501 17.7.0 V1.3.0]

Figure 2 shows reference point representation for a few functions of the core network. Point to point reference points are shown between two network functions, for example N22 between AMF and NSSF.

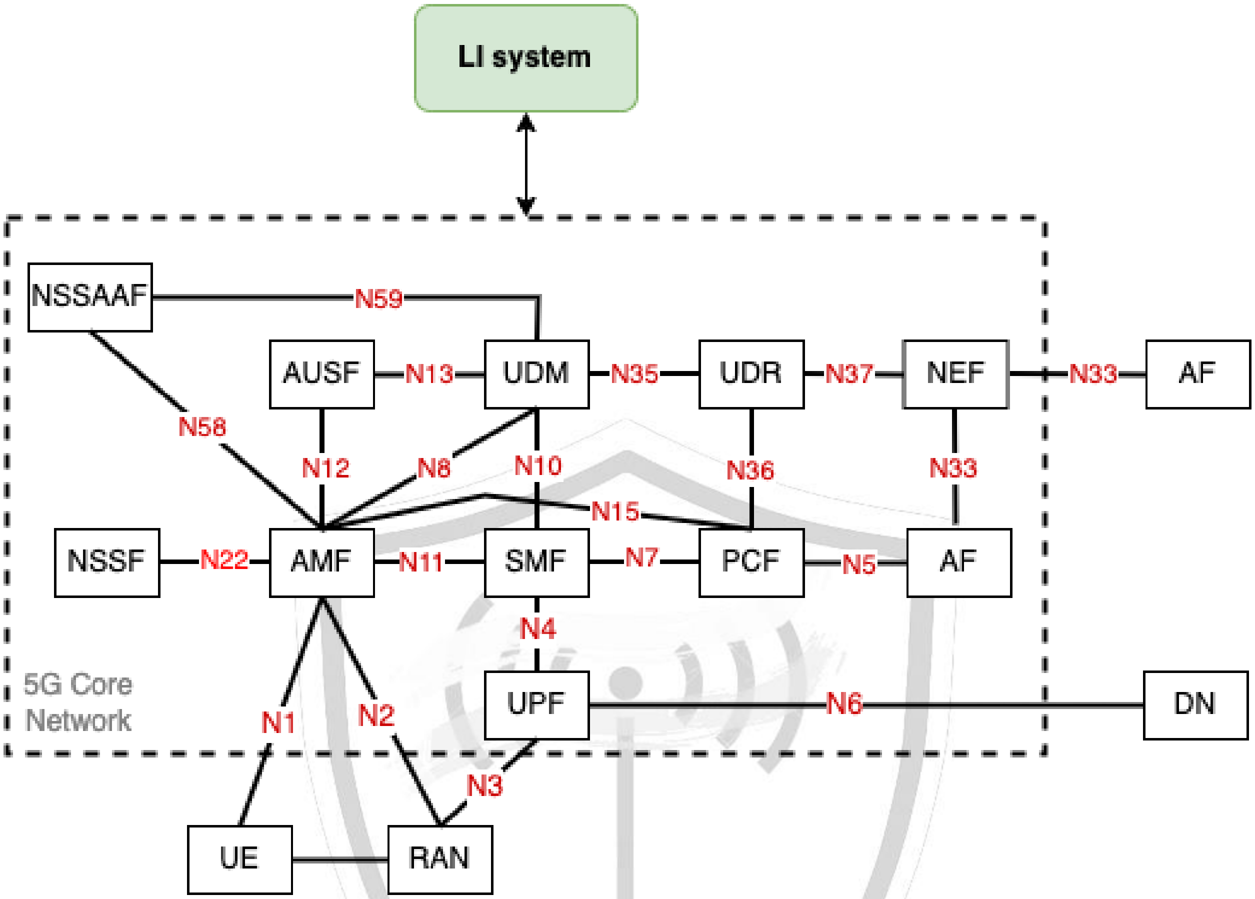

Figure 2: Reference point representation for 5GS [Adapted from TSDSI STD T1.3GPP 23.501 17.7.0 V1.3.0 and 3GPP 29.536 17.3.0]

Some of the core network functions and their functionalities are as follows:

1. Access and Mobility Management Function (AMF): Some of the functionalities of AMF are registration management, connection management, mobility management, access authentication and authorization, termination of Non-Access Stratum (NAS) and support for Short Message Service (SMS).
2. Session Management Function (SMF): Some of the functionalities of SMF are session establishment, modification and release, UE Internet Protocol (IP) address allocation and management, charging data collection and termination of interfaces towards Policy Control Function (PCF).
3. Authentication Server Function (AuSF): AuSF resides in the Home Network. It supports UE authentication for 3GPP and non-3GPP accesses.

4. User Plane Function (UPF): Some of the UPF functionalities include packet routing and forwarding, policy enforcement and QoS handling (related to user plane part) and traffic usage reporting for user planes. It is the anchor point for UE in case of Intra or Inter RAT mobility.
5. Application Function (AF): It interacts with the 3GPP Core Network to provide services, influences traffic routing by accessing Network Exposure Function (NEF) (and possibly PCF) and by interacting with the policy framework for policy control. In case of existence of more than one PCF in the CN, it reaches the concerned PCF through Binding Support Function (BSF).
6. Network Exposure Function (NEF): Some of the functionalities of NEF are exposure of capabilities, events and analytics, and secure provisioning of information from external applications to the 5G network.
7. Network Repository Function (NRF): NRF supports service discovery function and maintains NF profiles of available NF instances and their supported services. It receives NF discovery request from NF instances and provides information of the discovered NF instances to them.
8. Policy Control Function (PCF): PCF functionalities include support for a unified policy framework to govern the network behavior. PCF provides policy rules to control plane for enforcement and accesses subscription information relevant to policy decisions from UDR.
9. Unified Data Management (UDM): Some of the UDM functionalities are user identification handling, access authorization based on subscription data and UE's serving NF registration management.
10. Network Slice Admission Control Function (NSACF): NSACF is a 5GC NF that monitors and controls the no. of registered UEs and no. of established PDU sessions per network slice which are subject to NSAC. It provides services via service-based interface through API calls to AMF, SMF (or combined SMF+PGW-C), NWDAF and NEF within 5GC. It also provides event-based network slice status notifications and reports to other consumer NFs for monitoring or triggering event-based actions.

Any network function in the control plane can enable other authorized network functions to access their services using standard service-based interfaces.

1.3 General Security Architecture for 5G System

The 5G System works on the principle of service-based architecture which presents the need for consideration of security aspects. Secure interactions between the network functions are governed by the security features, i.e. Confidentiality, Integrity and Availability. The architecture enabling secure communications between the network entities is shown in Figure 3.

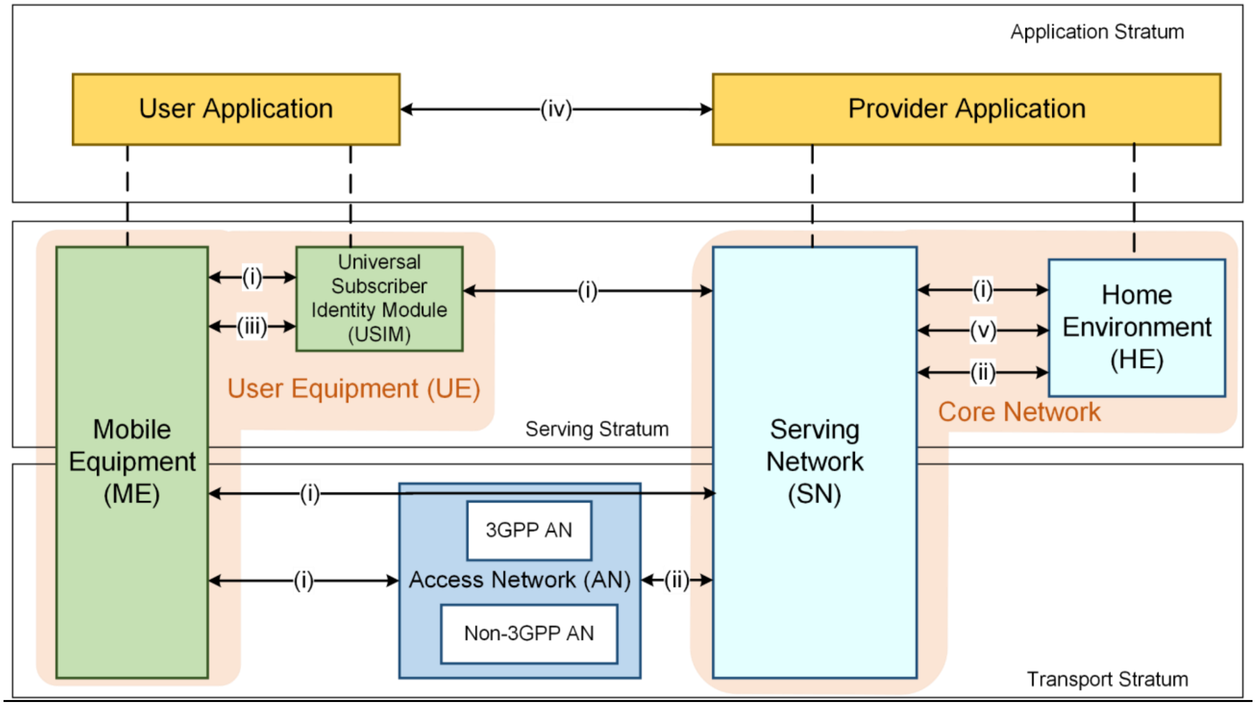

Figure 3: Overview of the security architecture [Adapted from TSDSI STD T1.3GPP 33.501-17.7.0 V1.1.0]

Mobile Equipment (ME) is served by 3GPP and non-3GPP access networks to facilitate connectivity with the Core Network. When MEs are outside the coverage area of the Home Environment (their primary service provider), they are served by the Visiting Network (as Serving Network). When the ME is in the coverage area of its primary service provider, there will be no distinction between the Serving Network (SN) and Home Environment (HE), they will be one and the same. ME's communication with the provider network is enabled using the Universal Subscriber Identity Module (USIM).

User Application is the application layer in the UE, which facilitates user interaction with provider application. Provider Application communicates with the user application using the logical link established through the 5G System.

The security features and the security mechanisms for the 5G System and the 5G Core can be categorized in following domains:

Network Access security: UEs are authenticated and provided access to the network using security features of this domain. It provides secure access via the 3GPP and non-3GPP networks, in particular protects radio interfaces against attacks. In addition, it includes security context delivery from Serving Network (SN) to Access Network (AN) to support access security.

Network Domain security: The security features of this domain allow network nodes to securely exchange signaling data and user plane data.

User domain security: Users can securely access the mobile equipment using security features of this domain.

Application domain security: The features of this security domain facilitate secure exchange of messages between applications in user domain and provider domain.

SBA domain security: The security features of this domain facilitate secure communication between NFs over the service-based interfaces within the serving network domain and with other network domains.

Visibility and configurability of security: The security features of this domain provide information about availability of security features to the user. This domain is not shown in the figure.

Common and specific security requirements of 5G Lawful Interception (LI) are covered in the present document. The following sections cover the overview of 5G LI along with its security aspects.

1.4 Introduction to LI and LI system

LI system provides a lawful interception capability. As required by the Law Enforcement Agency (LEA), it identifies target, detects & captures all Communication Content (CC) & Interception Related Information (IRI), delivers interception product in an agreed format to the LEA in a lawful, secure and undetectable way.

Thus, as a legally sanctioned official access to private communications, Lawful Interception (LI) is a security process in which a service provider or network operator collects and provides law enforcement officials with the intercepted communications of private individuals or organizations.

Communication Service Provider (CSP) hands over the interception product to the LEA that served the CSP with the warrant. An interception is associated with exactly one warrant.

Below is the basic LI flow diagram:

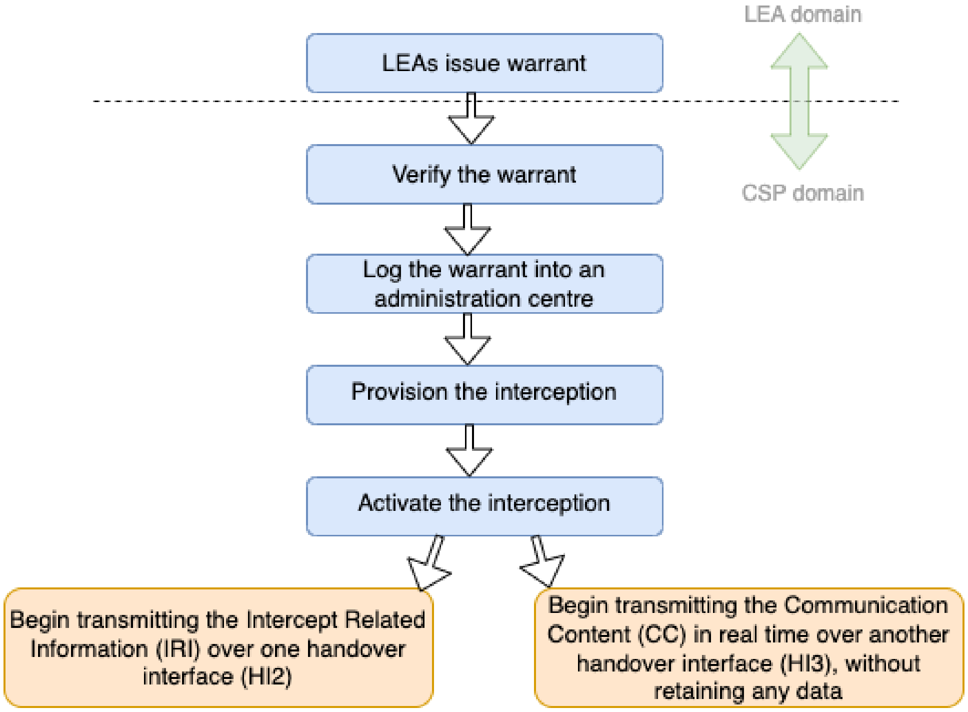
LEA domain
CSP domain
LEAs issue warrant
Verify the warrant
Log the warrant into an administration centre
Provision the interception
Activate the interception
Begin transmitting the Intercept Related Information (IRI) over one handover interface (HI2)
Begin transmitting the Communication Content (CC) in real time over another handover interface (HI3), without retaining any data

Figure 4. Basic LI flow diagram

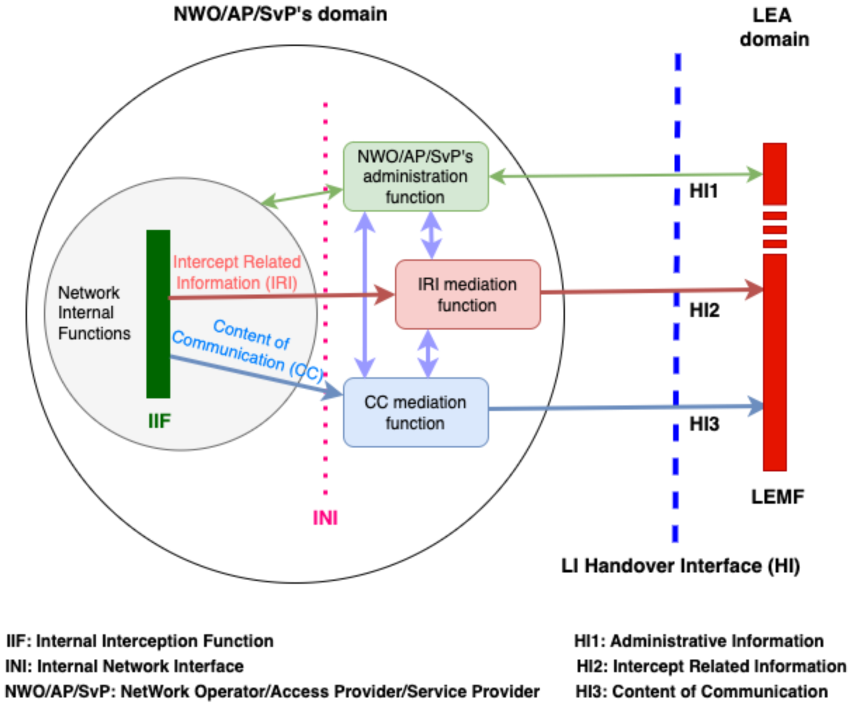
NWO/AP/SvP's domain
LEA domain
NWO/AP/SvP's administration function
Network Internal Functions
Intercept Related Information (IRI)
IRI mediation function
Content of Communication (CC)
CC mediation function
IIF
INI
HI1
HI2
HI3
LEMF
LI Handover Interface (HI)
IIF: Internal Interception Function
INI: Internal Network Interface
NWO/AP/SvP: NetWork Operator/Access Provider/Service Provider
HI1: Administrative Information
HI2: Intercept Related Information
HI3: Content of Communication

Figure 5: Generic LI system with handover interfaces [Adapted from ETSI-201.671 v3.2.1]

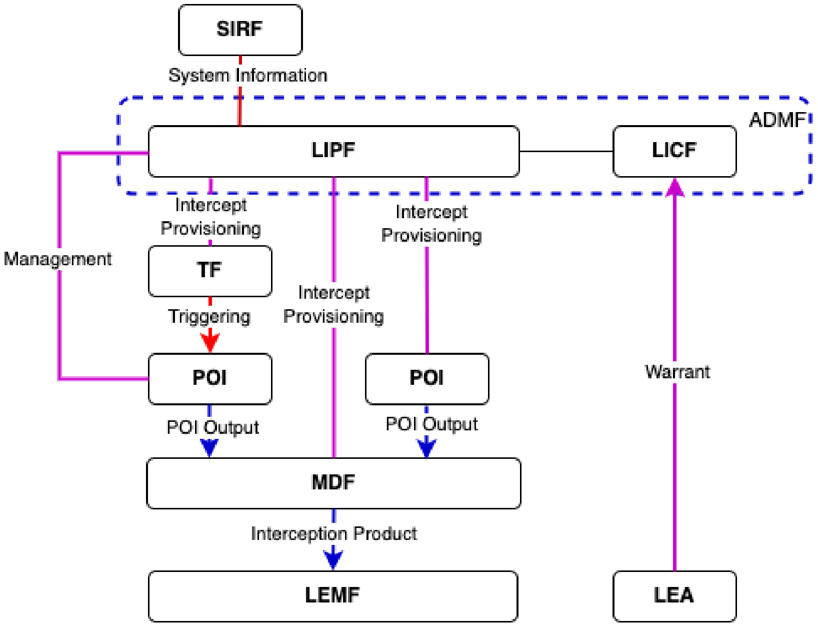

Figure 6: Conceptual view of LI architecture [Adapted from TSDSI STD T1.3GPP 33.127-17.9.0 V1.5.0]

The Law Enforcement Agency (LEA) is responsible for submitting the warrant to the CSPs.

The Mediation and Delivery Function (MDF) delivers the Interception Product to the Law Enforcement Monitoring Facility (LEMF).

The Point of Interception (POI) detects the target communication, derives the intercept related information or communications content from the target communications and delivers the POI output to the MDF. Multiple POIs may have to be involved in executing a warrant.

The Triggering Function (TF) is responsible for triggering POIs in response to network and service events matching the criteria provisioned by the Lawful Interception Provisioning Function (LIPF). The TF detects the target communications and sends a trigger to the associated triggered POI.

The Administration Function (ADMF) provides the CSP's administrative and management functions for the LI capability. This includes overall responsibility for the provisioning/activating, modifying, and de-activating/de-provisioning the Points Of Interception (POIs), Triggering Functions (TFs), and the Mediation and Delivery Functions (MDFs).

The System Information Retrieval Function (SIRF) is responsible for providing the LIPF with the system related information for Network Functions (NFs) that are known by the SIRF (e.g. service topology).

Figure below illustrates two variations of the MDF: MDF2 and MDF3. MDF2 generates the Intercept Related Information (IRI) messages from the xIRI and sends them to one or more LEMFs. The MDF3 generates the Communication Content (CC) from the xCC and delivers it to one or more LEMFs.

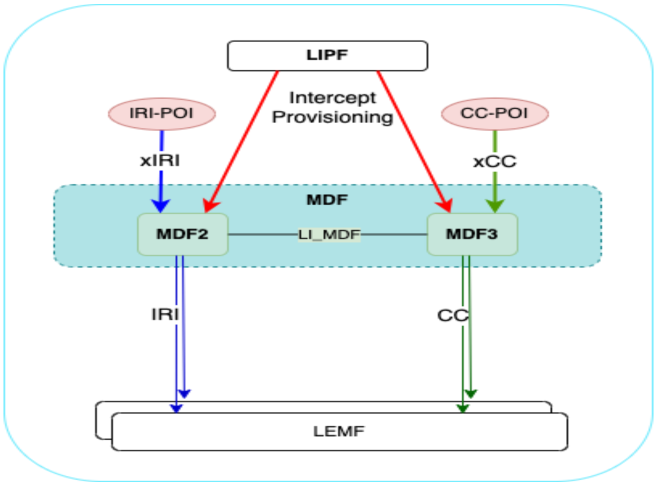

Figure 7: IRI and CC mediation & delivery functions [Adapted from TSDSI STD T1.3GPP 33.127-17.9.0 V1.5.0]

LI interfaces:

Below diagram shows major 5G LI interfaces-

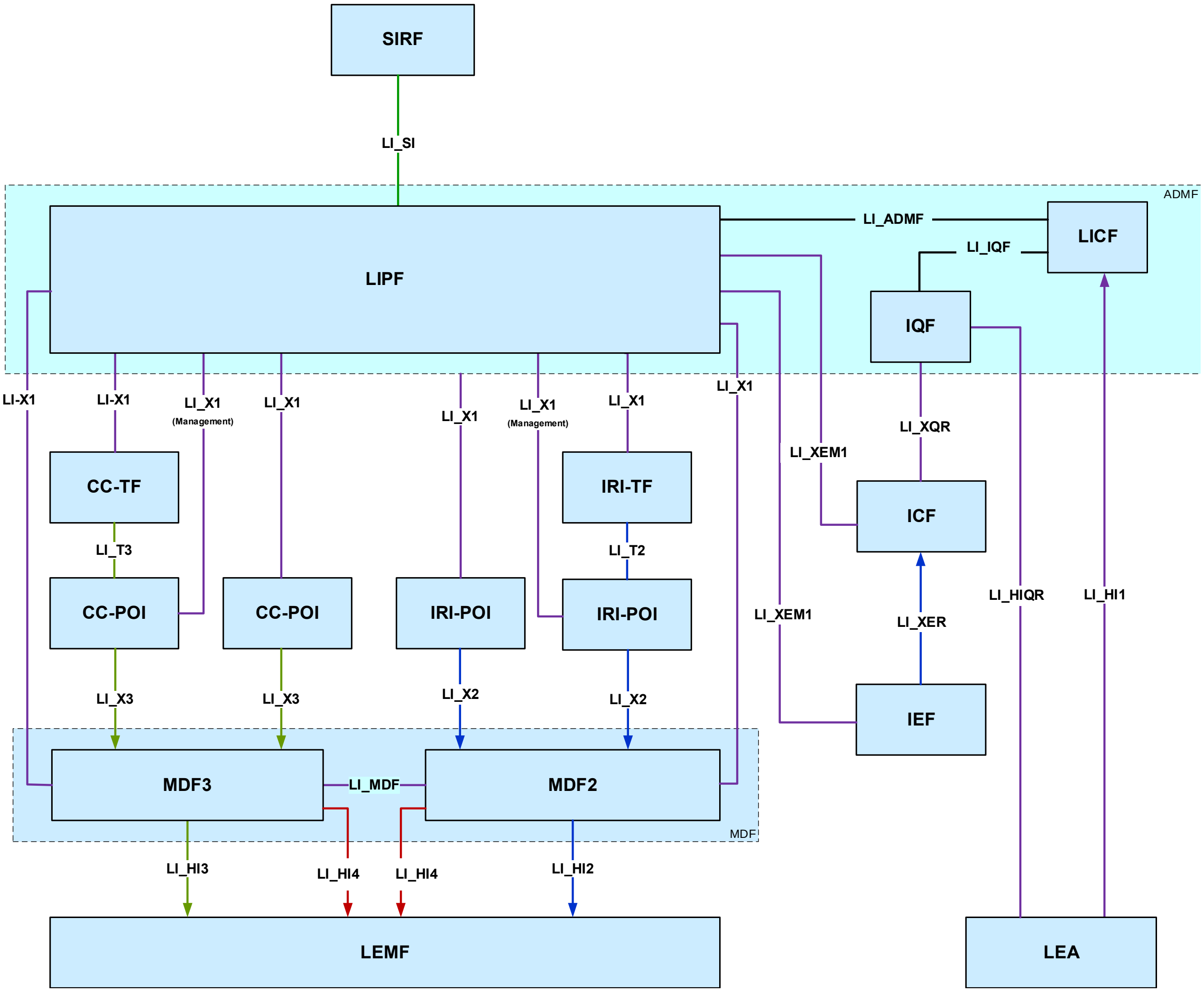

Figure 8: LI Interfaces [Adapted from TSDSI STD T1.3GPP 33.127-17.9.0 V1.5.0]

Note that all the IRI and CC POIs and TFs are provisioned by LI system in the 5G network functions (NFs) having standard LI capabilities. Administrative function (ADMF), MDFs constitute the separate LI system and LEMF/LEA constitute the LEA domain.
LI system can be a 3rd party solution, integrated to service provider network.
Lawful interception is governed by national regulation and all CSPs shall maintain regulatory compliance in an efficient, secure and effective manner.
LEA and CSPs generally agree on the operations terms like format of data transfer, authorization and other SLAs.

Major LI interfaces:

a) Handover Interfaces

Interface	Description
LI_HI1	Used to send warrant and other interception request information from LEA to operator.
LI_HI2	Used to send IRI from the MDF2 to the LEMF.
LI_HI3	Used to send CC from the MDF3 to the LEMF.
LI_HI4	Used to send LI notification information from MDF2/3 to LEMF.
LI_HIQR	Used to send warrant and other identifier association query information from LEA to CSP and used by the CSP to send query responses to the LEA.

b) Internal Interfaces

Interface	Description
LI_ST	Used to transfer LI state information to and from the LISSF.
LI_T2	Used to pass triggering information from the IRI-TF to a Triggered IRI-POI.
LI_T3	Used to pass triggering information from a CC-TF to a Triggered CC-POI.
LI_X1	Used to configure and audit Directly-provisioned POIs, TFs and MDFs.
LI_X1 (Management)	Used to audit Triggered POIs.
LI_X2	Used to pass xIRI from IRI-POIs to the MDF2.
LI_X3	Used to pass xCC from CC-POIs to the MDF3.
LI_XEM1	Used by the LICF/LIPF to manage IEFs and ICF.
LI_XER	Used to pass identifier association event records from IEFs to ICF.
LI_XQR	Used to pass queries from IQF to ICF and responses from ICF to IQF.

LI State Storage Function (LISSF) and LI_ST interface:

In SMF/UPF interception when using SMF set, in order to manage interception at the POI present in the UPF, a new NF, called LISSF is introduced. The TF that initiates the interception at a POI present in the UPF and stores the related necessary information (e.g. correlation information) in LISSF, in case a different TF in different SMF of the same SMF set has to manage the interception at that POI. This necessary related information is referred to as LI state information.

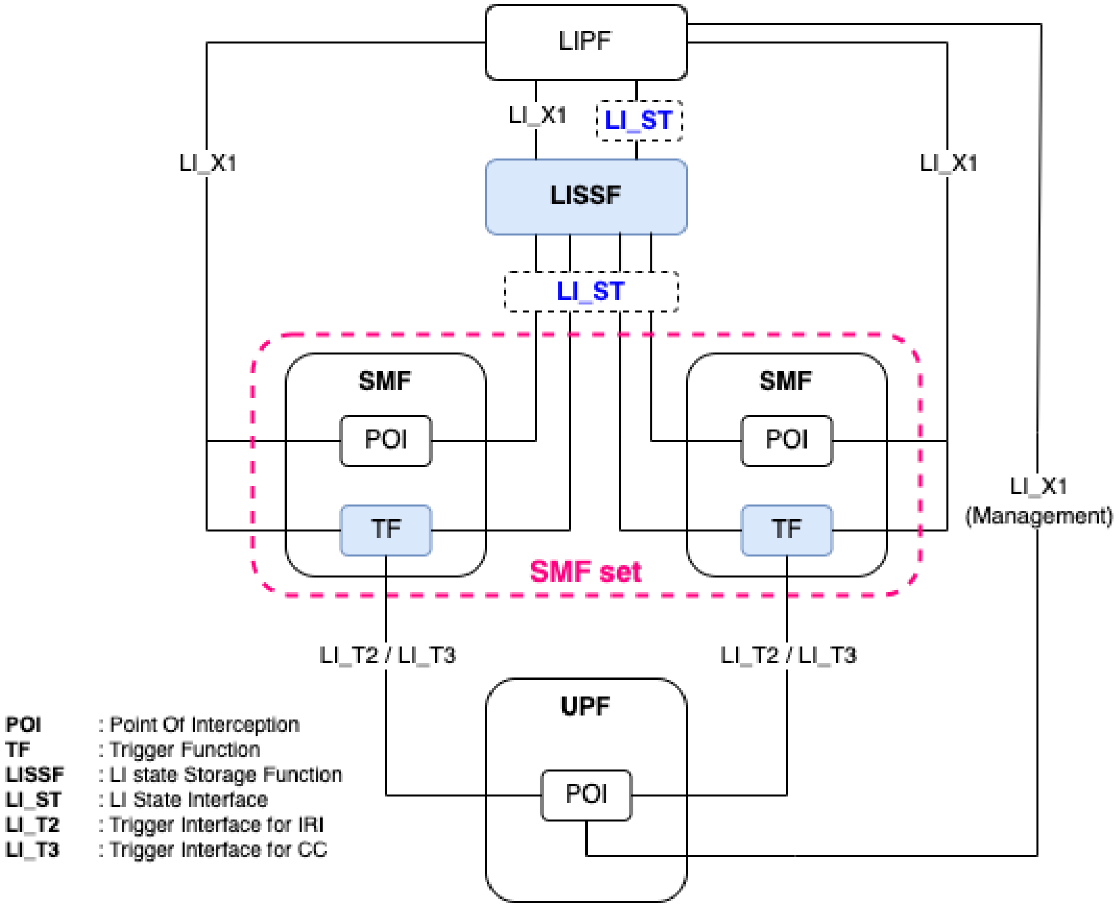
LIPF
LI_X1
LI_ST
LI_X1
LI_X1
LISSF
LI_ST
SMF
POI
TF
SMF
POI
TF
SMF set
LI_X1
(Management)
LI_T2 / LI_T3
LI_T2 / LI_T3
UPF
POI
POI : Point Of Interception
TF : Trigger Function
LISSF : LI state Storage Function
LI_ST : LI State Interface
LI_T2 : Trigger Interface for IRI
LI_T3 : Trigger Interface for CC

Figure 9: LI architecture for SMF/UPF interception when using SMF sets and LISSF [Adapted from TSDSI STD T1.3GPP 33.127-17.9.0 V1.5.0]

1.5 5G LI Security Aspects

LI deals with intercepting communication data of private parties under national regulation. Thus, data security and privacy are critical requirements. Lawful Interception by the CSP shall be undetectable by any party not explicitly authorized to have knowledge of it, and cannot be modified, altered or degraded by such a party.

To ensure SBA domain security, secure communications via SBI interface is considered. In addition, LI system will have interfaces with the Operations, Administration and Management (OAM) system to facilitate system administration and maintenance. Security aspects of the interface for OAM are also considered. Furthermore, LI system will have standard LI interfaces, security of those interfaces is considered along with secure storage (if required to store) and secure transfer/access of data.

Chapter -2 Common Security Requirements

Section 2.1: Access and Authorization

2.1.1 Authentication for Product Management and Maintenance interfaces

Requirement:

LI system shall support mutual authentication of entities on management interfaces, the authentication mechanism can rely on the management protocols used for the interface or other means.
Secure cryptographic controls prescribed in Table 1 of the latest document “Indian Telecommunication Security Assurance Requirements (ITSAR) for Cryptographic Controls” shall only be used for LI system management and maintenance.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.4.1]

2.1.2 Management Traffic Protection

Requirement:

LI system management traffic (information exchanged during interactions with OAM) shall be protected strictly using secure cryptographic controls prescribed in Table 1 of the latest document “ITSAR For Cryptographic Controls” only.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.2.4]

2.1.3 Role-based access control policy

Requirement:

LI system 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 (the domains could be Fault Management, Performance Management, System Admin, etc.) and what type of operation they can perform, i.e. the specific operation command or command group (e.g., View, Modify, Execute). LI system shall support RBAC with a minimum of 3 user roles, in particular, for OAM privilege management for LI system Management and Maintenance, including authorization of the operation for configuration data and software via LI system console interface.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.6.2]

Note: The reference to Console interface may not be applicable here for Generalized Virtual Network Product (GVNP) Models of Type 1 & 2

2.1.4 User authentication - Local/Remote

Requirement:

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

Authentication attributes include

a) Cryptographic keys
b) Token
c) Passwords

This means that authentication based on a parameter that can be spoofed (e.g., phone numbers, public IP addresses or Virtual Private Network (VPN) membership) 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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.2.1]

2.1.5 Remote login restrictions for privileged users

Requirement:

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

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

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.6.1]

2.1.7 Unambiguous identification of the user & group accounts

Requirement:

Users shall be identified unambiguously by the LI system.
LI system shall support the assignment of individual accounts per user, where the user could be a person, or, for Machine Accounts, an application, or a system.
LI system shall not enable the use of group accounts or group credentials, or sharing of the same account between several users.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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 the basis of the user identity and at least two authentication attributes shall be prevented. For machine accounts and local access one authentication attribute will be sufficient. System functions comprise, for example network services (like Secure Shell (SSH), Secure File Transfer Protocol (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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.1.1]

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

2.2.2 Authentication Support – External

Requirement:

If the LI system supports external authentication mechanism such as AAA server (for authentication, authorization and accounting services), then the communication between LI system 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 "ITSAR for Cryptographic Controls" only.

2.2.3 Protection against brute force and dictionary attacks

Requirement:

Protection against brute force and dictionary attacks that hinder authentication attribute (i.e. password) guessing shall be implemented in LI system.
Brute force and dictionary attacks aim to use automated guessing to ascertain authentication attributes 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 on 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 Completely Automated Public Turing test to tell Computers and Humans Apart (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 LI system. An exception to this requirement is machine accounts.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.3.3]

2.2.4 Enforce Strong Password

Requirement:

a) The configuration setting shall be such that LI system 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 LI system). 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:
      1) At least 1 uppercase character (A-Z)

2) At least 1 lowercase character (a-z)
3) At least 1 digit (0-9)
4) 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 LI system.
e) When a user is changing a password or entering a new password, LI system /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.). Passwords shall not be stored in clear text in the system; passwords shall be salted and hashed.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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.
LI system 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 [3]: 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 shall be possible to implement this function on this system. Password change shall be enforced after initial login (after successful authentication).

LI system shall enforce password change based on password management policy. In particular, the system shall enforce password expiry. LI system shall support a configurable period for expiry of passwords.
Previously used passwords shall not be allowed up to a certain number (Password History). The number of disallowed previously used passwords shall be:

a) Configurable;
b) Greater than 0;
c) And its minimum value shall be 3. This means that the LI system shall store at least the three previously set passwords. The maximum number of passwords that the LI system 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.
LI system to have an 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 LI system.
The minimum password age shall be set as one day i.e., recycling or flipping of passwords to immediate return to favorite password is not possible.
The password shall be changed (need not be automatic) based on key events including, not limited to

- Indication of compromise (IoC)
- Change of user roles
- When a user leaves the organization

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.3.2]
[Ref [25]: CIS_Benchmarks_Password_Policy_Guide_v21.12]

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 "*".
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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.3.4]

2.2.8 Removal of predefined or default authentication attributes

Requirement:

Predefined or default authentication attributes shall be deleted or disabled. Normally, authentication attributes such as password or cryptographic keys will be pre-configured from the producer, Original Equipment Manufacturer (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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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. LI system shall be able to continue to operate without interactive sessions.
Only for debugging purposes, processes under a logged-in user ID may be allowed to continue to run after detaching the interactive session.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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 shall 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 shall also be

possible via configuration, with the exception of administrative accounts, which shall get only temporarily locked.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.5]

2.2.11 Suspend accounts on non-use

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 [34]: CIS Password Policy Guide]

Section 2.3: Software Security

2.3.1 Secure Update

Requirement:

a) Software package integrity shall be validated during the software update stage.
b) LI system shall support software package integrity validation via cryptographic means, e.g., digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only. To this end, the LI system has a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software update originated from only these sources.
c) Tampered software shall not be executed or installed if integrity check fails.
d) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software update and modify the list mentioned in (b) above.

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

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

2.3.2 Secure Upgrade

Requirement:

a) Software package integrity shall be validated during the software upgrade stage.
b) LI system shall support software package integrity validation via cryptographic means, e.g., digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only. To this end, the LI system has a

list of public keys or certificates of authorized software sources, and uses the keys to verify that the software upgrade 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 (b) above.

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

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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 Telecom Security Testing Laboratory (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 LI system software which includes OEM developed code, third party software and open-source code libraries used/embedded in the LI system.
   ii) LI system software shall be free from Common Weakness Enumeration (CWE) top 25, Open Worldwide Application Security Project (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 LI system and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in (ii) above.

[Ref [4]: https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html]

[Ref [5]: https://owasp.org/www-project-top-ten/]

[Ref [6]: https://owasp.org/www-project-api-security/]

2.3.4 Known Malware and backdoor Check

Requirement:

OEM shall submit an undertaking stating that LI system is free from all known malware and backdoors as on the date of offer of LI system to designated TSTL for testing and shall submit their internal Malware Test Document (MTD) of the LI system 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 LI system shall not be present/configured.
Orphaned software components /packages shall not be present in LI system.
OEM shall provide the list of software that are necessary for LI system's operation. In addition, OEM shall furnish an undertaking as "LI system does not contain software that is not used in the functionality of LI system."

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.3]

2.3.6 Unnecessary Services Removal

Requirement:

LI system shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. In particular, by default the following services shall be initially configured to be disabled on LI system by the vendor except if services are needed during deployment. In that case those services shall be disabled according to vendor's instructions after deployment is done. Disabled protocols may still need to be enabled for other reasons by the operators, e.g., remote diagnostics.
LI system shall not support following services:

a) File Transfer Protocol (FTP)
b) Trivial File Transfer Protocol (TFTP)
c) Telnet
d) rlogin, Rate Control Protocol (RCP), Remote Shell Protocol (RSH)
e) HTTP
f) Simple Network Management Protocol (SNMP) v1 and v2
g) SSHv1
h) Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) Small Servers (Echo, Chargen, Discard and Daytime)
i) Finger
j) Bootstrap Protocol (BOOTP) server
k) Discovery protocols (Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP))
l) IP Identification Service (Identd)
m) Packet Assembler/Disassembler (PAD)

n) Maintenance Operations Protocol (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 LI system and their purpose needs to be provided by the OEM as a prerequisite for the test case.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.1]

2.3.7 Restricting System Boot Source

Requirement:

The LI system can boot only from the memory devices intended for this purpose.

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

LI system shall establish a secure communication channel through standard interface with the Network Time Protocol (NTP) / Precision Time Protocol (PTP) server as per appropriate TEC ER (essential requirement) document.
LI system shall establish a secure communication channel strictly using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" with NTP/PTP server.
LI system shall generate audit logs for all changes to time settings.

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

2.3.9 Restricted reachability of services

Requirement:

LI system shall restrict the reachability of services so that they can only be reached 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 LI system 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, Hyper Text Transfer Protocol Secure (HTTPS), Remote Desktop Protocol (RDP)) shall be restricted to interfaces in the management plane to support separation of management traffic from user traffic.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.2]

2.3.10 Self -Testing

Requirement:

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

Section 2.4: System Secure Execution Environment

2.4.1 No unused functions

Requirement:

Unused functions i.e. the software and hardware functions which are not needed for operation or functionality of the LI system shall be permanently deactivated. Permanently means that they shall not be reactivated again after the LI 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 LI system 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 LI system.
EXAMPLE: A debugging function in software which can be used for troubleshooting shall not be activated during normal operation of the LI system.

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

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

2.4.2 No unsupported components

Requirement:

OEM to ensure that the LI system shall not contain software and hardware components that are no longer supported by them or their 3rd Parties (e.g., vendor, producer or developer) including the opensource communities, such as components that have reached end-of-life or end-of-support. An undertaking in this regard shall be provided by OEM.

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

LI system shall not contain any access mechanism which is unspecified or not declared. An undertaking shall be given by the OEM as follows:
The LI system shall not contain any wireless, optical, magnetic or any other component that may be used as a covert channel.

Section 2.5: User Audit

2.5.1 Audit trail storage and protection

Requirement:
The security event log shall be access-controlled (file access rights) so only privileged users have access to the log files.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.6.3]

2.5.2 Audit Event Generation

Requirement:

LI system shall log all important Security events with unique System Reference details as given in the table below.
LI system shall record within each audit record at least information pertaining to date and time of the event, type of event, subject identity, protocol, service or program used for access, source and destination IP addresses & ports 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:

Sr. No.	Event Types (Mandatory or Optional)	Description	Event data to be logged
1.	Incorrect login attempts (Mandatory)	Records any user's incorrect login	Username
			Source (IP address) if remote access

		attempts to the LI system	Outcome of event (Success or failure)
			Timestamp
2.	Administrator access (Mandatory)	Records any access attempts to accounts that have system privileges.	Username
			Timestamp
			Length of session
			Outcome of event (Success or failure)
			Source (IP address) if remote access
3.	Account administration (Mandatory)	Records all account administration activity, i.e. configure, delete, copy, enable, and disable.	Administrator username
			Administered account
			Activity performed (configure, delete, enable and disable)
			Outcome of event (Success or failure)
			Timestamp
4.	Resource Usage (Mandatory)	Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period have exceeded their defined thresholds.	Value exceeded
			Value reached
			(Here suitable threshold values shall be defined depending on the individual system.)
			Outcome of event (Success or failure)
			Timestamp
5.	Configuration change (Mandatory)		Change made
			Timestamp

		Changes to configuration of the LI system	Outcome of event (Success or failure)
			Username
6.	Reboot/shutdown/ crash (Mandatory)	This event records any action on the network device/LI system that forces a reboot or shutdown OR where the network device/LI system 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 LI system (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 (Mandatory)	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 (Mandatory)	Resetting of user account passwords by the Administrator	Administrator username
			Administered account
			Activity performed (configure, delete, enable and disable)

			Outcome of event (Success or failure)
			Timestamp
10.	Services (Mandatory)	Starting and Stopping of Services (if applicable)	Service Identity
			Activity performed (start, stop, etc.)
			Timestamp
			Outcome of event (Success or failure)
11.	X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
			Reason for failure
			Subject identity
			Type of event
12.	Secure update (Mandatory)	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.	Audit data changes (Mandatory)	Changes to audit data including deletion of audit data	Timestamp
			Type of event (audit data deletion, audit data modification)
			Outcome of event (Success or failure)
			Subject identity
			User identity

			Origin of attempt to change time (e.g., IP address)
			Details of data deleted or modified
17.	User Login (Mandatory)	All use of Identification and authentication mechanisms.	User identity
			Origin of attempt (IP address)
			Outcome of event (Success or failure)
			Timestamp

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.6.1]

2.5.3 Secure Log Export

Requirement:

a) LI system shall support (near real time) forwarding of security event logging data to an external system available in redundant configuration by push or pull mechanism through diverse links.
b) Log functions should support secure uploading of log files to a central location or to a system external for the LI system.
c) LI system 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 with the secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.6.2]

2.5.4 Logging access to personal data

Requirement:

In some cases, access to personal data in 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 [3]: TSDSI STD T1.33.117-17.1.0 V1.1.0. Section 4.2.3.2.5]

Section 2.6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirement:

LI system shall communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.
OEM shall submit to TSTL, the list of the connected entities with LI system 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 LI system (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards.
Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format along with self-certified test reports.
An undertaking is to be submitted by the OEM mentioning that "Cryptographic module embedded inside the LI system (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards."
[Ref [17]: ENISA Recommendation "Standardization in support of the cybersecurity certification", Dec 2019]
[Ref [8]: 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 LI system shall be in compliance with the respective latest FIPS standards (for the specific crypto algorithm).
Till further instructions, this clause will be considered ‘complied’ by submission of an undertaking by the OEM in specified format along with self-certified test reports.
An undertaking is to be submitted by the OEM mentioning that “Cryptographic algorithms implemented inside the Crypto module of LI system is in compliance with the respective latest FIPS standards (for the specific crypto algorithm embedded inside the LI system).”

2.6.4. Protecting data and information – Confidential System Internal Data

Requirement:

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

[Ref [3]: TSDSI STD T1.33.117-17.1.0 V1.1.0. 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 LI 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 “ITSAR for Cryptographic Controls” with appropriate non-repudiation controls.
b) In addition, the following rules apply for:
   i) Systems that need access to identification and authentication data in the clear/readable form e.g., in order to perform an activity/operation. Such systems shall not store this data in the clear/readable form, but scramble or encrypt it by implementation-specific means.
   ii) Systems that do not need access to sensitive data (e.g., user passwords) in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” only.
   iii) Stored files in the LI system shall be protected against manipulation strictly using Secure cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” only.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.2.3]

2.6.6 Protection against Copy of Data

Requirement:

a) Without authentication & authorization and except for specified purposes, LI system shall not create a copy of data in use or data in transit.
b) Protective measures should exist against use of available system functions / software residing in LI system to create a copy of data for illegal transmission.

2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement:

a) LI system shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.
b) Establishment of outbound overt channels such as, HTTPS, Instant Messaging (IM), Peer-to-Peer (P2P), Email etc. are to be forbidden if they are auto-initiated by / auto-originated from the LI system.
c) Session logs shall be generated for establishment of any session initiated by either user or LI system.

2.6.8 Protection against Data Exfiltration - Covert Channel

Requirement:

a) LI system shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit (within its boundary).
b) Establishment of outbound covert channels and tunnels such as Domain Name System (DNS) Tunnel, HTTPS Tunnel, Internet Control Message Protocol (ICMP) Tunnel, Transport Layer Security (TLS), Secure Sockets Layer (SSL), SSH, Internet Protocol Security (IPSec), Virtual Private Network (VPN), Real-time Transfer Protocol (RTP) Encapsulation etc. are to be forbidden if they are auto-initiated by / auto-originated from the LI system.
c) Session logs shall be generated for establishment of any session initiated by either user or LI system.

Section 2.7: Network Services

2.7.1 Traffic Filtering – Network Level Requirement

Requirement:

LI system shall provide a mechanism to filter incoming IP packets on any interface (Refer to RFC 3871)
In particular the LI system shall provide a mechanism:

a) To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of the stack ISO/Open Systems Interconnection (OSI).
b) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:
   i) Discard/Drop: the matching message is discarded; no subsequent rules are applied and no answer is sent back.
   ii) Accept: the matching message is accepted.
   iii) 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 the protocol header
e) To reset the accounting.
f) LI system shall provide a mechanism to disable/enable each defined rule.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.6.2.1]

[Ref [11]: RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.2 Traffic Separation

Requirement:

The LI system shall support the physical or logical separation of traffic belonging to different network domains. For example, OAM traffic and control plane traffic belong to different network domains. Refer to RFC 3871 for further information.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.3.5.1]

[Ref [11]: RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.3 Traffic Protection – Anti-Spoofing

Requirement:

LI system 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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.3.3.1.1]

Section 2.8: Attack Prevention Mechanisms

2.8.1 Network-level and Application-level DdoS

Requirement:

LI system shall have protection mechanisms against Network-level and Application-level Distributed Denial of Service (DDoS) attacks.
LI system shall provide security measures to deal with overload situations which may occur as a result of a denial-of-service attack or during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided.
Potential protective measures may include:

a) Restricting available RAM per application
b) Restricting maximum sessions for a Web/Database application
c) Defining the maximum size of a dataset
d) Restricting Central Processing Unit (CPU) resources per process
e) Prioritizing processes
f) Limiting amount or size of transactions of an user or from an IP address in a specific time range
g) Limiting amount or size of transactions to an IP address/Port Address in a specific time range

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.1]

2.8.2 Excessive Overload Protection

Requirement:

LI system shall act in a predictable way if an overload situation cannot be prevented. LI system shall be built in such a way that it can react to 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 a case it shall be ensured that LI system cannot reach an undefined and thus potentially insecure, state. In an extreme case this means that a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.

OEM shall provide a technical description of the LI system's overload control mechanisms. (especially whether these mechanisms rely on cooperation of other network elements)

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.3]

2.8.3 Interface robustness requirements

Requirement:

LI system shall be not 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 LI system. 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:

a) Mass-produced TCP packets with a set Synchronize (SYN) flag to produce half-open TCP connections (SYN flooding attack).
b) Packets with the same IP sender address and IP recipient address (Land attack).
c) Mass-produced ICMP packets with the broadcast address of a network as target address (Smurf attack).
d) Fragmented IP packets with overlapping offset fields (Teardrop attack).
e) ICMP packets that are larger than the maximum permitted size (65,535 Bytes) of IP version 4 (IPv4) packets (Ping-of-death attack).
f) Uncorrelated reply packets (i.e. packets which cannot be correlated to any request).

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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 LI system are reasonably robust when receiving unexpected input.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.4.4]

2.9.2 Port Scanning

Requirement:

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

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.4.2]

2.9.3 Vulnerability Scanning

Requirement:

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

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

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

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

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

[Ref [9]: https://nvd.nist.gov/vuln-metrics/cvss]

[Ref [28]: GSMA NG 133 Cloud Infrastructure Reference Architecture]

Section 2.10: Operating System

2.10.1 Growing Content Handling

Requirement:

a) Growing or dynamic content shall not influence system functions.
b) A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop LI system from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided. The countermeasures are usage of dedicated filesystems, separated from main system functions, or quotas, or at least a file system monitoring.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.4.1.1.1]

2.10.2 Handling of ICMP

Requirement:

Processing of ICMP version 4 (ICMPv4) and ICMP version 6 (ICMPv6) packets which are not required for operation shall be disabled on the LI system.
In particular, there are certain types of ICMPv4 and ICMPv6 that are not used in most networks, but represent a risk.
ICMP message types which on receipt lead to responses or to configuration changes are not mentioned in this requirement, but they may be necessary to support relevant and specified networking features. Those must be documented.
Certain ICMP types are generally permitted and do not need to be specifically documented. Those are marked as "Permitted" in the table below.
LI system shall not send certain ICMP types by default but it may support the option to enable utilization of these types (e.g., for debugging) 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

LI system 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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.4.1.1.2.]

2.10.3 Authenticated Privilege Escalation only

Requirement:

LI system shall not support 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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.4.1.2.1]

2.10.4 System account identification

Requirement:

Each system user account in LI system shall have a unique User ID (UID) with appropriate non-repudiation controls.

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

a) IP Packet Forwarding between different interfaces of the network product.
b) Proxy Address Resolution Protocol (ARP) (to prevent resource exhaustion attack and man-in-the-middle attacks)
c) Directed broadcast (to prevent attacks like Smurf, Denial of Service etc.,)
d) 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.
e) Gratuitous ARP messages (to prevent ARP Cache Poisoning attacks)

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

LI system 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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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:

LI system 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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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 LI system 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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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:

LI system 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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section - 4.3.2.7]

2.10.10 SYN Flood Prevention

Requirement:

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

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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, LI system 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:

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

Section 2.11: Web Servers

This entire section of the security requirements is applicable if the LI system **supports web management interface.**

2.11.1 HTTPS

Requirement:

The communication between LI system Web client and LI system Web server shall be protected strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.2.5.1]

2.11.2 Webserver logging

Requirement:

Access to the webserver (for both successful as well as failed attempts) shall be logged by LI system.

The web server log shall contain the following information:

a) Access timestamp
b) Source (IP address)
c) Account (if known)
d) Attempted login name (if the associated account does not exist)
e) Relevant fields in http request. The Uniform Resource Locator (URL) should be included whenever possible.
f) Status code of web server response

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.2.5.2]

2.11.3 HTTPS input validation

Requirement:

LI system web server shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.
LI system web server 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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.2.5.4]

2.11.4 No system privileges

Requirement:

No LI system web server processes shall run with system privileges. If a process is started by a user with system privileges, execution shall be transferred to a different user without system privileges after the start.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.3.4.2]

2.11.5 No unused HTTPS methods

Requirement:

HTTPS methods that are not required for LI system operation shall be deactivated.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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 LI system operation.
In particular, Common Gateway Interface (CGI) or other scripting components, Server Side Includes (SSI), and Web based Distributed Authoring and Versioning (WebDAV) shall be deactivated if they are not required.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.3.4.4]

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

Requirement:

If CGI or other scripting technology is used, the CGI directory or other corresponding scripting directory shall not include compilers or interpreters.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.3.4.6]

2.11.9 No execution of system commands with SSI

Requirement:

If SSI is active, the execution of system commands shall be deactivated.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.3.4.7]

2.11.10 Access rights for web server configuration

Requirement:

Access rights for LI system web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges. Implementation example: Delete "read" and "write" access rights for "others." Only grant "write" access to the user who configures the web server.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.3.4.8]

2.11.11 No default content

Requirement:

Default content (examples, help files, documentation, aliases) that is provided with the standard installation of the LI system web server shall be removed.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.3.4.9]

2.11.12 No directory listings

Requirement:

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

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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 LI system web server and the modules/add-ons used.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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 LI system web server and the modules/add-ons used. Error messages shall not include internal information such as internal server names, error codes, etc. Default error pages of the LI system web server shall be replaced by error pages defined by the OEM.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.3.4.12]

2.11.15 Minimized file type mappings

Requirement:

File type or script-mappings that are not required for LI system operation shall be deleted e.g., php, phtml, js, sh, csh, bin, exe, pl, vbe, vbs.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 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 (e.g., via links or in virtual directories) reside in the LI system web server's document directory.
In particular, the LI system web server shall not be able to access files which are not meant to be delivered.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.3.4.14]

2.11.17 HTTP User sessions

Requirement:

To protect user sessions, LI system web server shall support the following session ID and session cookie requirements:

a) The session ID shall uniquely identify the user and distinguish the session from all other active sessions.
b) The session ID shall be unpredictable.

c) The session ID shall not contain sensitive information in clear text (e.g., account number, social security, etc.).
d) In addition to the Session Idle Timeout, LI system web server shall automatically terminate sessions after a configurable maximum lifetime. This maximum lifetime defines the maximum session span. When the maximum lifetime expires, the session shall be closed, the session ID shall be deleted and the user shall be forced to (re)authenticate in the web application and to establish a new session. The default value for this maximum lifetime shall be set to 8 hours.
e) Session ID's shall be regenerated for each new session (e.g., each time a user logs in).
f) The session ID shall not be reused or renewed in subsequent sessions.
g) LI system 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.
h) Where session cookies are used the attribute 'Http Only' shall be set to true.
i) Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.
j) 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.
k) LI system shall not accept session identifiers from GET/POST variables.
l) LI system shall be configured to only accept server generated session ID's.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.2.5.3]

Section 2.12: Other Security requirements

2.12.1 Remote Diagnostic Procedure – Verification

Requirement:

If the LI system 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:

a) User id
b) Time stamp
c) Interface type
d) Event type (e.g., CRITICAL, MAJOR, MINOR)
e) Command/activity performed
f) Result type (e.g., SUCCESS, FAILURE).
g) IP Address of remote machine

[Ref [50]: GSMA NG 133: GSM Association Non-confidential Official Document NG.133 - Cloud Infrastructure Reference Architecture managed by OpenStack section 2.2.7.7]

2.12.2 No System Password Recovery

Requirement:

No provision shall exist for System / Root password recovery in LI system.

2.12.3 Secure System Software Revocation

Requirement:

Once the LI system 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 only by the administrator with appropriate non-repudiation controls.
LI system shall support a well-established control mechanism for rolling back to previous software image.

2.12.4 Software Integrity Check – Installation

Requirement:

LI system shall validate the software package integrity before the installation stage strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” only.
Tampered software shall not be executed or installed if integrity check fails.

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

2.12.5 Software Integrity Check – Boot

Requirement:

The LI system 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 “ITSAR for Cryptographic Controls” to the expected reference value.

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

2.12.6 Unused Physical and Logical Interfaces Disabling

Requirement:

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

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

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

2.12.7 Predefined accounts shall be deleted or disabled

Requirement:

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

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

Chapter 3 – Specific Security Requirements

3.1 LI_HI1 and LI_HIQR related Requirements

3.1.1 Input validation against schema

Requirement:

If a Receiver receives a warrant information (WI) message which does not conform to the relevant schema (either XSD or JSON), it shall not attempt to process any of the contents. It shall respond with a top-level Action Unsuccessful message containing a suitable error code.

[Ref [35]: ETSI TS 103.120 v1.14.1 Section 9.2.2]

3.1.2 Message signing and/or encryption

Requirement:

XML-encoded messages must be digitally signed and/or encrypted. The signature information shall be placed in element as the last child element of the root message element. If the national profile specifies the relevant details for populating the signature element, that must be adhered.
For JSON-encoded messages, best practice is expected for encryption like JSON Object Signing and Encryption (JOSE) standard.

[Ref [35]: ETSI TS 103.120 v1.14.1 Section 9.2.4]
[Ref [36]: IETF https://datatracker.ietf.org/wg/jose/charter/]

3.1.3 Mutual Authentication

Requirement:

Implementation shall use mutual authentication using pre-shared keys as defined in RFC 4279. Secure cryptographic controls prescribed in Table 1 of the latest document "Indian Telecommunication Security Assurance Requirements (ITSAR) for Cryptographic Controls" shall only be used wherever required.

[Ref [35]: ETSI TS 103.120 v1.14.1 Section 9.3.4]

3.1.4 Transport Security

Requirement:

Implementation shall use HTTPS as defined in RFC 2818 with TLS v1.2 or above. Caching shall not be used.

Secure cryptographic controls prescribed in Table 1 of the latest document "Indian Telecommunication Security Assurance Requirements (ITSAR) for Cryptographic Controls" shall only be used.

[Ref [35]: ETSI TS 103.120 v1.14.1 Section 9.3.4]

3.2 Internal Handover interfaces LI_HI2, LI_HI3 and LI_HI4 related Requirements

3.2.1 Confidentiality, Authentication and Handover Integrity

Requirement:

The requirements for Confidentiality, Authentication and Handover Integrity shall be met either by using a VPN application or below methods.

1. To support the requirement for confidentiality and authentication,

   a) TLS 1.2 as defined in IETF RFC 5246 [46] and IETF RFC 7525 [47] shall be used.
   b) New implementations should support TLS 1.3 as defined in IETF RFC 8446 [48].

2. For Authentication, X.509 certificates as per IETF RFC 6818 [49] shall be used.

3. For Integrity support,

   a) To verify the integrity of the received intercepted data, the Handover Manager periodically may insert hash-based message digests into the data stream.
   b) To be able to prove the integrity and authenticity of these hash-based message digests, periodically a digitally signed message digest may be inserted.
   c) To support integrity checks, the following process is recommended:
   d) Within each Chain, a Hash is generated over the previously sent Data-PDUs and sent:
      i. when <hash-Timeout> is reached (timer starts when the first Data-PDU is to be included in the hash and is reset after <hash-timeout> is reached); or
      ii. when <data-Pdu-Count> of Data-PDUs are sent; or
      iii. when the intercept on the target is terminated and there are un-hashed-Data-PDUs.

   The included-Sequence-Numbers sequence shall contain the sequence numbers of the Data-PDUs over which the hash is computed, in the order they were included in the hash calculation.

   Within each Chain, a signature is generated and sent over the previously sent Hashes:

i. when <sign-Timeout> is reached (timer starts when the first hash is to be included in the signature and reset after <sign-timeout> is reached); or
ii. when <hash-Pdu-Count> of hashes are sent; or
iii. when the intercept on the target is terminated and there are unsigned hashes.

The included-Sequence-Numbers sequence shall contain the sequence numbers of the Integrity-Check PDUs over which the signature is computed, in the order they were sent.

[Ref [37]: ETSI TS 102.232-1 v3.30.1 Section 7.2 Security; Annex J: implementation of integrity checks]

3.3 X1 interface related Requirements

3.3.1 Message transport

Requirement:

HTTP/2 shall be used with TLS v1.2 or above.
X1 implementation must have configurable parameters, e.g. port, http request path etc.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 Section 7.2.2]

3.3.2 Authentication

Requirement:

X1 Implementation shall perform mutual authentication using X.509 certificates following IETF RFC 6125. Implementation shall ensure that it is configurable on which certificates are used.
The X1 architecture and message exchange technique shall provide both authentication of physical end points and authentication of the software application receiving the message.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 Section 8.2.4 and A.3]

3.3.3 Authorization

Requirement:

The X1 architecture and message exchange technique shall provide both authorization of physical end points and authorization of the software application receiving the message.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 A.3]

3.3.4 Accounting and audit

Requirement:

The X1 architecture and message exchange technique shall include sufficient information to enable Accounting & Auditing functions in the ADMF and NE. Information like 'ADMF Identifier, NE Identifier, Target Identifier, Message Timestamp, Version, X1TransactonID, Type of request, Protocol Error Details etc.' shall be included at the minimum.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 A.3]

3.3.5 Integrity protection

Requirement:

The X1 message exchange technique shall provide integrity protection for all messages exchanged between nodes in the X1 architecture. Use of Integrity protection shall be mandatory.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 A.3]

3.3.6 Confidentiality protection

Requirement:

The X1 message exchange technique shall provide confidentiality protection for all messages exchanged between nodes in the X1 architecture.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 A.3]

3.3.7 Replay protection

Requirement:

The X1 message exchange technique shall provide replay protection for all messages exchanged between nodes in the X1 architecture.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 A.3]

3.3.8 Standalone interface

Requirement:

The X1 architecture and message exchange technique shall be designed as a standalone physically dedicated LI interface. The design and selection of the protocol shall where possible ensure vulnerabilities in non-LI interfaces on the same node shall not impact LI interfaces and security.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 A.3]

3.3.9 Hardened protocol

Requirement:

The X1 message exchange technique shall use a hardened protocol containing minimal options or extensions which are not specifically required by X1.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 A.3]

3.3.10 Minimum security level

Requirement:

The X1 architecture and message exchange techniques shall provide a minimum level of security (including cypher suites and key length), which shall be supported by all nodes. At least two algorithms shall be specified. The protocol and algorithms shall be resistant to bid down attack.
Secure cryptographic controls prescribed in Table 1 of the latest document "Indian Telecommunication Security Assurance Requirements (ITSAR) for Cryptographic Controls" shall only be used.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 A.3]

3.3.11 Underlying infrastructure trust

Requirement:

The X1 architecture and message exchange techniques shall assume by default that the underlying network communication links and infrastructure are untrusted.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 A.3]

3.3.12 Firewall and NAT transversal

Requirement:

The X1 message exchange technique shall be compatible with existing operator firewall and NAT transversal architectures. The message exchange technique shall not require unrestricted opening of common ports (e.g. port 80 or 21). The message exchange technique shall not prohibit the development of future X1 aware firewall filtering to provide rejection of malicious X1 message at operator security gateways.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 A.3]

3.3.13 Certificate and key management

Requirement:

The X1 architecture and message exchange techniques shall include (where applicable) Certificate and Key Management mechanisms. In addition, mechanisms for Certificate/Key revocation shall be provided.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 A.3]

3.3.14 Single node compromise

Requirement:

The X1 architecture and message exchange techniques shall ensure that a vulnerability or weak implementation in one node does not adversely affect other nodes. Specifically, it shall not be possible to attack one interception node by using recovered plan text or other security parameters from a vulnerable one.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 A.3]

3.3.15 Node administration

Requirement:

The X1 architecture and message exchange techniques shall ensure by design that within node implementations, non-LI super-users can be prevented from making LI related parameters changes without authority from and knowledge of the LI administrator.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 A.3]

3.3.16 Encryption of target information

Requirement:

It shall be possible to use encrypted target information only by use of encrypted targets and encryption keys. In case of encrypted information, it shall be possible to change encrypted target information and encryption keys periodically without interruption of any active interception.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 A.3]

3.4 X2/X3 interfaces related Requirements

3.4.1 Message transport

Requirement:

HTTP/2 shall be used with TLS v1.2 or above.
X2/X3 implementation must have configurable parameters, e.g. port, http request path etc.

[Ref [39]: ETSI TS 103.221-2 v1.6.1 Section 6.2]

3.4.2 Authentication and Authorization

Requirement:

The architecture and message exchange technique shall provide authentication and authorization of end points. Implementation shall perform mutual authentication using X.509 certificates following IETF RFC 6125. Implementation shall ensure that it is configurable which certificates are used.

[Ref [39]: ETSI TS 103.221-2 v1.6.1 Section 6.2.3 and A.2, A4]

3.4.3 Accounting and audit

Requirement:

The architecture and message exchange technique shall provide Accounting and Auditing.

[Ref [39]: ETSI TS 103.221-2 v1.6.1 A.2, A4]

3.4.4 Integrity protection

Requirement:

The message exchange technique shall provide integrity protection for all messages exchanged between nodes in the X2/X3 architecture. Use of Integrity protection shall be mandatory.

[Ref [39]: ETSI TS 103.221-2 v1.6.1 A.2, A4]

3.4.5 Confidentiality protection

Requirement:

The message exchange technique shall provide confidentiality protection for all messages exchanged between nodes in the X2/X3 architecture.

[Ref [39]: ETSI TS 103.221-2 v1.6.1 A.2, A4]

3.4.6 Replay protection

Requirement:

The message exchange technique shall provide replay protection for all messages exchanged between nodes in the X2/X3 architecture.

[Ref [39]: ETSI TS 103.221-2 v1.6.1 A.2, A4]

3.4.7 Standalone interface

Requirement:

The X2/X3 architecture and message exchange technique shall be designed as a standalone physically dedicated LI interface. The design and selection of the protocol shall where possible ensure vulnerabilities in non-LI interfaces on the same node shall not impact LI interfaces and security.

[Ref [39]: ETSI TS 103.221-2 v1.6.1 A.2, A4]

3.4.8 Minimum security level

Requirement:

The X2/X3 architecture and message exchange techniques shall provide a minimum level of security (including cypher suites and key length), which shall be supported by all nodes. At least two algorithms shall be specified. The protocol and algorithms shall be resistant to bid down attack.
Secure cryptographic controls prescribed in Table 1 of the latest document "Indian Telecommunication Security Assurance Requirements (ITSAR) for Cryptographic Controls" shall only be used.

[Ref [39]: ETSI TS 103.221-2 v1.6.1 A.2, A4]

3.4.9 Underlying infrastructure trust

Requirement:

The X2/X3 architecture and message exchange techniques shall assume by default that the underlying network communication links and infrastructure are untrusted.

[Ref [39]: ETSI TS 103.221-2 v1.6.1 A.2, A4]

3.4.10 Firewall and NAT transversal

Requirement:

The X2/X3 message exchange technique shall be compatible with existing operator firewall and NAT transversal architectures. The message exchange technique shall not require unrestricted opening of common ports (e.g. port 80 or 21). The message exchange technique shall not prohibit the development of future X1 aware firewall filtering to provide rejection of malicious X1 message at operator security gateways.

[Ref [39]: ETSI TS 103.221-2 v1.6.1 A.2, A4]

3.4.11 Certificate and key management

Requirement:

The X2/X3 architecture relies on (where applicable) Certificate and Key Management mechanisms (including Certificate and Key revocation) from X1.

[Ref [39]: ETSI TS 103.221-2 v1.6.1 A.2, A

3.5 LI_XER, LI_XEM1, LI_XQR interfaces related Requirements

Requirement:

LI_XER records shall be realised using a TLS connection. TLS v1.2 or above shall be used.
LI_XQR and LI_XEM1 requests shall be realised using ETSI TS 103 221-1.

[Ref [40]: 3GPP TS 33.128 v17.10.0 section 4.2, 5.8, 5.9]

3.6 LI system Database related Requirements

LI system generally employs an internal database. Any structured or unstructured database, if used, shall only store data temporarily to meet LI requirements. Permanent storage of any LI related sensitive data is not allowed. In any case, strict database security shall be ensured.

3.6.1 Removal of default accounts in database

Requirement:

All default or predefined accounts (e.g., test@localhost) that are not required for the operation of the LI system database shall be deleted permanently.

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

3.6.2 Renaming of root/admin account in the database

Requirement:

The administrative (superuser) account on a LI system database (used for database administration) shall not have a simple/well-known name such as 'root@localhost' in order to avoid exposing a highly privileged account with an easy to guess name.

[Ref [29]: ITSAR for HSS V1.0.0 section 3.2]

3.6.3 Removal of default database

Requirement:

Default or test databases that are not required for normal operation of LI system shall be deleted.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.3]

3.6.4 Password management for the database

Requirement:

LI system database shall only accept passwords that comply with the following complexity criteria:

a) Absolute minimum length of 8 characters (shorter lengths shall be rejected by the network product). It shall not be possible setting this absolute minimum length to a lower value by configuration.

b) Comprising at least three of the following categories:

   i) at least 1 uppercase character (A-Z)

   ii) at least 1 lowercase character (a-z)

   iii) at least 1 digit (0-9)

   iv) at least 1 special character (e.g., @;!$.)

The default minimum length of password in the LI system database shall be 10 characters. The minimum length of characters in the passwords shall be configurable by the operator. If a central system is used for user authentication, password policy is performed on the central system and additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this subclause. If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the LI system Database. When a user is changing a password or entering a new password, the system checks and ensures that it meets the password requirements.

c) Following password expiration and reuse policy shall be used:

   i) Password Expiration: Change immediately based on events, with an expiration "backstop" as per operator determined policy.

   ii) Password reuse restrictions: To prevent old passwords from being chosen again, reuse of at least last ~~5~~ n passwords ('n' shall be as per operator policy) shall be denied.

d) At least two-factor authentication shall be used for LI system database access.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.3.1]
[Ref [25]: CIS_Benchmarks_Password_Policy_Guide_v21.12

3.6.5 Protection of the LI system database

Requirement:

LI system database shall be protected as detailed below:

For sensitive data in (persistent or temporary) storage read access rights shall be restricted. Files of a system that are needed for the functionality shall be protected against manipulation.

In addition, the following rules apply for:
- Systems that need access to identification and authentication data in the clear, e.g. in order to perform an authentication. Such systems shall not store this data in the clear, but scramble or encrypt it by implementation-specific means.
- Systems that do not need access to sensitive data (e.g. user passwords) in the clear. Such systems shall hash this sensitive data.
- Stored files on the network product: examples for protection against manipulation are the use of cryptographic methods.

Wherever encryption/hashing is mandated it shall be as per cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls".

[Ref [3]: TSDSI STD T1.33.117-17.1.0 V1.1.0. Section 4.2.3.2.3]

3.6.6 Database specific logging

Requirement:

a) Security events related to following database events shall be logged together with a unique reference (e.g., database name, user ID accessing the database) and the exact time the incident occurred.
   i) Database Management Server Login (success or error) events
   ii) Attempted/executed database statements/queries
b) Information available in the logs about authentication attributes shall be masked.
c) LI system shall support real-time forwarding of security event logging data to an external system. Secure transport protocols shall be used in accordance with section 2.1.2 of the current document.
d) Log functions should support secure uploading of log files to a central location or to an external system for the LI system database that is logging.

[Ref [3]: TSDSI STD T1.33.117-17.1.0 V1.1.0. Section 4.2.3.6]

3.6.7 User privileges on the database

Requirement:

All LI system database users shall perform only the operations that are permitted to them (as per the privileges assigned to them). Principle of 'least privilege' shall be used.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.6.1 and 4.2.3.4.6.2]

3.6.8 Unique Identity

Requirement:

All database user accounts shall be uniquely identified (for e.g., username, hostname) by the LI system database.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.1.2 and Section 4.2.4.2.2]

3.6.9 Protection from attacks

Requirement:

a) LI system database shall be protected from database injection attacks.
b) Port used by the database service shall not be accessed by unauthorized entities. LI system database shall use a different port other than the default port for its connections.
c) Database shall recover securely from corruption, loss, damage.
d) Database shall support security mechanisms to protect from DDoS attacks.
e) Database systems 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.
f) Potential protective measures shall include, but is not limited to the following:
   i) Use stored procedures instead of implementing Direct queries
   ii) The number of queries an account can issue per hour
   iii) The number of updates an account can issue per hour
   iv) The number of times an account can connect to the server per hour
   v) The number of simultaneous connections to the server by an account (global max_user_connections value is 10)
   vi) Validating and encoding all user inputs

[Ref [21]: https://owasp.org/www-community/attacks/]

3.6.10 LI system Database Integrity

Requirement:

Systems and mechanisms shall be in place to ensure integrity of LI system database. The documentation on specific methods or approaches used to address the integrity of LI system database shall be provided.

3.6.11 LI system Database Availability

Requirement:

Systems and mechanisms shall be in place to ensure availability of LI system database. The documentation on specific methods or approaches used to address the availability of LI system database shall be provided.

3.6.12 Support for ‘Data Redaction’ and ‘Data Masking’ feature

Requirement:

LI system database shall support features of data redaction/log redaction and data masking to prevent exposure of sensitive data.

3.6.13 Terminate session on logout or session termination event

Requirement:

When a user logs out, or when any other session termination event occurs, the LI system database must delete the user session(s) to minimize the potential for session(s) to be hijacked.

[Ref [27]: NIST SP 800-53 Rev. 5: SC-23 SESSION AUTHENTICITY]

3.6.14 Fail in known secure state

Requirement:

The LI system database must transition to a known secure state if failure occurs.
The principle of secure failure indicates that components fail in a state that denies rather than grants access. That is, In a known secure state, neither a failure in a system function or mechanism nor any recovery action in response to failure leads to a violation of security policy. The system may provide all or part of the functionality of the original system, or it may completely shut itself down to prevent any further violation of security policies.

[Ref [27]: NIST SP 800-53 Rev. 5: SC-24 FAIL IN KNOWN STATE and SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES- (23), (24)]

3.6.15 Disable server-side scripting if not needed

Requirement:

The LI system database shall ensure that server-side scripting is disabled if not needed.

[Ref [30]: Security Standard –Database Management Systems (SS-005) section 11.2.3]

3.6.16 Restrict access using IP filtering

Requirement:

The LI system database shall restrict access using IP filtering.

[Ref [30]: Security Standard –Database Management Systems (SS-005) section 11.2.11]

3.6.17 Database backup

Requirement:

The mechanisms for data base backups and restoration shall be supported.

[Ref [30]: Security Standard –Database Management Systems (SS-005) section 11.5.1]

3.7 Other security requirements for LI system

3.7.1 Terminating faults

Requirement:
All LI terminating faults must be logged for reporting, correction and auditing with sufficient details. Local recovery procedures should be followed before a Task is ended with a "terminating fault". In general, irrecoverable failures with an interception, or major security issues at an NE shall be considered terminating faults.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 section 5.1.1]

3.7.2 Target list encryption

Requirement:

The target list needs to be encrypted, as may the output traffic on X1. Any encryption needs to be robust, and not under full control within the VM layer.

[Ref [43]: ETSI TR 103.308 v1.1.1 section 4.2]

3.7.3 LI system backup

Requirement:

LI system shall have the capability to backup all configurations necessary to restore the system. It shall have the capability to exclude selective data backup by LI authorized user.

3.7.4 LISSF data storage

Requirement:

The following restrictions on the use of the LISSF shall apply:

- The LISSF shall be subject to the same location, geographic, security and other physical environment constraints as the LI functions for which it is storing data.
- LI state information stored in an LISSF shall only be accessible by the LI functions specifically authorised by the LICF.
- Other than the time required to acquire the LI state information, the use and placement of an LISSF within the LI architecture shall not introduce additional delay.
- The LISSF shall be directly under the control of the ADMF, and it shall be directly accessible and auditable by the LICF.

[Ref [42]: 3GPP TS 33.127 V17.10.0 section 6.2.7]

3.7.5 Dedicated LI control interface

Requirement:

NE implementers are strongly discouraged from exposing additional interfaces for controlling the LI functionality of the NE other than by X1 (e.g. via a local administrative interface at the NE). If such additional interfaces exist, any such action performed on the NE shall be captured on the NE audit/logging, and any consequences of such actions shall be able to be seen and controlled by the ADMF that is responsible for the NE i.e. the ADMF shall be able to use the X1 interface to stop or undo any changes made over a local administrative interface.

[Ref [38]: ETSI TS 103.221-1 v1.15.1 section 4.3]

3.7.6 Rapid monitoring and reporting capability

Requirement:

LI nodes shall support capability for rapid monitoring and reporting of loss of LI services, link failures, any compromise of the LI system.

[Ref [43]: ETSI_TR_103.308 v1.1.1 section 4.2]
[Ref [44]: ETSI_gs_nfv-sec009 v1.1.1 section 4.5.2]

3.7.8 No storage of LI information on intermediate node(s)

Requirement:

No intermediate node within the nodes that form a part of the connection path may store information. Only the utilized and provided storage of the target VM that the LI stores its collected data at is the only correct place to store said data. If necessary for LI operation, temporary caching is allowed on intermediate node(s).

[Ref [43]: ETSI_TR_103.308 v1.1.1 section 6.2]

3.7.9 Secure logging for LI-specific logs

Requirement:

Logging for LI purposes are mandated to be in LI- specific secure logs which are protected from other storage and have access protection from unauthorized users or processes. Unless there is a specific reason, the details that are logged should be less sensitive information (e.g. LI reference numbers, or dates and times that target lists were updated) rather than more highly sensitive information (e.g. target details).

[Ref [44]: ETSI-GS-NFV-SEC009-section-4.5.3, 6.2]

3.7.10 System robustness against unexpected input

Requirement:

During transmission of data to a system it is necessary to validate input to LI system before processing. This includes all data which is sent to the system. Examples of this are user input, inputs from LI system’s consumers, 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 [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.2.3.3.4]

3.7.11 Security of backup data

Requirement:

LI system shall support mechanisms for taking backup of nodes configuration and log files and their restoration. An effective backup and restoration strategy shall be in place and documented.

[Ref [18]: “Security Guidance for 5G Cloud Infrastructure Part III: Data Protection” by NSA & CISA]

3.7.12 Secure deletion of sensitive data

Requirement:

LI system shall support secure deletion of sensitive data by authorized users in such a manner that it cannot be recovered through any forensic means.

[Ref [18]: “Security Guidance for 5G Cloud Infrastructure Part III: Data Protection” by NSA & CISA]

3.7.13 Isolation of Compromised Element

Requirement:

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

[Ref [19]: ENISA Security in 5G Specifications, Controls in 3GPP Security Specifications (5G SA) February 2021 Section 4.1.3]

3.7.14 LI System POI provisioning events log

Requirement:

LI system shall log additional important Security events related to LI POI provisioning (creation/deletion/modification) with unique System Reference details as given below.

i) User Identity
ii) Origin of attempt (IP address)
iii) Outcome of event (Success or failure)
iv) Time stamp
v) POI host node/NF identity

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.6.1]

Annexure-I

Definitions

1. **5G Access Network:** An access network comprising a NG-RAN and/or non-3GPP AN connecting to a 5G Core Network. [1]
2. **5G Core Network:** The core network specified in the present document. It connects to a 5G Access Network. [1]
3. **5G System:** 3GPP system consisting of 5G Access Network (AN), 5G Core Network and UE. [1]
4. **Capture:** The action taken by the CSP to separate and copy the communications associated with a target identifier. [41]
5. **Content of Communication (CC):** Information exchanged between two or more users of a communications service, excluding intercept related information. This includes information which may, as part of some communications service, be stored by one user for subsequent retrieval by another. [41]
6. **Chain:** integrity checks run within the context of a communication-Identifier. This means there are separate integrity check "chains" for each combination of LIID, communication-Identifier (communications session) and data-Type (IRI, CC or iLHI). Each Chain has its own sequence-Number counter. In normal circumstances this results in 4 (four) Chains/sequence-Number counters per communication-Identifier: CC/hashes, IRI/hashes, CC/signatures, IRI/signatures). For Inter LEMF handover as defined in ETSI TS 103 462 [45] this results in 2 (two) Chains/sequence-Number counters per communication-Identifier: iLHI/hashes, iLHI/signatures. [37]
7. **DataPDU:** a PS-PDU containing either CC Payload, IRI payload or ILHI payload. [37]
8. **Data-Pdu-Count**: number of Data-PDUs after which a hash shall be generated. Value is up to national agreement; typical value is 1000. [37]
9. **DDoS**: DDoS is a distributed denial-of-service attack that renders the victim un-usable by the external environment.
10. **Generic Network Product:** Generic Network Product (GNP) model as defined in Section 4.1 and 4.3 of TSDSI RPT T1.3GPP 33.926-16.4.0 V1.0.0. [24]
11. **Generic virtualized network product model (GVNP) Type 1**: GVNP Model as defined in Section 5.2.3 of TSDSI RPT T1.3GPP 33.818-17.1.0 V1.0.0. [23]
12. **Generic virtualized network product model (GVNP)Type 2:** GVNP Model as defined in Section 5.2.3 of TSDSI RPT T1.3GPP 33.818-17.1.0 V1.0.0. [23]
13. **Generic virtualized network product model (GVNP)Type 3:** GVNP Model as defined in Section 5.2.3 of TSDSI RPT T1.3GPP 33.818-17.1.0 V1.0.0. [23]

14. **Hash:** An Integrity-Check PDU with check-Type hash (1), containing a Secure Hash Algorithm (SHA), described in the NIST publication FIPS PUB 180-4. The SHA type is up to national agreement, optionally identified by the hash Algorithm ASN.1 field.
15. **Handover Manager**: The task of the Handover Manager (HM) is to handover intercepted data of all running intercepts to the appropriate destination(s).
16. **Hash-Pdu-Count**: number of Hashes after which a signature shall be generated. Value is up to national agreement; typical value is 15.[37]
17. **Hash-Timeout:** number of seconds after which a hash shall be generated. Value is up to national agreement; typical value is 1 second.[37]
18. **Home Environment:** responsible for overall provision and control of the Personal Service Environment of its subscribers. [10]
19. **Interception:** The actions of Provisioning, Detection, Capture, Delivery, and De-Provisioning. [41]
20. **Interception product:** The Intercept Related Information (IRI) and/or Content of Communication (CC) generated as a result of isolating the target's communications or identities for the purpose of delivery to the requesting LEA. [41]
21. **Intercept Related Information (IRI):** Information or data associated with communication services involving the target identity, specifically communication associated information or data (e.g. unsuccessful communication attempts), service associated information or data, and location information. [41]
22. **Lawful Access Location Services (LALS):** A service provided by a CSP to an LEA in which action is performed by a CSP to obtain a target's location information by means of Location Services (LCS), and to provide that information to an LEA. [41]
23. **Lawful Interception (LI):** Actions taken by the CSP that include: provisioning the target identity in the network to enable isolation of target communications (separating it from other users' communications), duplicating the communications for the purpose of sending the copy to the LEA, and handing over the Interception Product to the LEA that served the CSP with the warrant. An interception is associated with exactly one warrant. [41]
24. **Lawful Interception Identifier (LIID):** Unique identifier that associates a warrant to Lawful Interception Product delivered by the CSP to the LEA. [41]
25. **LI delivery latency:** The time between isolation in the Point of Interception and delivery of the Product of Interception at the LEA at the agreed point of handover. [41]
26. **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. [3]
27. **Masking**: The process of systematically removing a field or replacing it with a value in a way that does not preserve the analytic utility of the value. [34]

28. **Medium Access Control**: A sub-layer of radio interface layer 2 providing unacknowledged data transfer service on logical channels and access to transport channels.
29. **Mobile Equipment (ME)**: The Mobile Equipment is functionally divided into several entities, i.e. one or more Mobile Terminations (MT) and one or more Terminal Equipment (TE). [3]
30. **Network Function:** A 3GPP adopted or 3GPP defined processing function in a network, which has defined functional behavior and 3GPP defined interfaces. NOTE 1: 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. [1]
31. **NF service:** a functionality exposed by a NF through a service-based interface and consumed by other authorized NFs. [1]
32. **NF Set ID**: A NF Set Identifier (NF Set ID) is a globally unique identifier of a set of equivalent and interchangeable Control Plane NFs from a given network that provide distribution, redundancy and scalability (see clause 5.21.3 of TS 23.501 [1]).
33. **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. [1]
34. **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) [1] [33]
35. **NSSAA**: Network Slice-Specific Authentication and Authorization-A serving PLMN or SNPN shall perform Network Slice-Specific Authentication and Authorization for the S-NSSAIs of the HPLMN or SNPN which are subject to it based on subscription information. The UE shall indicate in the Registration Request message whether it supports NSSAA feature. If the UE does not support NSSAA feature, AMF will not trigger the procedure. [1]
36. **NSSAI**: Network Slice Selection Assistance Information-The NSSAI is a collection of S-NSSAIs. 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]
37. **NSSF**: Network Slice Selection Function-The selection of the set of Network Slice instances for a UE is triggered by the first contacted AMF in a Registration procedure normally by interacting with the NSSF. [1]

38. **NSSI**: Network slice subnet instance-An instance of Network Slice Subnet representing the management aspects of a set of Managed Function instances and the used resources (e.g. compute, storage and networking resources). [1]
39. **NSSP**: Network Slice Selection Policy-This is used by the UE to associate the matching application with S- NSSAI. PCF provisions URSP rules to the UE. UE uses URSP rules (which contains NSSP) for associating the matching application with S-NSSAI. [1]
40. **NSSRG**: Network Slice Simultaneous Registration Group-The UE Subscription Information may contain restrictions to the simultaneous registration of network slices. This is provided to the serving AMF as part of the UE subscription, in the form of Network Slice Simultaneous Registration Group (NSSRG) information. [1]
41. **Personal data:** Any information relating to an identified or identifiable natural person ('data subject'). [3]
42. **Personal Service Environment:** contains personalized information defining how subscribed services are provided and presented towards the user. Each subscriber of the Home Environment has her own Personal Service Environment. The Personal Service Environment is defined in terms of one or more User Profiles. [10]
43. **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 (source: ITU-T I.112). [10]
44. **Protocol data unit (PDU):** In the reference model for OSI, a unit of data specified in an (N)-protocol layer and consisting of (N)-protocol control information and possibly (N)-user data (source: ITU-T X.200 / ISO-IEC 7498-1). [3]
45. **Public Land Mobile Network (PLMN):** A telecommunications network providing mobile cellular services. [3]
46. **Quality of Service (QoS):** The collective effect of service performances which determine the degree of satisfaction of a user of a service. It is characterized by the combined aspects of performance factors applicable to all services, such as;
    - service operability performance;
    - service accessibility performance;
    - service retainability performance;
    - service integrity performance; and
    - other factors specific to each service. [3]
47. **Redaction**: The removal of information from a document or dataset for legal or security purposes. [34]
48. **Secure state:** A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with an organizational security policy.
49. **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. [3]

50. **Serving Network:** The serving network provides the user with access to the services of home environment. [10]
51. **Signature:** An Integrity-Check PDU with check-Type signature (2), containing a DSS/DSA Signature as described in FIPS PUB 186-4. The choice of specific parameter sizes and SHA version to compute the DSA signature is up to national agreement. Generation and distribution of the DSA key is out of scope of the present document. [37]
52. **Sign-Timeout**: number of seconds after which a signature shall be generated. Value is up to national agreement; typical value is 300 seconds. [37]
53. **target identity:** A network or service identity that uniquely identifies a target for interception from all other non-targets within one or more CSP services. One target may have one or several target identities. The target identity can be a long-term subscription-based identity, a short-term network identity, a public identity or an internal (private) identity. [41]
54. **terminating fault:** fault signalled from NE to ADMF which terminates the specific Task. [41]
55. **Universal Subscriber Identity Module (USIM):** An application residing on the UICC used for accessing services provided by mobile networks, which the application is able to register on with the appropriate security. [3]
56. **User Equipment (UE):** Allows 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 the User Equipment is subdivided into the UICC domain and the ME Domain. The ME Domain can further be subdivided into one or more Mobile Termination (MT) and Terminal Equipment (TE) components showing the connectivity between multiple functional groups. [3]

Annexure-II

Acronyms

3GPP	-	Third Generation Partnership Project
4G	-	Fourth Generation
5G	-	Fifth Generation
5GC	-	5G Core
5GS	-	5G System
AAA	-	Authentication, Authorization and Accounting
ADMF	-	Admin Function
AF	-	Application Function
AMF	-	Access and Mobility Management Function
AN	-	Access Network
API	-	Application Programming Interfaces
ARP	-	Address Resolution Protocol
AS	-	Access Stratum
AUSF	-	Authentication Server Function
BOOTP	-	Bootstrap Protocol
CAPTCHA	-	Completely Automated Public Turing test to tell Computers and Humans Apart
CC	-	Content of Communication
CD	-	Compact DiskI
CDP	-	Cisco Discovery Protocol
CGI	-	Common Gateway Interface
CIS	-	Center for Internet Security
CISA	-	Cybersecurity and Infrastructure Security Agency
CLI	-	Command Line Interface
CN	-	Core Network
CP	-	Control Plane
CPU	-	Central Processing Unit
CWE	-	Common Weakness Enumeration
DDoS	-	Distributed Denial of Service
DN	-	Data Network
DNS	-	Domain Name System
DoT	-	Department of Telecommunications
DVD	-	Digital Versatile Disk
eMBB	-	Enhanced Mobile Broadband
ENISA	-	European Union Agency for Cybersecurity

EPC	-	Evolved Packet Core
ETSI	-	European Telecommunications Standards Institute
E-UTRA	-	Evolved Universal Terrestrial Radio
FIPS	-	Federal Information Processing Standards
FTP	-	File Transfer Protocol
gNB	-	Next Generation Node B
GUI	-	Graphical User Interface
GVNP	-	Generalized Virtual Network Product
HE	-	Home Environment
HM	-	Handover Manager
HTTP	-	Hypertext Transfer Protocol
HTTPS	-	Hyper Text Transfer Protocol Secure
ICF	-	Identifier Caching Function
ICMP	-	Internet Control Message Protocol
ICMPv4	-	ICMP version 4
ICMPv6	-	ICMP version 6
IE	-	Information Element
IEEE	-	Institute of Electrical and Electronics Engineers
IEF	-	Identifier Event Function
IETF	-	Internet Engineering Task Force
ILHI	-	Inter LEA Handover Interface
IMT	-	International Mobile Telecommunications
IP	-	Internet Protocol
IPSec	-	Internet Protocol Security
IPv4	-	IP version 4
IPv6	-	IP version 6
IRI	-	Intercept-Related Information
ISO	-	International Organization for Standardization
ISP	-	Internet service provider
IT	-	Information Technology
ITSAR	-	Indian Telecommunication Security Assurance Requirements
ITU	-	International Telecommunication Union
JSON	-	JavaScript Object Notation
JWS	-	JSON Web Signature
JWT	-	JSON Web Token
LALS	-	Lawful Access Location Services
LEA	-	Law Enforcement Agency
LEMF	-	Law Enforcement Monitoring Facility
LICF	-	LI Control Function
LIID	-	Lawful Intercept ID

LIPF	-	LI Provisioning Function
LISSF	-	LI State Storage Function
LLDP	-	Link Layer Discovery Protocol
LTE	-	Long Term Evolution
MAC	-	Medium Access Control
MDF	-	Mediation and Delivery Function
ME	-	Mobile Equipment
mMTC	-	Massive Machine Type Communication
MOP	-	Maintenance Operations Protocol
MTD	-	Malware Test Document
NAS	-	Non- Access Stratum
NCCS	-	National Centre for Communication Security
NEF	-	Network Exposure Function
NF	-	Network Function
NFV	-	Network Function Virtualization
NIST	-	National Institute of Standards and Technology
NR	-	New Radio
NRF	-	Network Repository Function
NSA	-	National Security Agency
NSA	-	Non -Standalone
NSACF	-	Network Slice Admission Control Function
NSI	-	Network Slice Instance
NSS	-	Network slice Subnet
NSSAA	-	Network Slice Specific Authentication and Authorization
NSSAI	-	Network Slice Selection Assistance Information
NSSF	-	Network Slice Selection Function
NSSI	-	Network slice subnet instance
NSSP	-	Network Slice Selection Policy
NSSRG	-	Network Slice Simultaneous Registration Group
NTP	-	Network Time Protocol
NTS	-	Network Time Security
OAM	-	Operations, Administration and Management
OEM	-	Original Equipment Manufacturer
OS	-	Operating System
OSI	-	Open Systems Interconnection
OWASP	-	Open Worldwide Application Security Project
P2P	-	Peer
PAD	-	Packet Assembler/Disassembler
PCF	-	Policy Control Function
PII	-	Personal Identifiable Information

PLMN	-	Public Land Mobile Network
POI	-	Point-Of-Intercept
PTP	-	Precision Time Protocol
QoS	-	Quality of Service
RAM	-	Random Access Memory
RAN	-	Radio Access Network
RAT	-	Radio Access Technology
RBAC	-	Role Based Access Control
RCP	-	Rate Control Protocol
RDP	-	Remote Desktop Protocol
REST	-	Representational State Transfer
RFC	-	Request For Comment
RPF	-	Reverse Path Filter
RSH	-	Remote Shell Protocol
RTP	-	Real Time Protocol
SA	-	Standalone
SBA	-	Service Based Architecture
SBI	-	Service Based Interface
SDN	-	Software Defined Networking
SFTP	-	Secure File Transfer Protocol
SHA	-	Secure Hash Algorithm
SIRF	-	System Information Retrieval Function
SMF	-	Session Management Function
SMS	-	Short Message Service
SN	-	Serving Network
SNMP	-	Simple Network Management Protocol
SSH	-	Secure Shell
SSI	-	Server Side Includes
SSL	-	Secure Sockets Layer
STD	-	Software Test Document
TCP	-	Transmission Control Protocol
TF	-	Triggering function
TFTP	-	Trivial File Transfer Protocol
TLS	-	Transport Layer Security
TSDSI	-	Telecommunications Standards Development Society, India
TSTL	-	Telecom Security Testing Laboratory
UDM	-	Unified Data Management
UDP	-	User Datagram Protocol
UDR	-	Unified Data Repository
UE	-	User Equipment

UID	-	User ID
UP	-	User Plane
UPF	-	User Plane Function
URL	-	Uniform Resource Locator
uRLLC	-	Ultra Reliable and Low Latency Communications
USB	-	Universal Serial Bus
USIM	-	Universal Subscriber Identity Module
VPN	-	Virtual Private Network
WebDAV	-	Web based Distributed Authoring and Versioning
WI	-	Warrant Information
WLAN	-	Wireless Local Area Network
XML	-	eXtensible Markup Language
XSD	-	XML Schema Definition

Annexure-III

List of Submissions

List of Undertaking to be furnished by the OEM for LI Security testing submissions.

1. Source Code Security Assurances (against test case 2.3.3)
2. Know Malware and backdoor check (against test case 2.3.4)
3. No unused software (against testcase 2.3.5)
4. No unsupported Components (against test case 2.4.2)
5. Avoidance of unspecified mode of 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 2.6.3)

Annexure-IV

References

1. TSDSI STD T1.3GPP 23.501 17.7.0 V1.3.0 “System architecture for the 5G System (5GS)”
2. TSDSI STD T1.3GPP 33.501-17.7.0 V1.1.0 “System architecture and procedures for 5G System”
3. TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 “Catalogue of general security assurance requirements”
4. https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html
5. https://owasp.org/www-project-top-ten/
6. https://owasp.org/www-project-api-security/
7. RFC 8915 - Network Time Security for the Network Time Protocol (NTP)
8. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
9. https://nvd.nist.gov/vuln-metrics/cvss
10. 3GPP TR 21.905 V17.1.0 (2021-12) “Vocabulary for 3GPP Specifications
11. RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure
12. RFC 6749 - The OAuth 2.0 Authorization Framework
13. RFC 7515 - JSON Web Signature (JWS)
14. RFC 7519 - JSON Web Token (JWT)
15. TSDSI STD T1.3GPP 33.127 17.7.0 V1.3.0 “Lawful Interception (LI) architecture and functions”
16. ENISA THREAT LANDSCAPE FOR 5G NETWORKS, Updated threat assessment for the fifth generation of mobile telecommunications networks (5G), December 2020
17. ENISA Recommendation “Standardization in support of the cybersecurity certification”, Dec 2019
18. “Security Guidance for 5G Cloud Infrastructure Part III: Data Protection” by NSA & CISA https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_III_508_Compliant.pdf
19. ENISA SECURITY IN 5G SPECIFICATIONS, Controls in 3GPP Security Specifications (5G SA) FEBRUARY 2021 Section 4.1.3 https://www.enisa.europa.eu/publications/security-in-5g-specifications
20. https://cheatsheetseries.owasp.org/cheatsheets/Database_Security_Cheat_Sheet.html
21. https://owasp.org/www-community/attacks/SQL_Injection#

22. TSDSI STD T1.3GPP 23.632-17.3.0 V1.2.0 “User data interworking, coexistence and migration”
23. TSDSI RPT T1.3GPP 33.818-17.1.0 V1.0.0 “Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products”
24. TSDSI RPT T1.3GPP 33.926-16.4.0 V1.0.0 “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes”
25. CIS_Benchmarks_Password_Policy_Guide_v21.12
26. MongoDB_Security_Architecture_WP.pdf
27. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
28. GSMA NG 133 Cloud Infrastructure Reference Architecture
29. ITSAR for HSS V1.0.0
30. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1175185/dwp-ss005-security-standard-database-management-systems.pdf
31. TSDSI STD T1.3GPP 29.536-17.2.0 V1.2.0
32. 3GPP TR 33.811 v15.0.0
33. https://www.gsma.com/newsroom/wp-content/uploads/NG.116-v8.0-1.pdf
34. https://csrc.nist.gov/glossary
35. ETSI TS 103.120 v1.14.1
36. IETF https://datatracker.ietf.org/wg/jose/charter/
37. ETSI TS 102.232-1 v3.30.1
38. ETSI TS 103.221-1 v1.15.1
39. ETSI TS 103.221-2 v1.6.1
40. 3GPP TS 33.128 v17.10.0
41. 3GPP TS 33.126 V17.4.0
42. 3GPP TS 33.127 V17.10.0
43. ETSI_TR_103.308 v1.1.1
44. ETSI_gs_nfv-sec009 v1.1.1
45. ETSI-GS-NFV-SEC003-v1.1.1
46. RFC 5246 Transport Layer Security
47. RFC 7525 Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)
48. RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3
49. RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
50. GSMA NG 133: GSM Association Non-confidential Official Document NG.133 - Cloud Infrastructure Reference Architecture managed by OpenStack section 2.2.7.7