सत्यमेव जयते

Indian Telecommunication Security Assurance Requirements (ITSAR)

Service Communication Proxy (SCP) of 5G

NCCS
Securing Networks

Draft For Comments

Release Date: Version: 1.0.0
Enforcement Date:

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

About NCCS

National Centre for communication Security (NCCS), with headquarters at Bengaluru was set up in 2018 with the objective to establish and operationalize a framework of security testing and certification within the country. Security Assurance Standards (SAS) division of NCCS is mandated to prepare Telecom security requirements/standards called Indian Telecom Security Assurance Requirements (ITSAR) that addresses the country specific security needs in telecommunication landscape and notify the same.

Document History

Sl. No	ITSAR Reference	Title	Remarks
1			

Contents

A) Outline:

The objective of this document is to present a comprehensive, country-specific security requirements for the Service Communication Proxy (SCP) network function of 5G Core. The SCP provides an option for Core NFs to communicate indirectly. It provides routing control, load balancing and delegated discovery.

The specifications produced by various regional/ international standardization bodies/ organizations/associations like 3GPP, ITU-T, ISO, ETSI, IEEE, IETF, NGMN, O-RAN, TIP, IRTF, GSMA,TSDSI along with the country-specific security requirements are the basis for this document.

This document commences with a brief description of 5G system architecture, SCP and its functionalities and then proceeds to address the common and entity specific security requirements of SCP.

B) Scope:

This document targets on the security requirements of the 5G Core- Service Communication Proxy function (SCP) as defined by 3GPP. This document does not cover the security requirements at the virtualization and infrastructure layers.

The regulations regarding Remote Access and Lawful Interceptions are not part of this ITSAR. The requirements specified here are binding both on operators (aka Telecommunication Service Provider- TSP) and network equipment providers (aka OEMs- Original Equipment Manufacturer).

C) Conventions

1. Must or shall or required denotes the absolute requirement of a particular clause of ITSAR.
2. Must not or shall not denote absolute prohibition of a particular clause of ITSAR.
3. Should or Recommended denotes that the 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

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

5G Architecture: The generic 5G system (5GS) architecture consists of User Equipment, Radio Access Network supporting New Radio (NR) and the cloud-native 5G core networks (5G-CN). 5G base station is called as Next Generation Node B (gNB). The deployment strategies possible are Non-Stand Alone (NSA) and Stand Alone (SA). SA denotes 5G NR connecting to 5G CN. In NSA mode, 5G NR gets connected to 4G EPC but uses LTE as anchor in control plane.

5G Core Network: Core network is the central part of mobile network. 5G Core network provides authentication, security, mobility management, session management services and enables the subscribers to avail the services. These functionalities are specified as "network functions". Some of the important core network functions are 1) AMF 2) SMF 3) AuSF 4) UPF 5)AF 6) NEF 7)NRF 8)PCF 9)UDM 10)UDR

The salient features of 5G Core are

1) Separation of user plane and control plane
2) Service Based Architecture (SBA)
3) Network Slicing
4) Network function virtualization and Software Define Networking
5) Automation
6) Access Agnostic
7) Framework for policy control and support of QoS
8) Secure exposure of network functions to 3rd party providers

In a SBA framework, the individual elements are defined as Network Functions (NFs) instead of Network entities. Through Service Based Interface (SBI) each of the NFs consumes services offered by other service producer-other NFs. RESTful APIs are used in 5G SBA which use HTTP/2 as application layer protocol.

Service Communication Proxy (SCP): The Service Communication Proxy (SCP) includes one or more of the following functionalities. Some or all of the SCP functionalities may be supported in a single instance of an SCP:

- Indirect Communication.
- Delegated Discovery.
- Message forwarding and routing to destination NF/NF service.
- Message forwarding and routing to a next hop SCP.
- Communication security (e.g. authorization of the NF Service Consumer to access the NF Service Producer API), load balancing, monitoring, overload control, etc.
- Optionally interact with UDR, to resolve the UDM Group ID/UDR Group ID/AUSF Group ID/PCF Group ID/CHF Group ID/HSS Group ID based on UE identity, e.g. SUPI or IMPI/IMPU (see clause 6.3.1 for details).

SCPs can be deployed at PLMN level, shared-slice level and slice-specific level. It is left to operator deployment to ensure that SCPs can communicate with relevant NRFs.

In order to enable SCPs to route messages through several SCPs (i.e. next SCP hop discovery), an SCP may register its profile in the NRF. Alternatively, local configuration may be used.

Chapter 2 – COMMON SECURITY REQUIREMENTS

Section 1: Access and Authorization

2.1.1 Management Protocols Mutual Authentication

Requirement:

The network product management shall support mutual authentication mechanisms, the mutual authentication mechanism can rely on the protocol used for the interface itself or other means.

Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" shall only be used for SCP management and maintenance.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.4.1]

2.1.2 Management Traffic Protection

Requirement:

SCP management traffic shall be protected strictly using secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.4]

2.1.3 Role-based access control policy

Requirement:

SCP shall support Role-Based Access Control (RBAC). A role-based access control system uses a set of controls that determines how users interact with domains and resources.
The RBAC system controls how users or groups of users are allowed access to the various domains and what type of operation they can perform, i.e., the specific operation command

or command group (e.g View,Modify ,Execute). SCP supports RBAC with minimum of 3 user roles, in particular, for OAM privilege management for SCP Management and Maintenance, including authorization of the operation for configuration data and software via the network product console interface.

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

2.1.4. User Authentication – Local/Remote

Requirement:

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

- Cryptographic keys
- Token
- Passwords

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.2.1]

2.1.5 Remote login restrictions for privileged users

Requirement:

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

[Reference TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.6]

2.1.6 Authorization Policy

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.6.1]

2.1.7 Unambiguous identification of the user & group accounts removal

Requirement:

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Sections 4.2.3.4.1.2]

Section 2: Authentication Attribute Management

2.2.1 Authentication Policy

Requirement:
The usage of a system function without successful authentication on basis of the user identity and at least two authentication attribute (e.g. password, certificate) shall be prevented. For machine accounts and local access one authentication attribute will be sufficient. System functions comprise, for example network services (like SSH, SFTP, Web services), local

access via a management console, local usage of operating system and applications. This requirement shall also be applied to accounts that are only used for communication between systems

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

2.2.2 Authentication Support – External

Requirement:
If the SCP supports external authentication mechanism such as AAA server (for authentication, authorisation and accounting services) , then the communication between SCP and the external authentication entity shall be protected using the authentication and related service protocols built strictly using the Secure cryptographic controls prescribed in Table1 of the latest document " Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

2.2.3 Protection against brute force and dictionary attacks

Requirement:
A protection against brute force and dictionary attacks that hinder authentication attribute guessing shall be implemented in SCP.
Brute force and dictionary attacks aim to use automated guessing to ascertain authentication attribute for user and machine accounts.
Various measures or a combination of the following measures can be taken to prevent this:
(i) Using the timer delay (this delay could be the same or increased depending the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").
(ii) Blocking an account following a specified number of incorrect attempts. However, it has to be taken into account that this solution needs a process for unlocking and an attacker can force this to deactivate accounts and make them unusable.
(iii) Using an authentication attribute blacklist to prevent vulnerable passwords.
(iv) Using CAPTCHA to prevent automated attempts (often used for Web applications).
In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by SCP. An exception to this requirement is machine accounts.

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

2.2.4 Enforce Strong Password

Requirement:
(a) The configuration setting shall be such that a SCP 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 SCP). It shall not be possible setting this absolute minimum length to a lower value by configuration.
(ii) Password shall mandatorily comprise all the following four categories of characters:
- at least 1 uppercase character (A-Z)
- at least 1 lowercase character (a-z)
- at least 1 digit (0-9)
- at least 1 special character (e.g. @;!$.)

b) The minimum length of characters in the passwords and the set of allowable special characters shall be configurable by the operator. The special characters may be categorized in sets according to their Unicode category.
c) If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this sub-clause.
d) If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the SCP.
e) When a user is changing a password or entering a new password, SCP /central system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.).
Password shall not be stored in clear text in the system; passwords shall be salted and hashed.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section 4.2.3.4.3]

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.
SCP shall monitor inactive sessions of administrative login users and initiate session locking mechanism based on user configurable timers. Unlocking the session shall be permissible only by authentication. If the inactivity period further continues for a defined period, Session /user ID time out must occur after this inactivity.

The timer values can be admin configurable as per requirement, normally set between 2 to 5 minutes.
[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.5.2]

2.2.6 Password Changes

Requirement:
If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time. When an external centralized system for user authentication is used it should be possible to implement this function on this system.
Password change shall be enforced after initial login.
SCP shall enforce password change based on password management policy.
In particular, the system shall enforce password expiry. SCP shall support a configurable period for expiry of passwords.
Previously used passwords shall not be allowed upto a certain number (Password History).

The number of disallowed previously used passwords shall be:
• Configurable;
• Greater than 0;
• And its minimum value shall be 3. This means that the UDM shall store at least the three previously set passwords. The maximum number of passwords that the UDM 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.

SCP to have in-built mechanism to support this requirement.

If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password change policies as laid down for the local system in this subclause.
And if a central system is not used for user authentication, the assurance on password changes rules shall be performed on the SCP.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.2]

2.2.7 Protected Authentication feedback

Requirement:

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

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

2.2.8 Removal of predefined or default authentication attributes

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.2.3]

2.2.9 Logout function

Requirement:

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

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

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

2.2.10 Policy regarding consecutive failed login attempts

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

[Reference TSDSI STD T1.3GPP 33.117- 16.7.0 V.1.0.0. Section 4.2.3.4.5]

Section 3: Software Security

2.3.1 Secure Update

Requirement:
For software updates, SCP shall support software package integrity validation via cryptographic means, e.g. digital signature, code signing certificate (valid and not time expired) and using Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” only.
To this end, the SCP has a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software update is originated from only these sources.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.5]

2.3.2 Secure Upgrade

Requirement:

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

(ii) SCP shall support software package integrity validation via cryptographic means, e.g., digital signature, code signing certificate (valid and not time expired), and using Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only. To this end, the SCP has a list of public keys or certificates of authorized software sources and uses the keys to verify that the software update originated from only these sources.

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

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.5]

2.3.3 Source code security assurance

Requirement:
a) OEM shall follow best security practices including secure coding for software development. Source code shall be made available either at TSTL premises or at the mutually agreed location for source code review by the designated TSTL. It may be supported by furnishing the Software Test Document (STD).
b) Also, OEM shall submit the undertaking as below:
(i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the SCP Software which includes OEM developed code, third party software and opensource code libraries used/embedded in the SCP.
(ii)SCP software shall be free from CWE top 25 and OWASP top10 security weaknesses on the date of offer of product to designated TTSL for testing. For other security weaknesses, OEM shall give mitigation plan.
(iii) The binaries for SCP and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

2.3.4 Known Malware and backdoor Check

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

[Reference: TSDSI STD T1.3GPP 33.117 -16.7.0 V.1.0.0. Section 4.3.2.3]

2.3.6 Unnecessary Services Removal

Requirement:
SCP shall only run protocol handlers and services which are needed for its operation and which do not have any known security vulnerabilities. By default, all other ports and services will be permanently disabled. SCP Shall not support following services

- FTP
- TFTP
- Telnet
- rlogin, RCP, RSH
- HTTP
- SNMPv1 and v2
- SSHv1
- TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- BOOTP server

- Discovery protocols (CDP, LLDP)
- IP Identification Service (Identd)
- PAD
- MOP

Any other protocols, services that are vulnerable are also to be permanently disabled.
Full documentation of required protocols and services (communication matrix) of the SCP and their purpose needs to be provided by the OEM as prerequisite for the test case.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.1]

2.3.7 Restricting System Boot Source

Requirement:

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

[Reference– TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section- 4.2.3.3.2]

2.3.8 Secure Time Synchronization

Requirement:
SCP shall use reliable time and date information provided through NTP/PTP server. SCP shall establish secure communication channel with the NTP/PTP server.
SCP shall establish secure communication channel strictly using Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" with NTP/PTP server.
SCP shall generate audit logs for all changes to time settings.

2.3.9 Restricted reachability of services

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

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

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

2.3.10 Self Testing

Requirement:
SCP shall perform self-tests (integrity of the firmware and software as well as correct operation of cryptographic Module as per security requirement area of "self-test" of FIPS-140-2 or Later version etc.,) to identify failures in its security Mechanisms during i) power on ii) when Administrator Instructs iii) Periodic, with period configurable and iv) at the time of restart.

Section 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 SCP shall be deactivated in the SCP's software and/or hardware.
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 SCP.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.4]

2.4.2 No unsupported components

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

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

2.4.3 Avoidance of Unspecified mode of Access

Requirement:

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

An undertaking shall be given by the OEM as follows:

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

Section 5: User Audit

2.5.1 Audit trail storage and protection

Requirement:
The security event log shall be access controlled (file access rights) such that only privilege users including the administrator have access to read the log files. The only allowed operations on security event log are archiving/saving and viewing.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.3]

2.5.2 Audit Event Generation

Requirement:
The SCP shall log all important Security events with unique System Reference details as given in the Table below.
SCP shall record within each audit record at least information pertaining to Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

Additional audit record information, depending on the audit event, shall also be provided as given in the Table below:

Event Types (Mandatory or optional)	**Description**	**Event data to be logged**
Incorrect login attempts (Mandatory)	Records any user incorrect login attempts to the SCP.	Username
		Source (IP address) if remote access

		Outcome of event (Success or failure)
		Timestamp
Administrator access (Mandatory)	Records any access attempts to accounts that have system privileges.	Username,
		Timestamp,
		Length of session
		Outcome of event (Success or failure)
		Source (IP address) if remote access
Account administration Mandatory)	Records all account administration activity, i.e. configure, delete, copy, enable, and disable.	Administrator username,
		Administered account,
		Activity performed (configure, delete, enable and disable)
		Outcome of event (Success or failure)
		Timestamp
Resource Usage (Mandatory)	Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period have exceeded their defined thresholds.	Value exceeded,
		Value reached
		(Here suitable threshold values shall be defined depending on the individual system.)
		Outcome of event (Threshold Exceeded)
		Timestamp
Configuration change (Mandatory)	Changes to configuration of the network device	Change made
		Timestamp
		Outcome of event (Success or failure)
		Username
Reboot/shutdown/crash (Mandatory)	This event records any action on the network device/SCP that forces a reboot or shutdown OR where the network device/SCP has crashed.	Action performed (boot, reboot, shutdown, etc.)
		Username (for intentional actions)
		Outcome of event (Success or failure)
		Timestamp

Interface status change (Mandatory)	Change to the status of interfaces on the network device/SCP (e.g. shutdown)	Interface name and type
		Status (shutdown, down missing link, etc.)
		Outcome of event (Success or failure)
		Timestamp
Change of group membership or accounts (Optional)	Any change of group membership for accounts	Administrator username,
		Administered account,
		Activity performed (group added or removed)
		Outcome of event (Success or failure)
		Timestamp.
Resetting Passwords (Optional)	Resetting of user account passwords by the Administrator	Administrator username
		Administered account
		Activity performed (configure, delete, enable and disable)
		Outcome of event (Success or failure)
		Timestamp
Services (Optional)	Starting and Stopping of Services (if applicable)	Service identity
		Activity performed (start, stop, etc.)
		Timestamp
		Outcome of event (Success or failure)
X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
		Reason for failure
		Subject identity
		Type of event
Secure Update (Optional)	Attempt to initiate manual update, initiation of update, completion of update	User identity
		Timestamp
		Outcome of event (Success or failure)
		Activity performed
Time change (Mandatory)	Change in time settings	Old value of time
		New value of time

		Timestamp
		origin of attempt to change time (e.g.IP address)
		Subject identity
		Outcome of event (Success or failure)
		User identity
Session unlocking/ termination (Optional)	Any attempts at unlocking of an interactive session, termination of a remote session by the session locking mechanism, termination of an interactive session.	User identity (wherever applicable)
		Timestamp
		Outcome of event (Success or failure)
		Subject identity
		Activity performed
		Type of event
Trusted Communication paths with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorised remote administrators (Optional)	Initiation, Termination and Failure of trusted Communication paths	Timestamp
		Initiator identity (as applicable)
		Target identity (as applicable)
		User identity (in case of Remote administrator access)
		Type of event
		Outcome of event (Success or failure, as applicable)
Audit data changes (Optional)	Changes to audit data including deletion of audit data	Timestamp
		Type of event (audit data deletion, audit data modification)
		Outcome of event (Success or failure)
		Subject identity
		User identity
		origin of attempt to change time (e.g.IP address)
		Details of data deleted or modified

User Login (Mandatory)	All use of Identification and authentication mechanisms.	User identity
		Origin of attempt (IP address)
		Outcome of event (Success or failure)
		Timestamp

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.1]

2.5.3 Secure Log Export

Requirement:
(I) (a) The SCP shall support forwarding of security event logging data to an external system by push or pull mechanism.

(b) Log functions should support secure uploading of log files to a central location or to a system external for the SCP.
(II) SCP shall be able to store the generated audit data itself may be with limitations.
(III)SCP shall alert administrator when its security log buffer reaches configured threshold limit.
(IV) In the absence of external system (due to loss of connectivity or due to node failure or due to any other reasons), SCP shall have mechanism to store audit data locally. SCP shall have sufficient memory (minimum 100 MB) allocated for this purpose. OEM shall submit justification document for sufficiency of local storage requirement.
(V) Secure Log export shall comply the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.2]

2.5.4 Logging access to personal data

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.5]

Section 6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirements:

SCP shall Communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

OEM shall submit to TSTL, the list of the connected entities with SCP and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration, detailed procedure of establishing the communication with each entity and any other details required for verifying this requirement.

2.6.2 Cryptographic Module Security Assurance

Requirement:

Cryptographic module embedded inside the SCP (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 SCP (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".

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

2.6.3. Cryptographic Algorithms implementation Security Assurance

Requirement:
Cryptographic algorithm implemented inside the Crypto module of SCP shall be in compliance with the respective FIPS standards (for the specific crypto algorithm).

Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format along with self-certified test reports.

An undertaking is to be submitted by the OEM mentioning that "Cryptographic algorithm implemented inside the Crypto module of SCP is in compliance with the respective FIPS standards (for the specific crypto algorithm embedded inside the SCP)"
OEM shall submit cryptographic algorithm implementation testing document and the detailed self / Lab test report along with test results for scrutiny.

2.6.4. Protecting data and information – Confidential System Internal Data

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.2.]

2.6.5. Protecting data and information in storage

Requirement:
a) For sensitive data (persistent or temporary) in storage, read access rights shall be restricted. Sensitive files of SCP system that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" with appropriate non-repudiation controls.

b)In addition, the following rules apply for:

(i)Systems that need access to identification and authentication data in the clear/readable form e.g. in order to perform an activity/operation. Such systems shall not store this data in the clear/readable form, but scramble or encrypt it by implementation-specific means.
(ii)Systems that do not need access to sensitive data in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.
(iii)Stored files in the SCP: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section 4.2.3.2.3]

2.6.6 Protection against Copy of Data

Requirement:

a) Without authentication, SCP 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 SCP to create copy of data for illegal transmission.

c) The software functions, components in the SCP for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement**:**

a) SCP shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.

b) Establishment of outbound overt channels such as, HTTPS, IM, P2P, Email etc. are to be forbidden if they are auto-initiated by / auto-originated from the SCP.

Session logs shall be generated for establishment of any session initiated by either user or SCP.

---

2. 6.8 Protection against Data Exfiltration - Covert Channel

Requirement:

a) SCP shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.

b) Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc. are to be forbidden if they are auto-initiated by / auto-originated from the SCP.

c) Session logs shall be generated for establishment of any session initiated by either user or SCP system.

Section 7: Network Services

2.7.1: Traffic Filtering – Network Level Requirement:

SCP shall provide a mechanism to filter incoming IP packets on any IP interface.

In particular the SCP shall provide a mechanism:

(i) To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of the stack ISO/OSI.

(ii) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:

-Discard/Drop: the matching message is discarded, no subsequent rules are applied and no answer is sent back.

-Accept: the matching message is accepted.

-Account: the matching message is accounted for i.e. a counter for the rule is incremented. This action can be combined with the previous ones.

This feature is useful to monitor traffic before its blocking.

(iii) To enable/disable for each rule the logging for Dropped packets, i.e. details on messages matching the rule for troubleshooting.

(iv) To filter on the basis of the value(s) of source IP, destination IP and port addresses of protocol header.

(v) To reset the accounting.

(vi) The SCP shall provide a mechanism to disable/enable each defined rule.

[Reference– TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section 4.2.6.2.1]

2.7.2 Traffic Separation

Requirement:

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

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

2.7.3: Traffic Protection –Anti-Spoofing:

Requirement:

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.3.1.1]

2.7.4 GTP-C Filtering (when 5GC is interworking with EPC)

Requirement:
The following capability is conditionally required:
- For each message of a GTP-C-based protocol, it shall be possible to check whether the sender of this message is authorized to send a message pertaining to this protocol.
- At least the following actions should be supported when the check is satisfied:
- Discard: the matching message is discarded.
- Accept: the matching message is accepted.
- Account: the matching message is accounted for, i.e., a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.
This requirement is conditional in the following sense: It is required that at least one of the following two statements holds:
- SCP supports the capability described above, and this is stated in the product documentation.
- The SCP's documentation states that the capability is not supported and that the SCP needs to be deployed together with a separate entity that provides the capability described above.

[Reference– TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.6.2.3]

2.7.5 GTP-U Filtering

Requirement:
The following capability is conditionally required:
- For each message of a GTP-U-based protocol, it shall be possible to check whether the sender of this message is authorized to send a message pertaining to this protocol.
- At least the following actions should be supported when the check is satisfied:
- Discard: the matching message is discarded.
- Accept: the matching message is accepted.
- Account: the matching message is accounted for, i.e., a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.
This requirement is conditional in the following sense: It is required that at least one of the following two statements holds:
- SCP supports the capability described above, and this is stated in the product documentation.

- The SCP's product documentation states that the capability is not supported and that the SCP needs to be deployed together with a separate entity which provides the capability described above.

[Reference– TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.6.2.4]

Section 8: Attack Prevention Mechanisms

2.8.1 Network Level and application-level DDoS

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

- Restricting of available RAM per application
- Restricting of maximum sessions for a Web application
- Defining the maximum size of a dataset
- Restricting CPU resources per process
- Prioritizing processes
- Limiting of amount or size of transactions of an user or from an IP address in a specific time range
- Limiting of amount or size of transactions to an IP address/Port Address in a specific time range

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.1]

2.8.2 Excessive Overload Protection

Requirement:
SCP shall act in a predictable way if an overload situation cannot be prevented. SCP shall be built in this way that it can react on an overload situation in a controlled way.
However, it is possible that a situation happens where the security measures are no longer sufficient. In such case it shall be ensured that SCP cannot reach an undefined and thus potentially insecure, state.

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

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

2.8.3 Manipulated packets that are sent to an address of the network device shall not lead to an impairment of availability.

Requirement:
SCP shall not be affected in its availability or robustness by incoming packets from other network elements that are manipulated or differing the norm. This means that appropriate packets shall be detected as invalid and be discarded. The process shall not be affecting the performance of the SCP. This robustness shall be just as effective for a great mass of invalid packets as for individual or a small number of packets.

Examples of such packets are:

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

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

Section 9: Vulnerability Testing Requirements

2.9.1 Fuzzing – Network and Application Level

Requirement:

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 section 4.4.4]

2.9.2 Port Scanning

Requirement:

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

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

2.9.3 Vulnerability Scanning

Requirement:

It shall be ensured that no known critical/high/medium (as per CVE-IDs of NIST-NVD) vulnerabilities (as on date of offer of SCP to the designated TTSL for testing) shall exist in the SCP. For low/uncategorized (as per CVE-IDs of NIST-NVD) category vulnerabilities remediation plan is to be provided.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 section 4.4.3]

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.1.1]

2.10.2 Handling of ICMP

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

SCP shall not send certain ICMP types by default but it may support the option to enable utilization of these types which are marked as "Optional" in below table:

Type (IPv4)	Type (IPv6)	Description	Send	Respond to
0	128	Echo Reply	Optional (i.e. as automatic reply to "Echo Request")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	129	Echo Request	Permitted	Optional
11	3	Time Exceeded	Optional	N/A
12	4	Parameter Problem	Permitted	N/A
N/A	2	Packet too Big	Permitted	N/A
N/A	135	Neighbor Solicitation	Permitted	Permitted
N/A	136	Neighbor Advertisement	Permitted	N/A

SCP 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	Not Permitted	N/A	N/A

		Reply	(i.e. as automatic reply to "Timestamp")		
N/A	133	Router Solicitation	N/A	Not Permitted	Not Permitted
N/A	134	Router Advertisement	N/A	N/A	Not Permitted

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.1.2.]

2.10.3 Authenticated Privilege Escalation only

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.1.2.1]

2.10.4 System account identification

Requirement:
Each system account in SCP shall have a unique identification with appropriate non-repudiation controls

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.2.2]

2.10.5 OS Hardening - Minimized kernel network functions

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

1. IP Packet Forwarding between different interfaces of the network product.
2. Proxy ARP

3. Directed broadcast
4. IPv4 Multicast handling
5. Gratuitous ARP messages

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

2.10.6 No automatic launch of removable media

Requirement:
SCP shall not automatically launch any application when a removable media device is connected.
[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.3]

2.10.7 Protection from buffer overflows

Requirement:

SCP 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.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section - 4.3.3.1.5]

2.10.8 External file system mount restrictions

Requirement:
If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in SCP 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.

[Reference– TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 Section - 4.3.3.1.6]

2.10.9 File-system Authorization privileges

Requirement:
SCP shall be designed to ensure that only users that are authorized to modify files, data,

directories or file systems have the necessary privileges to do so.

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

2.10.10 Syn Flood Prevention

Requirement:
SCP shall support a mechanism to prevent Syn Flood attacks. This feature shall be enabled by default.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.4]

2.10.11 Handling of IP options and extensions

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.2.4.1.1.3]

2.10.12 Restrictions on running Scripts / Batch-processes

Requirement:
Scheduled tasks for carrying out the activities such as taking the backups, monitoring disk space and system maintenance activities shall be executed by the privileged user such as administrator only. Similarly, SCP 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:
SCP 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 11: Web Servers

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

2.11.1 HTTPS

Requirement:
The communication between Web client and Web server shall be protected strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.1]

2.11.2 Webserver logging

Requirement:
Access to the SCP webserver (for both successful as well as failed attempts) shall be logged by SCP.
The web server log shall contain the following information:

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.2]

2.11.3 HTTPS input validation

Requirement:
The SCP shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.

SCP shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.4]

2.11.4 No system privileges

Requirement:
No SCP web server processes shall run with system privileges.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.2]

2.11.5 No unused HTTPS methods

Requirement:
HTTPS methods that are not required for SCP operation shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 section 4.3.4.3]

2.11.6 No unused add-ons

Requirement:
All optional add-ons and components of the web server shall be deactivated if they are not required for SCP operation.

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.4]

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

Requirement:
If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory or other corresponding scripting directory shall not include compilers or interpreters.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.5]

2.11.8 No CGI or other scripting for uploads

Requirement:
If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.6]

2.11.9 No execution of system commands with SSI

Requirement:
If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.
[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.7]

2.11.10 Access rights for web server configuration

Requirement:
Access rights for SCP web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 section 4.3.4.8]

2.11.11 No default content

Requirement:

Default content that is provided with the standard installation of the SCP web server shall be removed.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.9]

2.11.12 No directory listings

Requirement:
Directory listings (indexing) / "Directory browsing" shall be deactivated.
[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.10]

2.11.13 Web server information in HTTPS headers

Requirement:
The HTTPS header shall not include information on the version of the SCP web server and the modules/add-ons used.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.11]

2.11.14 Web server information in error pages

Requirement:
User-defined error pages and Error messages shall not include version information and other internal information about the SCP web server and the modules/add-ons used.
Default error pages of the SCP web server shall be replaced by error pages defined by the OEM.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.12]

2.11.15 Minimized file type mappings

Requirement:
File type or script-mappings that are not required for SCP operation shall be deleted.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.13]

2.11.16 Restricted file access

Requirement:

Restrictive access rights shall be assigned to all files which are directly or indirectly reside in the SCP web server's document directory.
In particular, the SCP web server shall not be able to access files which are not meant to be delivered.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0 section 4.3.4.14]

2.11.17 Execute rights exclusive for CGI/Scripting directory

Requirement:

If CGI or other scripting technology is used, only the CGI/Scripting directory is configured with execute rights. Other directories used or meant for web content do not have execute rights.
[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.15]

2.11.18 HTTP User session

Requirement:
To protect user sessions, SCP shall support the following session ID and session cookie requirements:
1. The session ID shall uniquely identify the user and distinguish the session from all other active sessions.
2.The session ID shall be unpredictable.
3.The session ID shall not contain sensitive information in clear text (e.g., account number, social security, etc.).
4.In addition to the Session Idle Timeout, SCP shall automatically terminate sessions after a configurable maximum lifetime. This maximum lifetime defines the maximum session span. When the maximum lifetime expires, the session shall be closed, the session ID shall be deleted and the user shall be forced to (re)authenticate in the web application and to establish a new session. The default value for this maximum lifetime shall be set to 8 hours.

5.Session IDs shall be regenerated for each new session (e.g., each time a user logs in).
6.The session ID shall not be reused or renewed in subsequent sessions.
7.The SCP shall not use persistent cookies to manage sessions but only session cookies. This means that neither the "expire" nor the "max-age" attribute shall be set in the cookies.
8.Where session cookies are used the attribute 'HttpOnly' shall be set to true.
9.Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.
10.Where session cookies are used the 'path' attribute shall be set to ensure that the cookie can only be sent to the specified directory or sub-directory.
11.The SCP shall not accept session identifiers from GET/POST variables.
12.The SCP shall be configured to only accept server generated session ID.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.3]

Section 12: General SBA/SBI Aspects

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

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

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0Section - 4.3.6.2]

2.12.2 Validation of the unique key values in IEs

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

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0Section - 4.3.6.3]

2.12.3 Validation of the IEs limits

Requirement:
The valid format and range of values for each IE, when applicable, shall be defined unambiguously:
- For each message the number of leaf IEs shall not exceed 16000.
- The maximum size of the JSON body of any HTTP request shall not exceed 2 million bytes.
- The maximum nesting depth of leaves shall not exceed 32.

[Reference: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0Section - 4.3.6.4]

2.12.4 Protection at the transport layer

Requirement:
NF Service Request and Response procedure shall support mutual authentication between NF consumer and NF producer.
All network functions shall support TLS. Network functions shall support both server-side and client-side certificates.
Authentication between network functions within one PLMN can use the following method:
- If the PLMN uses protection at the transport layer, authentication provided by the transport layer protection solution shall be used for authentication between NFs.

[Reference TSDSI STD T1.3GPP 33.117- 16.7.0 V.1.0.0. Section 4.2.2.2.2]

2.12.5 Authorization token verification failure handling within one PLMN

Requirement:
The NF Service producer shall verify the access token as follows:
- The NF Service producer ensures the integrity of the access token by verifying the signature using NRF's public key or checking the MAC value using the shared secret. If integrity check is successful, the NF Service producer shall verify the claims in the access token as follows: - It checks that the audience claim in the access token matches its own identity or the type of NF service producer. If a list of NSSAIs or list of NSI IDs is present, the NF service producer shall check that it serves the corresponding slice(s).
- If an NF Set ID is present, the NF Service Producer shall check the NF Set ID in the claim matches its own NF Set ID.
- If the access token contains "additional scope" information (i.e. allowed resources and allowed actions (service operations) on the resources), it checks that the additional scope matches the requested service operation.
- If scope is present, it checks that the scope matches the requested service operation.

- It checks that the access token has not expired by verifying the expiration time in the access token against the current data/time.

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

[Reference TSDSI STD T1.3GPP 33.117- 16.7.0 V.1.0.0. Section 4.2.2.2.3.1]

2.12.6 Authorization token verification failure handling in different PLMNs

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

[Reference TSDSI STD T1.3GPP 33.117- 16.7.0 V.1.0.0. Section 4.2.2.2.3.2]

2.12.7 Correct handling of client credentials assertion validation failure

Requirement:

The verification of the Client credentials assertion shall be performed by the receiving node, i.e., NRF or NF Service Producer in the following way:
- It validates the signature of the JWS as described in RFC 7515.
- If validates the timestamp (iat) and/or the expiration time (exp) as specified in RFC 7519. If the receiving node is the NRF, the NRF validates the timestamp (iat) and the expiration time (exp). If the receiving node is the NF Service Producer, the NF service Producer validates the expiration time, and it may validate the timestamp.
- It checks that the audience claim in the client credentials assertion matches its own type. It verifies that the NF instance ID in the client credentials assertion matches the NF instance ID in the public key certificate used for signing the assertion.

[Reference TSDSI STD T1.3GPP 33.117- 16.7.0 V.1.0.0. Section 4.2.2.2.4.1]

2.13.1 Remote Diagnostic Procedure – Verification

Requirement:

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

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

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

2.13.2 No System Password Recovery

Requirement:

No provision shall exist for SCP System / Root password recovery.

2.13.3 Secure System Software Revocation

Requirement:

Once the SCP software image is legally updated/upgraded with New Software Image, it should not be possible to roll back to a previous software image.

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

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

2.13.4 Software Integrity Check –Installation

Requirement:

SCP shall validate the software package integrity before the installation/upgrade stage strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

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

2.13.5 Software Integrity Check – Boot

Requirement:

The SCP shall verify the integrity of a software component by comparing the result of a measurement of the component, typically a standard cryptographic hash generated strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" to the expected reference value.

2.13. 6 Unused Physical and Logical Interfaces Disabling

Requirement:

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

2.13.7 No Default Profile

Requirement:

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

Chapter 3 Specific Security Requirements

3.1 The SCP has interfaces with Network Functions (NF) and peer SCPs within the PLMN. The interface between the SCP and the NFs and between the two SCPs shall fulfil the following requirements:

3.1.1 Mutual authentication shall be performed between the SCP and NFs, and between the two SCPs within the PLMN.

3.1.2 All communication between the SCP and NFs and between SCPs shall be confidentiality, integrity and replay protected.

If SCP endpoints are co-located with the NFs, the above two requirements may be satisfied by colocation.

3.1.3 The SCP shall provide confidentiality, integrity and replay protection for its internal communication over SCP internal network interfaces.

[Reference: 3GPP TS 33.501 V.17.4.2. Section 5.9.2.4]

Annexure-I (Definition)

1. AuSF: AuSF is a network function with which SEAF and UDM interact during the authentication of UE.
2. DDOS: DDoS is a distributed denial-of-service attack that renders the victim un-usable by the external environment.
3. GUTI: The purpose of the GUTI is to provide an unambiguous identification of the UE that does not reveal the UE or the user's permanent identity.
4. Downlink: Unidirectional radio link for the transmission of signals from a RAN access point to a UE. Also, in general the direction from Network to UE.
5. Medium Access Control: A sub-layer of radio interface layer 2 providing unacknowledged data transfer service on logical channels and access to transport channels.
6. Mobility: The ability for the user to communicate whilst moving independent of location.
7. Network Element: A discrete telecommunications entity which can be managed over a specific interface e.g. the RNC
8. NG-RAN: It is the radio access network introduced for accessing 5G.
9. Node B: A logical node responsible for radio transmission / reception in one or more cells to/from the User Equipment. Terminates the Iub interface towards the RNC.
10. Non-Access Stratum: Protocols between UE and the core network that are not terminated in the RAN.
11. Original Equipment Manufacturer (OEM): manufacturer of communication and its related products under whose brand, the products are sold or proposed to be sold to operators in the country.
12. Packet: An information unit identified by a label at layer 3 of the OSI reference model. A network protocol data unit (NPDU).
13. PLMN Area: The PLMN area is the geographical area in which a PLMN provides communication services according to the specifications to mobile users. In the PLMN area, the mobile user can set up calls to a user of a terminating network. The terminating network may be a fixed network, the same PLMN, another PLMN or other types of PLMN. Terminating network users can also set up calls to the PLMN. The PLMN area is allocated to a PLMN. It is determined by the service and network provider in accordance with any provisions laid down under national law. In general the PLMN area is restricted to one country. It can also be determined differently, depending on the different telecommunication services, or type of MS. If there are several PLMNs in one country, their PLMN areas may overlap. In border areas, the PLMN areas of different countries may overlap. Administrations will have to take

precautions to ensure that cross border coverage is minimized in adjacent countries unless otherwise agreed.

14. PLMN Operator: Public Land Mobile Network operator. The entity which offers telecommunications services over an air interface.
15. Protocol data unit: 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.
16. 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.
17. QoS profile: a QoS profile comprises a number of QoS parameters. A QoS profile is associated with each QoS session. The QoS profile defines the performance expectations placed on the bearer network.
18. QoS session: Lifetime of PDP context. The period between the opening and closing of a network connection whose characteristics are defined by a QoS profile. Multiple QoS sessions may exist, each with a different QoS profile.
19. Quality of Service: 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.
20. Radio link: A "radio link" is a logical association between single User Equipment and a single RAN access point. Its physical realization comprises one or more radio bearer transmissions.
21. Radio Resource Control: A sublayer of radio interface Layer 3 existing in the control plane only which provides information transfer service to the non-access stratum. RRC is responsible for controlling the configuration of radio interface Layers 1 and 2.
22. Registered PLMN (RPLMN): This is the PLMN on which the UE has performed a location registration successfully.
23. Registration Area: A (NAS) registration area is an area in which the UE may roam without a need to perform location registration, which is a NAS procedure.
24. Remote Access: The access which is not Local access. This includes access from the EMS (Element Management System) network, and access that originates or passes through the internet.
25. RRC Connection: A point-to-point bi-directional connection between RRC peer entities on the UE and the UTRAN sides, respectively. An UE has either zero or one RRC connection.

26. SEAF is an entity which is subsumed by UPF which communicates with UE and AuSF during device authentication.
27. Security: The ability to prevent fraud as well as the protection of information availability, integrity, and confidentiality.
28. Serving Network: The serving network provides the user with access to the services of the home environment.
29. Software refers to the programs and data components which are usually stored on erasable media (e.g., disk), that can be dynamically written and modified during execution. Two general categories of software are system software and application software.
30. Subscriber: The responsibility for payment of charges incurred by one or more users may be undertaken by another entity designated as a subscriber. This division between use of and payment for services has no impact on standardization
31. Transmission or Transport is the transfer of information from one entity (transmitter) to another (receiver) via a communication path.
32. 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.
33. Uplink: An "uplink" is a unidirectional radio link for the transmission of signals from a UE to a base station.
34. User Equipment: A device allowing a user access to network services. The interface between the UE and the network is the radio interface. A User Equipment can be subdivided into a number of domains, the domains being separated by reference points.

Annexure-II(Acronyms)

5GC	-	5G Core Network
5GMM	-	5GS Mobility Management
5GS	-	5G System
5GSM	-	5G Session Management
AAA	-	Authentication, Authorization and Accounting
AF	-	Application Function
AKA	-	Authentication and Key Agreement
AKA’	-	AKA Prime
AKMA	-	Authentication and key management for applications
ARP	-	Address Resolution Protocol/Allocation and Retention Priority
ARPF	-	Authentication Credential Repository and Processing Function
AS	-	Access Stratum
ATSSS	-	Access Traffic Steering, Switching, Splitting
AuSF	-	Authentication Server Function
AUTS	-	Authentication failure message with synchronization failure
BSF	-	Binding Support Function
CAPIF	-	Common API Framework for 3GPP northbound APIs
CHF	-	Charging Function
CIoT	-	Cellular Internet of things
CLI	-	Command Line Interface
CM	-	Connection Management
CP	-	Control Plane
DCCF	-	Data Collection Coordination Function
DDoS	-	Distributed Denial of Service
DL	-	Downlink
DN	-	Data Network
DNN	-	Data Network Name
DS-TT	-	Device Side TSN Translator
DTLS	-	Datagram Transport Layer Security
EAP	-	Extensible Authentication Protocol
EASDF	-	Edge Application Server Discovery Function
ECS	-	EDNS Client Subnet
EDNS	-	Extension Mechanism for DNS
EMM	-	EPS Mobility Management
EPC	-	Evolved Packet Core
EPS	-	Evolved Packet System
F-TEID	-	Fully Qualified Tunnel Endpoint Identifier

FQDN	-	Fully Qualified Domain Name
GMLC	-	Gateway Mobile Location Centre
gNB	-	5G Next Generation base station
gPTP	-	Generalized Precision Time Protocol
GTP-C	-	GPRS Tunneling Protocol Control Plane
GTP-U	-	GPRS Tunneling Protocol User Plane
GUI	-	Graphical User Interface
GUTI	-	Globally Unique Temporary Identifier
HE	-	Home Environment
HTTP	-	Hypertext Transfer Protocol
HTTPS	-	Hypertext Transfer Protocol Secure
ICMP	-	Internet Control Message Protocol
IKE	-	Internet Key Exchange
IMS	-	IP Multimedia Subsystem
IMPI	-	IMS Private Identity
IMPU	-	IMS Public Identity
IPUPS	-	Inter-PLMN User Plane Security
IE	-	Information Element
IP	-	Internet Protocol
IPX	-	IP exchange
ISO-OSI	-	International organization of Standardization – Open System Interconnection
JSON	-	JavaScript Object Notation
JWS	-	JSON Web Signature
JWT	-	JSON Web Token
LBO	-	Local Breakout
LMF	-	Location Management Function
L-NEF	-	Local NEF
MA PDU	-	Multiple Access PDU
MFAF	-	Messaging Framework Adaptor Function
ML	-	Machine Learning
MOBIKE	-	IKEv2 Mobility and Multihoming Extension
N3IWF	-	Non-3GPP Interworking Function
NAS	-	Non-Access Stratum
NDS	-	Network Domain Security
NEF	-	Network Exposure Function
NF	-	Network Function
NG	-	Next Generation
ng-eNB	-	Next Generation e-NodeB
NG-RAN	-	Next Generation Radio Access Network

NIDD	-	Non-IP Data Delivery
NRF	-	Network Repository Function
NSAC	-	Network Slice Admission Control
NWDAF	-	Network Data Analytics Function
NW-TT	-	Network -side TSN Translator
O&M	-	Operations and Maintenance
OAM	-	Operations, Administration, Maintenance
OS	-	Operating System
PCF	-	Policy Control Function
PDR	-	Packet Detection Rule
PDU	-	Protocol Data Unit
PFCP	-	Packet Forwarding Control Protocol
PFD	-	Packet Flow Descriptor
PLMN	-	Public Land Mobile Network
PRINS	-	Protocol for N32 Interconnect Security
PSA	-	PDU Session Anchor
QoS	-	Quality of Service
RAM	-	Random Access Memory
RAN	-	Radio Access Network
RAT	-	Radio Access Technology
RES	-	Response
REST	-	Representational State Transfer
RFC	-	Request For Comments
RM	-	Registration Management
RRC	-	Radio Resource Control
S-NSSAI	-	Single - Network Slice Selection Assistance Information
SBI	-	Service Based Interfaces
SCP	-	Service Communication Proxy
SCEF	-	Service Capability Exposure Function
SDF	-	Service Data Flow
SEAF	-	Security Anchor Function
SEPP	-	Security Edge Protection Proxy
SIDF	-	Subscription Identifier De-concealing Function
SMF	-	Session Management Function
SNPN	-	Stand Alone Non-Public Network
SSC	-	Session and Service Continuity
SUCI	-	Subscription Concealed Identifier
SUPI	-	Subscription Permanent Identifier
TA	-	Tracking Area
TNGF	-	Trusted Non-3GPP Gateway Function

TSC	-	Time Sensitive Communication
TSN	-	Time Sensitive Networking
TSTL	-	Telecom Security Testing Laboratory
TT function	-	TSN Translator Function
UDM	-	Unified Data Management
UDR	-	Unified Data Repository
UE	-	User Equipment
UL	-	Uplink
UPF	-	User Plane Function
URI	-	Uniform Resource Identifier
URL	-	Uniform Resource Locator
URLLC	-	Ultra Reliable Low Latency Communication
VN	-	Virtual Network
WLAN	-	Wireless Local Area Network

Annexure-III (List of Submissions)

1. Source Code Security Assurance (against test case 2.3.3)
2. Known Malware and backdoor Check (against test case 2.3.4)
3. No unused Software (against test case 2.3.5)
4. Communication matrix (against test case 2.3.6)
5. No Unused Functions (against test case 2.4.1)
6. Avoidance of Unspecified Wireless Access (against test case 2.4.3)
7. Cryptographic Based Secure Communication (against test case 2.6.1)
8. Cryptographic Module Security Assurance (against test case2.6.2)
9. Cryptographic Algorithms implementation Security Assurance (against test case 2.6.3)

Annexure-IV (References)

1. TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0: "Catalogue of General Security Assurance Requirements".
2. TSDSI STD T1.3GPP 33.522-17.0.0 5G Security Assurance Specification (SCAS), Service Communication Proxy (SCP).
3. TSDSI STD T1.3GPP 33.501-17.4.2 V.1.0.0 Security architecture and procedures for 5G System
4. 3GPP TS 33.501 V.17.4.2.
5. TSDSI STD T1.3GPP 33.210-17.0.0 V.1.0.0; Network Domain Security (NDS); IP network layer security
6. RFC 7540 Hypertext Transfer Protocol Version 2 (HTTP/2)
7. RFC 7515 JSON Web Signature (JWS)
8. RFC 7519 JSON Web Token (JWT)
9. RFC 6749 The OAuth 2.0 Authorization Framework

-End of Document-