सत्यमेव जयते

# Indian Telecom Security Assurance Requirements

## for

## 4G - Serving Gateway (S-GW)

**NCCS / ITSAR / CORE /4G-S-GW**

**DRAFT FOR APPROVAL**

Securing Networks

Release Date: 25-03-2022 Version: 1.0.0

Date of Enforcement:

**Security Assurance Standards (SAS) Division**
**National Centre for Communication Security (NCCS), Bengaluru**
**Department of Telecommunications**
**Ministry of Communications**
**Government of India**

# Abstract

This document defines the security requirements of Serving Gateway abbreviated as S-GW, which is an important logical functional entity in the Long Term Evolution (LTE). The S-GW. The main function of S-GW is routing and forwarding of user packets in both directions ie.,from eNB to PGW and PGW to eNB. For every UE accessing the network a S-GW is assigned, S-GW receives instructions from MME to set-up or tear down sessions for a particular UE.

The objective of this document is to present a comprehensive, country specific security requirements for the S-GW.

# Table of Contents


Scope ..... 7

Common Security Requirements ..... 7

Section 1: Access and Authorization ..... 7

1.1 Management Protocols Mutual Authentication ..... 7

1.2 Management Traffic Protection ..... 7

1.3 Role-Based access control ..... 7

1.4 User Authentication – Local and Remote ..... 8

1.5 Remote login restrictions for privileged users ..... 8

1.6 Authorization Policy ..... 9

1.7 Unambiguous identification of the user & group accounts removal ..... 9

Section 2: Authentication Attribute Management ..... 9

2.1 Authentication Policy ..... 10

2.2 Authentication Support – External ..... 10

2.3 Protection against brute force and dictionary attacks ..... 10

2.4 Enforce Strong Password ..... 11

2.5 Inactive Session Timeout ..... 12

2.6 Password Changes ..... 12

2.7 Protected Authentication feedback ..... 13

2.8 Removal of predefined or default authentication attributes ..... 13

Section 3: Software Security ..... 13

3.1 Secure Update ..... 13

3.2 Secure Upgrade ..... 14

3.3 Source code security assurance ..... 14

3.4 Known Malware and backdoor Check ..... 15

3.5 No unused software ..... 15

3.6 Unnecessary Services Removal ..... 15

3.7 Restricting System Boot Source ..... 16

3.8 Secure Time Synchronization ..... 16

3.9 Restricted reachability of services ..... 17
3.10 Self Testing ..... 17
Section 4: System Secure Execution Environment ..... 17
4.1 No unused functions ..... 17
4.2 No unsupported components ..... 17
4.3 Avoidance of Unspecified Mode of Access ..... 18
Section 5: User Audit ..... 18
5.1 Audit trail storage and protection ..... 18
5.2 Audit Event Generation ..... 18
5.3 Secure Log Export ..... 21
Section 6: Data Protection ..... 22
6.1 Cryptographic Based Secure Communication with connecting entities ..... 22
6.2 Cryptographic Module Security Assurance ..... 22
6.3 Cryptographic Algorithms implementation Security Assurance ..... 23
6.4 Protecting data and information – Confidential System Internal Data ..... 23
6.5 Protecting data and information in storage ..... 23
6.6 Protection against Copy of Data ..... 24
6.7 Protection against Data Exfiltration - Overt Channel ..... 24
6.8 Protection against Data Exfiltration - Covert Channel ..... 25
Section 7: Network Services ..... 25
7.1 Traffic Filtering – Network Level ..... 25
7.2 Traffic Separation ..... 26
7.3 Traffic Protection – Anti-Spoofing ..... 26
Section 8: Attack Prevention Mechanisms ..... 26
8.1 Network Level and application-level DDoS ..... 26
8.2 Excessive Overload Protection ..... 27
8.3 Filtering IP Options ..... 27
Section 9: Vulnerability Testing Requirements ..... 27
9.1 Fuzzing – Network and Application Level ..... 27
9.2 Port Scanning ..... 28
9.3 Vulnerability Scanning ..... 28
Section 10: Operating System ..... 28

10.1 Growing Content Handling ..... 28
10.2 Handling of ICMP ..... 28
10.3 Authenticated Privilege Escalation only ..... 29
10.4 System account identification ..... 30
10.5 OS Hardening ..... 30
10.6 No automatic launch of removable media ..... 30
10.7 Protection from buffer overflows ..... 30
10.8 External file system mount restrictions ..... 31
10.9 File-system Authorization privileges ..... 31
10.10 Restrictions on running Scripts / Batch-processes ..... 31
10.11 Restrictions on Soft-Restart ..... 31
Section 11: Web Servers ..... 32
11.1 HTTPS ..... 32
11.2 Webserver logging ..... 32
11.3 HTTPS input validation ..... 32
11.4 No system privileges ..... 33
11.5 No unused HTTPS methods ..... 33
11.6 No unused add-ons ..... 33
11.7 No compiler, interpreter, or shell via CGI or other server-side scripting ..... 33
11.8 No CGI or other scripting for uploads ..... 33
11.9 No execution of system commands with SSI ..... 34
11.10 Access rights for web server configuration ..... 34
11.11 No default content ..... 34
11.12 No directory listings ..... 34
11.13 Web server information in HTTPS headers ..... 34
11.14 Web server information in error pages ..... 35
11.15 Minimized file type mappings ..... 35
11.16 Restricted file access ..... 35
11.17 Execute rights exclusive for CGI/Scripting directory ..... 35
Section 12: Other Security requirements ..... 36
12.1. Remote Diagnostic Procedure – Verification ..... 36
12.2 No System / Root Password Recovery ..... 36

12.3 Secure System Software Revocation ..... 36
12.4 Software Integrity Check – Installation ..... 37
12.5 Software Integrity Check – Boot ..... 37
12.6 Unused Physical and Logical Interfaces Disabling ..... 37
12.7 No Default Profile ..... 37
12.8 Security Algorithm Modification ..... 38
Specific Security Requirements ..... 38
Section 13: SNMP Security ..... 38
13.1 Login User Credentials ..... 38
13.2 MIB Whitelisting ..... 38
13.3 Community Naming Convention ..... 39
13.4 Remote Packet Capture Facility ..... 39
13.5 SNMP Query Redirection ..... 39
Section 14: NDS / IP Support ..... 40
14.1 Network Domain Security - Architecture ..... 40
14.2 IPSEC on Interfaces ..... 40
14.3 Cryptographic Algorithms – ESP Security Transforms, IKEv2 Profiles ..... 41
14.4 Initialization Vectors for Crypto Keys ..... 43
14.5 Security Policy Granularity ..... 44
14.6 Protection against VPN Attacks ..... 44
14.7 SA Lifetime – Key Freshness ..... 45
14.8 Security Policy Database (SPD) ..... 45
Section 15: EPS Bearer Security ..... 46
15.1 Inactive EPS Bearers ..... 46
15.2 GTP Protocol Support ..... 46
15.3 Uniqueness of Terminal Identifiers ..... 46
15.4 Randomness of Terminal Identifiers ..... 47
15.5 Protection of GTP-C – Inter Security Domain ..... 47
15.6 Policy Discrimination of GTP-C and GTP-U ..... 47
Section 16: Database Security ..... 48
16.1 Guard against Database Attacks ..... 48
Section 17: Diameter Interfaces ..... 48

17.1 End to End security for Diameter Interface ..... 48
17.2 Configuration of Diameter Peers ..... 48
Section 18: Network Security ..... 49
18.1 VLAN Support ..... 49
18.2 NAT / Tr. GW Restrictions ..... 49
18.3 IPV6 Vulnerabilities ..... 49
18.4 DHCP Security ..... 50
18.5 DNS Security ..... 50
18.6 Protection against Rogue NEs, Insider Attacks ..... 51
18.7 Security of Pooled NEs ..... 51
Section 19: Lawful Interception ..... 51
19.1 LI Interface Support ..... 52
19.2 LI Events ..... 52
19.3 LI Message Exchange Requirement ..... 52
19.4 Unique Correlation Number ..... 54
19.5 Encrypted Data Handling ..... 54
19.6 LI Administration Security ..... 55
19.7 Intercept Related Information (IRI) Security ..... 55
19.8 Communication Content (CC) Security ..... 56
19.9 LI Data at Rest Security ..... 56
Section 20: Additional Security Requirements ..... 57
20.1 No Known vulnerabilities in ASICs, SOC Solutions ..... 57
Annexure- I ..... 57
Annexure- II ..... 61

# Scope

This document contains Indian Telecom Security Assurance Requirements (ITSAR) specific to S-GW (Serving Gateway), an LTE (Long Term Evolution) network core element.

# Common Security Requirements

# Section 1: Access and Authorization

## 1.1 Management Protocols Mutual Authentication

**Requirement:**

The protocols used for the S-GW management and maintenance shall support mutual authentication mechanisms only

Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” shall only be used for S-GW management and maintenance.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.4.1]

## 1.2 Management Traffic Protection

**Requirement:**

S-GW management traffic shall be protected strictly using secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.2.3.2.4]

## 1.3 Role-Based access control

**Requirement:**

S-GW shall support Role Based Access Control (RBAC). A role-based access control system uses a set of controls which determines how users interact with domains and resources. The RBAC system controls how users or groups of users are allowed

access to the various domains and what type of operation they can perform i.e. the specific operation command or command group.

S-GW supports Role Based Access Control (RBAC) with minimum of 3 user roles, in particular, for OAM privilege management, for S-GW Management and Maintenance, including authorization of the operation for configuration data and software.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.6.2]

## 1.4 User Authentication – Local and 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 (single authentication attribute in case of machine account) for protecting the all accounts from misuse.

**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.

**Local access:** The access from Console interface, from local Console network, from LMT (Local Maintenance Terminal interface) or from S-GW local hardware interface.

**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.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.2.1]

## 1.5 Remote login restrictions for privileged users

**Requirement:**

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

This remote root user access restriction is also applicable to application softwares / tools such as TeamViewer, desktop sharing etc which provide remote access to the S-GW.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.6]

## 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.6.1]

## 1.7 Unambiguous identification of the user & group accounts removal

**Requirement:**

Users shall be identified unambiguously by the S-GW.

S-GW shall support assignment of individual accounts per user, where a user could be a person, or, for machine accounts, an application, or a system.

S-GW shall not enable the use of group accounts or group credentials, or sharing of the same account between several users.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Sections 4.2.3.4.1.2]

# Section 2: Authentication Attribute Management

## 2.1 Authentication Policy

**Requirement:**

The usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes in case of user accounts (e.g. password, certificate, token) and single authentication attribute in case of machine account, shall be prevented. 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.1.1]

## 2.2 Authentication Support – External

**Requirement:**

If the S-GW supports external authentication mechanism such as AAA server (for authentication, authorization and accounting services) then the communication between S-GW 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 of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

## 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. 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 S-GW. [Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3.3]

## 2.4 Enforce Strong Password

**Requirement:**

The configuration setting shall be such that an S-GW 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 S-GW). 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. @;!$.)

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.

S-GW shall have in-built mechanism to support this requirement, further if a central system is used for user authentication password policy then additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this subclause.

And if a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the S-GW.

When a user is changing a password or entering a new password, S-GW/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.).

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.2.3.4.3.1]

## 2.5 Inactive Session Timeout

**Requirement:**

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

S-GW 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.5.2]

## 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 is possible to redirect or implement this function on this system.

Password change shall be enforced after initial login.

The system shall enforce password change based on password management policy.

In particular, the system shall enforce password expiry. S-GW shall support a configurable period for expiry of passwords.

Previously used passwords shall not be allowed up to a certain number (password history).

The number of disallowed previously used passwords shall be:

- Configurable;
- Greater than 0;
- And its minimum value shall be 3. This means that the S-GW shall store at least the three previously set passwords. The maximum number of passwords that the S-GW 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.

S-GW 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 S-GW.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3.2]

## 2.7 Protected Authentication feedback

**Requirement:**

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3.4]

## 2.8 Removal of predefined or default authentication attributes

**Requirement:**

Predefined or default authentication attributes shall be deleted or disabled.

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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.2.3]

# Section 3: Software Security

## 3.1 Secure Update

**Requirement:**

For software updates, S-GW shall support software package integrity validation via cryptographic means, e.g. digital signature, code signing certificate (valid and not time expired) and using the secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

To this end, the network product has a list of public keys or certificates of authorised software sources, and uses the keys to verify that the software update is originated from only these sources.

## 3.2 Secure Upgrade

**Requirement:**

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

(ii) (ii) S-GW shall support software package integrity validation via cryptographic means, e.g. digital signature, code signing certificate (valid and not time expired) and using the secure cryptographic controls as prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”. To this end, the S-GW shall have a list of public keys or certificates of authorised software sources, and uses the keys to verify that the software upgrade is originated from only these sources.

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

(iv) (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 point (ii)

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.3.5]

## 3.3 Source code security assurance

**Requirement:**

a) OEM shall follow 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 S-GW software, which includes

OEM developed code, third party software and open source code libraries used/embedded in the S-GW.

(ii)The S-GW software is free from CWE top 25 & OWASP top 10 security weaknesses on the date of offer of S-GW to designated TSTL for testing. For other security weaknesses, OEM shall give mitigation plan.

(iii) The binaries for S-GW and upgrades/updates thereafter generated from the source code are free from CWE top 25 & OWASP top 10 security weaknesses.

## 3.4 Known Malware and backdoor Check

**Requirement:**

OEM shall submit an undertaking stating that S-GW is free from all known malware and backdoors as on the date of offer of S-GW to designated TSTL for testing and shall submit Malware test document (MTD).

## 3.5 No unused software

**Requirement:**

Software components or parts of software which are not needed for operation or functionality of the S-GW shall not be present.

Orphaned software components /packages shall not be present in S-GW.

OEM shall provide the list of software that are necessary for its operation.

OEM shall furnish an undertaking as “S-GW does not contain Software that is not used in the functionality of S-GW”

[Reference: 1) TSDSI STD T1.3GPP 33.117 -14.2.0 V.1.0.0 Section 4.3.2.3]

## 3.6 Unnecessary Services Removal

**Requirement:**

S-GW 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. S-GW Shall not support following services. Any other protocols, services that are vulnerable are also to be permanently disabled.

- 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

Full documentation of required protocols and services (Communication matrix) of the Network product and their purpose needs to be provided by the OEM as prerequisite for the test case.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.1]

## 3.7 Restricting System Boot Source

**Requirement:**

S-GW shall boot only from memory devices intended for this purpose.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.3.2]

## 3.8 Secure Time Synchronization

**Requirement:**

S-GW shall provide reliable time and date information provided by itself or through NTP/PTP server.

S-GW shall provide reliable time and date information provided through NTP/PTP server. S-GW shall establish secure communication channel with the NTP/PTP server.

S-GW shall establish secure communication channel strictly using Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” with NTP/PTP server.

S-GW shall generate audit logs for all changes to time settings.

## 3.9 Restricted reachability of services

**Requirement:**

The S-GW 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.2]

## 3.10 Self Testing

**Requirement:**

S-GW 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.

# Section 4: System Secure Execution Environment

## 4.1 No unused functions

**Requirement:**

Unused functions i.e. the software and/or hardware functions which are not needed for operation or functionality of the S-GW shall not be present in the S-GW’s software and/or hardware.

List of the used functions of the Networks software and hardware as given by the OEM shall match the list of used software and hardware functions that are necessary for the operation of the S-GW.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.4]

## 4.2 No unsupported components

**Requirement:**

OEM to ensure that the S-GW shall not contain software and/or hardware components that are no longer supported by OEM or its third parties including the open-source communities, such as components that have reached end-of-life or end-of-support.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.5]

## 4.3 Avoidance of Unspecified Mode of Access

**Requirement:**

S-GW shall not contain any mode of access (eg:Wireless access) mechanism which is unspecified or not declared.

An undertaking shall be given by the OEM as follows:

“The S-GW does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel”.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.6.1]

# Section 5: User Audit

## 5.1 Audit trail storage and protection

**Requirement:**

The security event log shall be access controlled using file access rights such that only privilege users including the administrator have access to read the log files. The rights to delete or modify the log files are to be restricted, a trail of delete or modify activities may be logged in separate log file.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0. V.1.0.0 section 4.2.3.6.3]

## 5.2 Audit Event Generation

**Requirement:**

The S-GW shall log all important security events with unique System Reference details as given in the Table below.

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

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

| | | |
|---|---|---|
| | | origin of attempt to change time (e.g. IP address) |
| | | Subject identity |
| | | outcome of event (Success or failure) |
| | | user identity |
| Session unlocking/ termination (Optional) | Any attempts at unlocking of an interactive session, Termination of a remote session by the session locking mechanism, Termination of an interactive session | user identity (wherever applicable) |
| | | Timestamp |
| | | Outcome of event (Success or failure) |
| | | Subject identity |
| | | Activity performed |
| | | Type of event |
| Trusted Communication paths (with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorised remote administrators) (Optional) | Initiation, Termination and Failure of trusted Communication paths | Timestamp |
| | | Initiator identity (as applicable) |
| | | Target identity (as applicable) |
| | | User identity (in case of Remote administrator access) |
| | | Type of event |
| | | Outcome of event (Success or failure, as applicable) |
| Audit data changes (Optional) | Changes to audit data including deletion of audit data | Timestamp |
| | | Type of event (audit data deletion, audit data modification) |
| | | Outcome of event (Success or failure, as applicable) |
| | | Subject identity |
| | | user identity |
| | | origin of attempt to change time (e.g. IP address) |
| | | Details of data deleted or modified |
| Port Scan Attempts | Any attempt to scan the network interface shall lead to triggering of logging of the appropriate parameters | Date & Time Stamp |
| | | Source IP Address |
| | | Destination Port Address |

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.6.1;
2) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.5]

## 5.3 Secure Log Export

| Document Name | ITSAR for Serving Gateway (SGW) | | |
|---|---|---|---|
| Doc. No. | Version | Release date | Enforcement date |
| ITSAR-SGW-0001 | 1.0.0 | 25-Mar-2022 | XX-XXX-XXXX |

**Requirement:**

(i) (a) The S-GW shall support forward of security event logging data to an external system by push or pull mechanism.
(b) Log functions should support secure uploading of log files to a central location or to a system external for the S-GW.
(ii) S-GW shall be able to store generated audit data itself, may be with limitations.
(iii) S-GW 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), S-GW shall have mechanism to store audit data locally. S-GW shall have sufficient memory (minimum 100 MB) allocated for this purpose. OEM to 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 of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)".

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.6.2]

# Section 6: Data Protection

## 6.1 Cryptographic Based Secure Communication with connecting entities

**Requirements:**

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

## 6.2 Cryptographic Module Security Assurance

Cryptographic module embedded inside the S-GW (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 S-GW (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 submit cryptographic Module testing document and the detailed self / Lab test report along with test results for scrutiny.

## 6.3 Cryptographic Algorithms implementation Security Assurance

Cryptographic algorithms embedded in the crypto module of S-GW shall be implemented in compliance with 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 algorithms embedded in the crypto module of S-GW shall be implemented in compliance with respective FIPS standards (for the specific crypto algorithm)."

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

## 6.4 Protecting data and information – Confidential System Internal Data

**Requirement:**

When S-GW 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 to users and administrators.

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.2]

## 6.5 Protecting data and information in storage

**Requirement:**

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

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, encrypt it by implementation-specific means, strictly using the cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

(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 of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)””.

(iii) Stored files: Files having sensitive data shall be protected against manipulation strictly using checksum or cryptographic methods as defined in NCCS approved Secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

**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.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.3]

## 6.6 Protection against Copy of Data

**Requirement:**

Without authentication, S-GW shall not create a copy of data in use or data in transit.

Protective measures shall exist against use of available system functions/software residing in S-GW to create copy of data for illegal transmission. The software functions, components in the S-GW for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

## 6.7 Protection against Data Exfiltration - Overt Channel

**Requirement:**

S-GW shall have mechanisms to prevent data exfiltration attacks for theft of data in use / data in transit. Establishment of outbound overt channels such as, HTTPS IM, P2P, Email etc. are to be forbidden if they are auto-initiated by / auto-originated from the Network product.

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

## 6.8 Protection against Data Exfiltration - Covert Channel

**Requirement:**

S-GW shall have mechanisms to prevent data exfiltration attacks for theft of data in use / data in transit. Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPsec VPN, RTP Encapsulation etc. are to be forbidden if they are auto-initiated by / auto-originated from the Network Product.

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

# Section 7: Network Services

## 7.1 Traffic Filtering – Network Level

**Requirement:**

S-GW shall provide a mechanism to filter incoming IP packets on any IP interface

In particular the Network product 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 any portion of the protocol header.

(v) To reset the accounting.

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.6.2.1]

## 7.2 Traffic Separation

**Requirement:**

S-GW shall support physical and/or logical separation of Operation & Maintenance traffic and control plane traffic. See RFC 3871 [3] for further information.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.5.1].

## 7.3 Traffic Protection – Anti-Spoofing

**Requirement:**

Systems 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.3.1.1]

# Section 8: Attack Prevention Mechanisms

## 8.1 Network Level and application-level DDoS

**Requirement:**

S-GW shall have protection mechanism against known network level and application-level DDoS attacks.

S-GW 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 (as applicable to S-GW) include, but not limited to, the following:

- Restricting of available RAM per application
- Restricting of maximum sessions for a Web application

- Defining the maximum size of a dataset
- Restricting CPU resources per process
- Prioritizing processes
- Limiting of amount or size of transactions of a user or from an IP address in a specific time range
- Limiting of amount or size of transactions to an IP address/port address in a specific time range

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.3.1]

## 8.2 Excessive Overload Protection

**Requirement:**

S-GW shall act in a predictable way if an overload situation cannot be prevented. S-GW 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 S-GW cannot reach an undefined and thus potentially insecure state. In an extreme case, a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.3.3]

## 8.3 Filtering IP Options

**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: 1) 1TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.4.1.1.3]

# Section 9: Vulnerability Testing Requirements

## 9.1 Fuzzing – Network and Application Level

**Requirement:**

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.4.4]

## 9.2 Port Scanning

**Requirement:**

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.4.2]

## 9.3 Vulnerability Scanning

**Requirement:**

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.4.3]

# Section 10: Operating System

## 10.1 Growing Content Handling

**Requirements:**

Growing or dynamic content on S-GW shall not influence system functions. A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop S-GW from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.4.1.1.1]

## 10.2 Handling of ICMP

**Requirement:**

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

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

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

S-GW shall not respond to, or process (i.e. do changes to configuration), under any circumstances certain ICMP message types as marked in below table.

| Type (IPv4) | Type (IPv6) | Description | Send | Respond to | Process (i.e. do changes to configuration) |
|---|---|---|---|---|---|
| 5 | 137 | Redirect | N/A | N/A | Not Permitted |
| 13 | N/A | Timestamp | N/A | Not Permitted | N/A |
| 14 | N/A | Timestamp Reply | Not Permitted (i.e. as automatic reply to "Timestamp") | N/A | N/A |
| N/A | 133 | Router Solicitation | N/A | Not Permitted | Not Permitted |
| N/A | 134 | Router Advertisement | N/A | N/A | Not Permitted |

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.4.1.1.2]

## 10.3 Authenticated Privilege Escalation only

**Requirement:**

S-GW 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.4.1.2.1]

## 10.4 System account identification

**Requirement:**

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.4.2.2]

## 10.5 OS Hardening

**Requirement:**

Appropriate OS hardening procedures including security measures required to ensure the kernel security and miniaturization etc. shall be implemented in S-GW.

Kernel based network functions not needed for the operation of the S-GW shall be deactivated.

[Reference: 1)1 TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.3.1.2]

## 10.6 No automatic launch of removable media

**Requirement:**

S-GW shall not automatically launch any application when removable media device is connected.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.3.1.3]

## 10.7 Protection from buffer overflows

**Requirement:**

S-GW 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 the OEM.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.3.1.5]

## 10.8 External file system mount restrictions

**Requirement:**

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in S-GW 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: 1)1 TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.3.1.6]

## 10.9 File-system Authorization privileges

**Requirement:**

S-GW 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.7]

## 10.10 Restrictions on running Scripts / Batch-processes

**Requirement:**

S-GW shall have feature to restrict Scripts/Batch-processes/Macros usage among various users. It shall be administratively configurable to permit or deny the use. E.g., It is possible to administratively configure scheduled tasks usage (permit/deny) among various users like Normal users, privileged users.

## 10.11 Restrictions on Soft-Restart

**Requirement:**

S-GW 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 S-GW supports web management interface.

## 11.1 HTTPS

**Requirement:**

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.5.1]

## 11.2 Webserver logging

**Requirement:**

Access to the S-GW webserver (for both successful as well as failed attempts) shall be logged by S-GW.

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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.2.5.2.1]

## 11.3 HTTPS input validation

**Requirement:**

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

S-GW 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.5.4]

## 11.4 No system privileges

**Requirement:**

No S-GW web server processes shall run with system privileges.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.2]

## 11.5 No unused HTTPS methods

**Requirement:**

HTTPS methods that are not required for S-GW operation shall be deactivated.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.3]

## 11.6 No unused add-ons

**Requirement:**

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

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.4]

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

**Requirement:**

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.5]

## 11.8 No CGI or other scripting for uploads

**Requirement:**

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.6]

## 11.9 No execution of system commands with SSI

**Requirement:**

If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.7]

## 11.10 Access rights for web server configuration

**Requirement:**

Access rights for S-GW web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.8]

## 11.11 No default content

**Requirement:**

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.9]

## 11.12 No directory listings

**Requirement:**

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.10]

## 11.13 Web server information in HTTPS headers

**Requirement:**

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.11]

## 11.14 Web server information in error pages

**Requirement:**

User-defined error pages and error messages shall not include version information and other internal information about the S-GW web server and the modules/add-ons used.

Default error pages of the S-GW web server shall be replaced by error pages defined by the OEM.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.12]

## 11.15 Minimized file type mappings

**Requirement:**

File type or script-mappings that are not required for S-GW operation shall be deleted.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.13]

## 11.16 Restricted file access

**Requirement:**

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

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.14]

## 11.17 Execute rights exclusive for CGI/Scripting directory

**Requirement:**

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.15]

# Section 12: Other Security requirements

## 12.1. Remote Diagnostic Procedure – Verification

**Requirement:**

If the S-GW 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 the remote machine.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.6]

## 12.2 No System / Root Password Recovery

**Requirement:**

No provision shall exist for S-GW System / Root password recovery.

In the event of system password reset (e.g., through press of Hard-reset button), the entire configuration of the S-GW shall be irretrievably deleted.

## 12.3 Secure System Software Revocation

**Requirement:**

Once the S-GW software image is legally updated/upgraded with new software image, it shall not be possible to roll back to a previous software image.

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

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

## 12.4 Software Integrity Check – Installation

**Requirement:**

S-GW shall validate the software package integrity before the installation/upgrade stage strictly using the secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

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

## 12.5 Software Integrity Check – Boot

**Requirement:**

The S-GW shall verify the integrity of software component(s) at boot time by comparing the result of a standard cryptographic hash generated strictly using the Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” to the expected reference value.

## 12.6 Unused Physical and Logical Interfaces Disabling

**Requirement:**

S-GW shall support the mechanism to verify both the physical and logical interfaces exist in the product.

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

## 12.7 No Default Profile

**Requirement:**

No pre-defined user accounts other than one Highest privilege (Admin / Root) user account would be available

## 12.8 Security Algorithm Modification

**Requirement:**

It shall not be possible to modify security algorithms supported by S-GW without admin / root credentials. Bidding-down beyond prescribed security / cryptographic algorithms by means of negotiation by communicating entities is not permitted.

# Specific Security Requirements

# Section 13: SNMP Security

SNMP is one of the popular network management protocol suite used by industry. This section describes security requirement for SNMP, if a OEM equipment has different TMN protocols, then equivalent security requirements for his TMN protocols shall apply.

## 13.1 Login User Credentials

**Requirement:**

The SNMP login user credential management shall follow the guidelines as defined in S-GW ITSAR Common security requirements document. Each SNMP login user / machine user shall be uniquely identified with UserID and authentication attribute (e.g. password). Group usage is not permitted. Authentication protocols is as per RFC 7860.

[Reference: IETF RFCs: 2570, 3877, 7860]

## 13.2 MIB Whitelisting

**Requirement:**

SNMPv3 Management Information Base (MIB) whitelisting needs to be whitelisted such that the Object Identifiers (OIDs) are limited to that needed for normal device

monitoring/configuration operations. This can be implemented with SNMP view commands with predefined list of MIB objects.

[Reference: IETF RFCs: 2570, 3877, 7860]

## 13.3 Community Naming Convention

**Requirement:**
Factory Default / Commonly used community names like PUBLIC, SYSTEM etc. to be avoided to prevent attacker guessing the names. S-GW needs to prompt admin user during initial configuration for changing the community name.

[Reference: IETF RFCs: 2570, 3877, 7860]

## 13.4 Remote Packet Capture Facility

**Requirement:**
Remote packet capture facility a useful tool for network diagnostics may be exploited by attacker if network access is compromised. This facility is to be default disabled, administratively controlled for troubleshooting purposes.

[Reference: IETF RFCs: 2570, 3877, 7860]

## 13.5 SNMP Query Redirection

~~**Requirement:**~~
S-GW shall not redirect SNMP queries it receives to any other network element, network filters / firewalls. An attacker may purposefully craft packet with non- existing / different node address and send to S-GW, which in turn may redirect packets to other nodes, network filters / firewalls, thereby attacker may learn network rules. S-GW to have mechanism against reconnaissance attacks.

[Reference: IETF RFCs: 2570, 3877, 7860]

# Section 14: NDS / IP Support

## 14.1 Network Domain Security - Architecture

**Requirement:**
S-GW shall support NDS/IP security architecture for connectivity with other network elements, nodes. The NDS/IP key management and distribution architecture is based on the IKEv2 (RFC 7296 [43]) protocol. The NDS/IP architecture is to provide hop-by-hop security in accordance with the *chained-tunnels* or *hub-and-spoke* models of operation. The use of hop-by-hop security also makes it easy to operate separate security policies with-in a security domain and towards other external security domains. S-GW shall support inter-working with SEG (Security Gateway) for Za, Zb security associations.

OEM to provide documentary evidence on NDS /IP architecture support and its mechanisms provided by S-GW.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.210, TS 33.401]

## 14.2 IPSEC on Interfaces

**Requirement:**
S-GW shall support IPSEC feature on all physical / logical interfaces that connect to other Network elements, Nodes. The security association categories of NDS /IP to be followed. Following is the interface specific requirement of IPSEC.

| S.No | Interface Type / Connections | IPSEC Type | Security Association |
|---|---|---|---|
| 1 | S5, S1U, S11, Gxc, Gz, Rf | IPSEC-ESP in with IKEv2 in Tunnel Mode | Zb |
| 2 | S8, S12, S4, S2c | IPSEC-ESP with IKEv2 in Tunnel Mode | Za (necessary that S-GW to have SEG functionality inbuilt) |
| 3 | Network DNS, NTP | IPSEC - ESP | Zb |

**Note:** If any of the remote NEs, Nodes defined under security association Zb fall under different security domain than that of S-GW, then security association Za shall apply.

ISAKMP with Main Mode is the preferred mode to be used for establishment of IPSEC. Aggressive mode shall not be used to minimize dictionary-based crypto attacks.

The IPSEC shall be established between LTE nodes, and shall overlay any transport router infrastructure that connects the LTE nodes.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.210, TS 33.401]

## 14.3 Cryptographic Algorithms – ESP Security Transforms, IKEv2 Profiles

**Requirement:**

The recommended algorithms, transforms and profiles are given in below:

**ESP Encryption Transforms**

The implementation conformance requirements for ESP encryption transforms (including authenticated encryption transforms) in RFC 7321 [45] shall be followed.

Only the ESP encryption algorithms (including authenticated encryption algorithms) mentioned in RFC 7321 [45] shall be used. Algorithms marked with "MUST" shall be supported. AES-256 should be supported. AES-GCM with a 16 octet ICV shall be supported.

**ESP Authentication Transforms**

The implementation conformance requirements for ESP authentication transforms in RFC 7321 [45] shall be followed.

Only the ESP authentication algorithms mentioned in RFC 7321 [45] shall be used. Algorithms marked with "MUST" shall be supported. AES-GMAC with AES-128 shall be supported.

ESP shall always be used to provide integrity, data origin authentication, and anti-replay services, thus the NULL authentication algorithm is explicitly not allowed for use, unless an authenticated encryption algorithm is used.

**IKEv2 Profiles**

The Internet Key Exchange protocol IKEv2 shall be supported for negotiation of IPsec SAs. The following additional requirements apply.

**General:**

IKEv2 Configuration Payload as defined in RFC 7296 [43] should be supported.

Protocol support for High Availability as defined in RFC 6311 [42] should be supported.

**For IKE_SA_INIT exchange:**

The following algorithms are listed with their names according to [44].

Following algorithms shall be supported:

- Confidentiality: ENCR_AES_CBC with 128-bit key length;
- Confidentiality: AES-GCM with a 16 octet ICV with 128-bit key length;
- Pseudo-random function: PRF_HMAC_SHA2_256;
- Integrity: AUTH_HMAC_SHA2_256;
- Diffie-Hellman group 14 (2048-bit MODP);
- Diffie-Hellman group 19 (256-bit random ECP group) ;

Following algorithms should be supported:

- Confidentiality: AES-GCM with a 16 octet ICV with 256-bit key length;
- Pseudo-random function: PRF_HMAC_SHA2_384;
- Diffie-Hellman group 20 (384-bit random ECP group).

NOTE 1: The IANA IKEv2 registry [44] contains further references for the algorithms listed.

For security reasons, the use of Diffie-Hellman MODP groups less than 2048-bit shall not be supported.

**For IKE_AUTH exchange:**

- Authentication method 2 - Shared Key Message Integrity Code shall be supported;
- IP addresses and Fully Qualified Domain Names (FQDN) shall be supported for identification;
- Re-keying of IPsec SAs and IKE SAs shall be supported as specified in RFC 7296 [43].
- In addition to the requirements defined in RFC 7296 [43], rekeying shall not lead to a noticeable degradation of service.

**For the CREATE_CHILD_SA exchange:**

- Perfect Forward Secrecy is optional.

**For reauthentication:**

- Reauthentication of IKE SAs as specified in RFC 7296 [43] section 2.8.3 shall be supported;
- A NE shall proactively initiate reauthentication of IKE SAs, and creation of its Child SAs, i.e. the new SAs shall be established before the old ones expire;
- A NE shall destroy an IKE SA and its Child SAs when the authentication lifetime of the IKE SA expires;

NOTE 2: NE actions related to reauthentication are controlled by locally configured lifetimes according to RFC 4301 [35]: a soft authentication lifetime that warns the implementation to initiate reauthentication, and a hard authentication lifetime when the current IKE SA and its Child SAs are destroyed.

- In addition to the requirements defined in RFC 7296 [43], reauthentication shall not lead to a noticeable degradation of service.

Cryptographic algorithms to be selected as per cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)"

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.210, TS 33.401, IETF RFC: 7296, 7321]

## 14.4 Initialization Vectors for Crypto Keys

**Requirement:**

The Initialization Vector (IV) must be generated in a manner that ensures uniqueness. The same IV and key combination shall not be used more than once. - It is explicitly not allowed to construct the IV from the encrypted data of the preceding encryption process.

The common practice of constructing the IV from the encrypted data of the preceding encryption process means that the IV is disclosed before it is used. A predictable IV exposes IPsec to certain attacks irrespective of the strength of the underlying cipher algorithm. This practice is forbidden in the context of NDS/IP.

These requirements imply that the S-GW must have a capability to generate random data. RFC 4086 [69] gives guidelines for hardware and software pseudorandom number generators.

For CBC mode: the IV field shall be the same size as the block size of the cipher algorithm being used. The IV shall be chosen at random, and shall be unpredictable to any party other than the originator.

- For CTR, GCM, CCM, and GMAC mode: the IV field shall be 8 octets. The IV must be generated in a manner that ensures uniqueness. The same IV and key combination shall not be used more than once. The IV shall be chosen at random, and shall be unpredictable to any party other than the originator.

- It is explicitly not allowed to construct the IV from the encrypted data of the preceding encryption process.

S-GW shall have protection mechanism against RNG compromise / subversion attacks.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.210, TS 33.401, IETF RFC 4086]

## 14.5 Security Policy Granularity

**Requirement:**
The S-GW shall support fine grained security granularity for connectivity between other nodes of the same security domain, and supports coarse grained security granularity for connectivity to the nodes of different security domain. S-GW shall also support security granularity while interworking with SEG (Security Gateways) for inter-domain connectivity.

Operational requirements could range from having VPN granularity at Interface level, APN level, and up to bearer level, SDF, and IP flow levels. S-GW need to support various granularities of IPSEC VPN establishment for meeting operational needs.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.210, TS 33.401]

## 14.6 Protection against VPN Attacks

**Requirement:**
An Attack could utilize the negotiation feature of IPSEC to lower the key size, choose non-prescribed algorithms to lower the security mechanism. S-GW shall have permitted negotiation-matrix feature and procedures to prevent bidding-down attacks.

S-GW shall not permit use of NULL cipher keys, truncated keys, padded keys, weak keys for VPN establishment, operations.

S-GW may provide dynamic IPSEC VPN establishment for certain types of services. It shall have protection mechanism against VPN flood attacks, one of the mitigation strategies is to scrub Infrastructure ACLs before accepting VPN requests.

S-GW shall support feature against DOS attack on the VPN interface. S-GW (endpoint) MUST NOT conclude that the other NE (endpoint) has failed based on any routing information (e.g., ICMP messages) or IKE messages that arrive without cryptographic protection. S-GW must conclude that the other endpoint has failed only when repeated attempts to contact it by sending empty INFORMATIONAL request have gone unanswered for a timeout period or when a cryptographically protected INITIAL_CONTACT notification is received on a different IKE SA to the same authenticated identity. [RFC 7296]

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.210, TS 33.401, IETF RFC 7296]

## 14.7 SA Lifetime – Key Freshness

**Requirement:**
Key freshness is an important security criterion to minimize risks of exploitations based on key shelf-life, dictionary based crypto attacks. The Security Associations (SA) lifetimes should be administrator defined. S-GW shall have the capability of creating, negotiating child SAs with new set of cryptographic keys in parallel with same traffic selectors with the remote NE before expiry of lifetime of existing SA. The rekeying of SA with remote NE shall be such that no packet loss is observed and no noticeable degradation of performance is observed while shifting the traffic from old SA to new SA. The old SA keys shall be destructed / deleted.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.210, TS 33.401, IETF RFC 7296]

## 14.8 Security Policy Database (SPD)

**Requirement:**
The Security Policy Database (SPD) is a policy instrument to decide which security services are to be offered and in what fashion.
The SPD shall be consulted during processing of both inbound and outbound traffic. This also includes traffic that shall not/need not be protected by IPsec. In order to achieve this the SPD must have unique entries for both inbound and outbound traffic such that the SPD can discriminate among traffic that shall be protected by IPsec, that shall bypass IPsec or that shall be discarded by IPsec.

The SPD plays a central role when defining security policies, both within the internal security domain and towards external security domains. The security policy towards external security domains will be subject to roaming agreements.

The Security Association Database (SAD) contains parameters that are associated with the active security associations. Every SA has an entry in the SAD. For outbound processing, a lookup in the SPD will point to an entry in the SAD. If an SPD entry does not point to an SA that is appropriate for the packet, an SA shall be automatically created.

S-GW shall maintain logically separate databases SAD, SPD for each interface, depicting separate entries for each of Security Associations (SAs) and for SPIs.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.210, TS 33.401, IETF RFC 7296]

# Section 15: EPS Bearer Security

## 15.1 Inactive EPS Bearers

**Requirement:**
EPS inactive bearers may get hijacked by malicious attacker for fraudulent usage before the bearers are withdrawn due to system defined timeouts. Suitable mechanism should exist to putdown the inactive bearers before they are made for reuse.

This also applies for inactive emergency bearers. The inactivity period to be administratively configurable.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33. 210, TS 33. 250, TS 33.401]

## 15.2 GTP Protocol Support

**Requirement:**
S-GW shall support GTPv2-C / eGTP-C for control messages and GTPv1-U / eGTP-U for data traffic and GTP' / GTPP for charge transfer.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.210, TS 33.401, TS 29.281]

## 15.3 Uniqueness of Terminal Identifiers

**Requirement:**
S-GW shall generate unique TEIDs for GTP tunnels to minimize repudiation based attacks. A TEID is not assigned to more than one active GTP tunnel at the same time. The reuse of TEID is possible after a GTP tunnel has been terminated and the TEID related to this GTP tunnel has been released

[Reference: TSDSI STD T1.3GPP Release-14: TS 29.281, TS 33. 210, TS 33. 250, TS 33.401]

## 15.4 Randomness of Terminal Identifiers

**Requirement:**
S-GW shall generate random TEIDs for GTP tunnels to minimize reconnaissance, sequence guessing, dictionary based attacks.

[Reference: TSDSI STD T1.3GPP Release-14: TS 29.281, TS 33. 210, TS 33.401]

## 15.5 Protection of GTP-C – Inter Security Domain

**Requirement:**
IPSec ESP in Tunnel mode shall be used with origin determination, encryption and integrity protection for all GTP-C messages traversing inter-security domain boundaries.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.210, TS 33.401, TS 29.281]

## 15.6 Policy Discrimination of GTP-C and GTP-U

**Requirement:**
It must be possible to discriminate between GTP-C, GTP-U messages, which shall receive protection, and other messages, that may or may not be protected as per the administrative configurations. Since GTP-C is assigned a unique UDP port-number in (TS29.060 [6]) IPsec can easily distinguish GTP-C datagrams from other datagrams that may not need IPsec protection.

SGW shall support the user plane traffic differentiation (e.g. enterprise, internet, etc) by setting the specific APNs, and shall support the traffic isolation based on the APNs (e.g. using VPN).

Security policies shall be checked for all traffic (both incoming and outgoing) so datagrams can be processed in the following ways:

- discard the datagram;
- bypass the datagram (do not apply IPsec);
- apply IPsec.

The SPD shall have pointer to an entry in the Security Association Database (SAD) which details the actual protection to be applied to the datagram.

For preventing Eavesdrop, MITM attacks both GTP-C, GTP-U packets shall be IPsec encrypted.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.210, TS 33.250, TS 33.401, TS 29.281]

# Section 16: Database Security

## 16.1 Guard against Database Attacks

**Requirement:**
S-GW may store information with regard to PDP connections, Context information, UE profiles, ME Identities, Bearer TFTs etc., in the form of database, tables or data structures. Successful attack on S-GW data can cause corruption of information, disclose the information or lead to loss of information that impairs confidentiality, performance of the network. The S-GW Database need to be secured against all well-known SQL Injection / Database attacks.

# Section 17: Diameter Interfaces

## 17.1 End to End security for Diameter Interface

**Requirement:**
Diameter protocol is used to exchange charging data information exchange, including sensitive data like User ID, Passwords etc. The diameter interfaces Gxc, Gr, Rf which are supported by S-GW shall necessarily deploy TLS / DTLS (refer to “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” to communicate with other end node.

[Reference: 3GPP Release-15 TS 32.299, IETF RFC 3588, 6733]

## 17.2 Configuration of Diameter Peers

**Requirement:**
Proper configuration of the trust model with a Diameter peer is essential to security. The peers may be administratively configured or with use of root certificates for dynamic peering. Diameter connectivity will not be established to arbitrary peers.

Trusted security association is required with mutual authentication for establishment of Diameter connection.

[Reference: 3GPP Release-15 TS 32.299, IETF RFC 3588, 6733]

# Section 18: Network Security

S-GW to support various network level security features mentioned in this section

## 18.1 VLAN Support

**Requirements:**
S-GW shall support VLAN configurations to segregate various types of logical interfaces over physical interfaces.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.210, TS 33.401]

## 18.2 NAT / Tr. GW Restrictions

**Requirements:**

Network Address Translation (NAT) / Transition Gateway (Tr. GW) features not to be supported by S-GW on its interfaces as hop by hop security is envisaged under NDS / IP.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.210, TS 33.401]

## 18.3 IPV6 Vulnerabilities

**Requirements:**
S-GW may utilize IPV6 for bearer traffic, mobility anchoring, for hand-over traffic and for handling traffic from non-3GPP networks. Following common IPV6 vulnerabilities need to be suitably addressed in S-GW design.

**Dual Stack operation**: S-GW may need to serve both IPV4 and IPV6 traffics for performing various functionalities. The ACLs, rate limiters need to be harmonized between both technologies to prevent adjacent attacker exploiting the IPV4, IPV6

address assignments. S-GW ingress filters need to have capability to prevent DOS attacks originating from iPV4 address space and using IPV6 capabilities like ICMPV6 and vice versa (e.g. Smurf attack using ICMPV6 packets for reply to a IPV6 address).

**Address Assignment**: S-GW to follow random address allotment with in the assigned IPV6 address pool to minimize reconnaissance attacks by insiders.

**Assignment of multiple address**: The proxy IPV6 address assignment generally to be limited to 1 per HoA, unless specific need exists. Allotment of multiple addresses to same resource burdens Filtering policies of the S-GW.

**Link Layer Security**: Neighbor discovery protocol (NDP) is to be secured to prevent address spoofing, duplicate address, redirection, DOS amplification attacks, S-GW shall have protection mechanisms against Link Layer vulnerabilities of IPV6. The network to be planned as point-to-point links so that it has no link layer address discovery, such policy avoids address resolution requirement and prevents attacks based on duplicate address.

**Fragmentation:** S-GW should not permit fragmentation feature of IPV6 packets as an attack can be sent to target node through fragments, when reassembly takes place, chance for remote code execution exists.

[Reference: RFC 2460, TSDSI STD T1.3GPP Release-14: TS 29.061]

## 18.4 DHCP Security

**Requirement:**
S-GW receives IP allotment offer messages / notifications for Infrastructure IPs, Tunnel IPs, and Proxy IPs from various DHCP servers deployed in the network. To prevent Rogue DHCP servers, spoofing attacks, S-GW need to establish Trust relationships, secure paths to the DHCP servers before accepting the notifications.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.402, TS 23.402]

## 18.5 DNS Security

**Requirement:**
S-GW need to support DNSSEC implementation by the network on IPv4 / IPv6. Zone segregation, not permitting recursive queries to authoritative servers are some of the measures deployed by networks to build DNS security,.

S-GW shall have mechanisms for Origin determination, Message integrity checks to avoid spoofed DNS replies from poisoned DNS caches, compromised servers, MITM attacks.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.402, TS 23.402, IETF RFC 4033]

## 18.6 Protection against Rogue NEs, Insider Attacks

**Requirement:**

. S-GW shall have whitelisting policy of network neighbors for detecting Rogue NEs. S-GW should have ability to monitor malicious packets, inspect and drop packets found suspicious

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.402, TS 23.402]

## 18.7 Security of Pooled NEs

**Requirement:**

The LTE core equipment may be deployed under pool for traffic sharing. GTP-C is used for messaging overload conditions and for load balancing functions.

During S-GW to S-GW load re-balancing, ECM-CONNECTED states might be transferred to new S-GW along with bearer traffic in buffer. During the context transfer it is to be ensured that IMSI, IMEI and ME Identities are not revealed or transferred. Before commencement of the load transfer procedures, IPSEC VPN to be established between the S-GWs for establishing trusted relationship.

[Reference: TSDSI STD T1.3GPP Release-14: TS 33.402, TS 23.402]

# Section 19: Lawful Interception

The requirements under this section are applicable to SGW if it supports X1_1, X2, X3 interfaces. Lawful Interception feature shall comply with Indian National standards TEC GR/WS/LIS -003/01 MARCH, 2011 and its latest versions Or Indian national standards for Lawful Interception issued from time to time, and shall follow TSDSI STD T1.3GPP TS 33.106, TS 33.107 and TS 33.108 standards of Release 14 or later.

## 19.1 LI Interface Support

**Requirement:**
S-GW to support LI interface standards and the type of traffic / data to be handled

| Sr. No. | LI Interface | Traffic / Data flow | Connected Element |
|---|---|---|---|
| 1 | X1_1 | LI requests | ADMF |
| 2 | X2 | Intercept Related Information (IRI) | DF2 |
| 3 | X3 | Communication Content (CC) | DF3 |

[Reference: TEC GR/WS/LIS -003/01 MARCH, 2011, TSDSI STD T1.3GPP-Release-14: TS 33.106, TS 33.107, TS33.108]

## 19.2 LI Events

**Requirement:**
The following events are applicable to the S-GW:

- Bearer activation (valid for both Default and Dedicated bearer);
- Start of intercept with bearer active;
- Bearer modification;
- Bearer deactivation;
- UE Requested Bearer Resource Modification;
- Packet Data Header Information.
- A data packet is transmitted to or from a target

Intercept Related Information (Events) shall be sent at attach/tunnel activation, detach/tunnel deactivation, tunnel modification, start of interception with active PMIP tunnel, PMIP session modification, PDN-GW initiated PDN-disconnection, UE requested PDN connectivity, Serving Evolved Packet System, subscriber record change, registration termination, location information request , and LALS Location Report.

[Reference: TEC GR/WS/LIS -003/01 MARCH, 2011, TSDSI STD T1.3GPP-Release-14: TS 33.106, TS 33.107, TS33.108]

## 19.3 LI Message Exchange Requirement

**Requirement:**

**Target Information:** Target identities used for interception for each domain and service are: target service and equipment associated with target use or any derived IDs from such elements that are to be defined in TSDSI STD T1.3GPP TS 33.107 [9] and TS 33.108 [10]. Examples of these identities are IMSI, MSISDN, NAI, Tel URI, SIP URI, for the target service and IMEI, MAC for the equipment. Normally the long-term / permanent identities such as IMSI, MSISDN, ME identity are used for Target Identity.

This information to be accepted on X1_1 interface.

**S-GW to DF2 Information on X2 Interface:** target identity (IMSI, MSISDN, ME identity);

- events and associated parameters as defined reference documents may be provided;
- the target location (if available) or the IAs in case of location dependent interception;
- correlation number;
- Quality of Service (QoS) information (if available);
- encryption parameters (keys and associated parameters for decrypting CC), if available and necessary.
- meta data information of the target identity and its data

**S-GW to DF3 Information on X3 Interface:** S-GW to send Communication content to DF3 on X3 interface. In addition to the intercepted content of communication, the following information needs to be transferred from the S-GW to the DF3 to perform its functionality:

- target identity;
- correlation number;
- time stamp (optional);
- direction (indicates whether T-PDU is MO or MT) - optional;
- the target location (if available) or the IAs in case of location dependent interception.

If more than one bearer is active, for each of them an event record is generated. The parameters which are defined for bearer activation (see related section) will be sent, if available, by the S-GW to the DF2, in case the event is sent due to a change of the involved S-GW, the new S-GW may provide as additional parameter, the "old location information". However, the absence of this information does not imply that interception has not started in the old location S-GW for an active bearer.

This event is used to provide packet header reports on a per packet basis (non-summarized reporting) and is triggered by each packet sent or received by the target. These elements will be delivered by the S-GW either directly to DF2.

[Reference: TEC GR/WS/LIS -003/01 MARCH, 2011, TSDSI STD T1.3GPP-Release-14: TS 33.106, TS 33.107, TS33.108]

## 19.4 Unique Correlation Number

**Requirement:**
For the delivery of the CC and IRI, the S-GW provides correlation number and target identity to the DF2 and DF3 which is used there in order to select the different LEAs where the product shall be delivered.

The correlation number is unique in the whole PLMN and is used to correlate CC with IRI and the different IRI's of one IP-CAN session. However, when different protocols (i.e. GTP and PMIP) are used in the network, different values can be generated by different nodes. The correlation number shall be generated by using existing parameters related to the IP-CAN session.

[Reference: TEC GR/WS/LIS -003/01 MARCH, 2011, TSDSI STD T1.3GPP-Release-14: TS 33.106, TS 33.107, TS33.108]

## 19.5 Encrypted Data Handling

**Requirement:**
When encryption is provided and managed by the network like Hop by Hop encryption, the network provides the intercepted communication to the LEA decrypted, or encrypted with keys and additional information to make decryption possible. End-to-end encryption implemented in the user equipment based on encryption features

provided by the operator is considered to be a network-managed encryption and is subject to the same requirements.

When compression is provided and managed by the network, the network provides the intercepted communication to the LEA decompressed, or compressed with information to make decompression possible.

When encoding is provided and managed by the network, the network provides the intercepted communication to the LEA decoded, or encoded with capability (e.g., codec information) to make decoding possible.

[Reference: TEC GR/WS/LIS -003/01 MARCH, 2011, TSDSI STD T1.3GPP-Release-14: TS 33.106, TS 33.107, TS33.108]

## 19.6 LI Administration Security

**Requirement:**
The administration of the LI function, i.e. Activation, Deactivation and Interrogation of Lawful Interception, in the S-GW and the DFs shall be done securely as described below:

- The user access to LI functionality shall be controlled with authentication mechanism. It shall be possible to configure the authorized user access within the serving network to Activate, Deactivate and Interrogate Lawful Interception separately for every physical or logical port at the S-GW and DF.
- Only the ADMF is allowed to have access to the LI functionality of the S-GW and DF.
- The communication links between ADMF to S-GW shall be secure using IPSEC-ESP VPN and Mutual authentication, Origin Determination to prevent attacks like masquerading, spoofing.

Through the use of user access restrictions, no unauthorized network entities or remote equipment shall be able to view or manipulate LI data in the 3G GSN, 3G MSC Server, LI LCS Client, CSCF, 3GPP ICE, any 3GPP nodes, and Administration nodes of this specification or the DFs.

[Reference: TEC GR/WS/LIS -003/01 MARCH, 2011, TSDSI STD T1.3GPP-Release-14: TS 33.106, TS 33.107, TS33.108]

## 19.7 Intercept Related Information (IRI) Security

**Requirement:**

**Normal operation:** The transmission of the IRI shall be done in a secure manner using IPSEC-ESP VPN between S-GW and DF2 on X2 interface.

**Communication failure:** Depending on the national law in case of communication failure IRI may be buffered in the S-GW. After successful transmission of IRI the whole buffer shall be deleted. It shall be possible to delete the content buffer via command or a timer, in an un-restorable fashion.

[Reference: TEC GR/WS/LIS -003/01 MARCH, 2011, TSDSI STD T1.3GPP-Release-14: TS 33.106, TS 33.107, TS33.108]

## 19.8 Communication Content (CC) Security

**Requirement:**
The transmission of the CC shall be done in a secure manner using IPSEC-ESP VPN between S-GW and DF3 on X3 interface.

In case of transmission failure, no buffering is required within the intercepting network.

[Reference: TEC GR/WS/LIS -003/01 MARCH, 2011, TSDSI STD T1.3GPP-Release-14: TS 33.106, TS 33.107, TS33.108]

## 19.9 LI Data at Rest Security

**Requirement:**

**Data Confidentiality:** The data pertaining to target, IRI data, meta-data information, CC data and the corresponding LOGs shall be protected in S-GW and are accessible only to authorized administrator with authentication.

**Log files:** Log files for LI activity shall be generated by the ADMF, DF2, DF3, S-GW. All log files are retrievable by the ADMF, and are maintained by the ADMF in a secure manner.

**Data consistency:** The administration function in the ADMF or S-GW shall be capable of performing a periodic consistency check to ensure that the target list of target

identities in all involved S-GWs and the DFs contain the appropriate target Ids consistent with the intercept orders in the ADMF. The reference data base is the ADMF data base.

[Reference: TEC GR/WS/LIS -003/01 MARCH, 2011, TSDSI STD T1.3GPP-Release-14: TS 33.106, TS 33.107, TS33.108]

# Section 20: Additional Security Requirements

## 20.1 No Known vulnerabilities in ASICs, SOC Solutions

**Requirement:**

In addition to general purpose Processors, the S-GW may utilize in its design various ASICs, System on Chip (SOC) solutions that are application specific or of custom make. OEM need to provide self-test / third-party / Chip-Maker test report indicating that such ASICs, SOCs are free from malware, known-vulnerabilities. OEM shall submit an undertaking stating that ASCIs, SOC solutions used in S-GW is free from all known malware and backdoors.

# Annexure- I

| | |
|---|---|
| AAA Server | Authentication, Authorization, and Accounting Server |
| CVE | Common Vulnerabilities and Exposures |
| CWE | Common Weakness Enumeration |
| DDOS | Distributed Denial of Service |
| S-GW | Network Element |
| FIPS | Federal Information Processing Standards |
| HTTP | Hypertext Transfer Protocol |

| | |
|---|---|
| HTTPS | Hypertext Transfer Protocol Secure |
| IPSec VPN | Internet Protocol Security Virtual Private Network |
| MISRA | Motor Industry Software Reliability Association |
| NIST | National Institute of Standards and Technology |
| NTP | Network Time Protocol |
| OS | Operating System |
| PTP | Precision Time protocol |
| RADIUS | Remote Authentication Dial-In User Service |
| RIP | Routing Information Protocol |
| SFTP | Secure File Transfer Protocol |
| SHA | Secure hash Algorithm |
| SIP | Session Initiation Protocol |
| SNMP | Simple Network Management Protocol |
| SSH | Secure Shell |
| SSL | Secure Sockets Layer |
| TFTP | Trivial File Transfer Protocol |
| TLS VPN | Transport Layer Security Virtual Private Network |
| URPF | Unicast Reverse Path Forwarding |
| AES | Advanced Encryption Standard |
| AK | Anonymity Key |
| AKA | Authentication and Key Agreement |
| AMF | Authentication Management Field |
| AN | Access Network |
| AS | Access Stratum |
| AUTN | Authentication token |
| AV | Authentication Vector |
| ASME | Access Security Management Entity |
| DoS | Denial of Service |

| | |
|---|---|
| EEA | EPS Encryption Algorithm |
| EIA | EPS Integrity Algorithm |
| eNB | Evolved Node-B |
| EPC | Evolved Packet Core |
| EPS | Evolved Packet System |
| EPS-AV | EPS authentication vector |
| E-UTRAN | Evolved UTRAN |
| GUTI | Globally Unique Temporary Identity |
| HE | Home Environment |
| HSS | Home Subscriber Server |
| IK | Integrity Key |
| IKE | Internet Key Exchange |
| IMEI | International Mobile Station Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| KDF | Key Derivation Function |
| KSI | Key Set Identifier |
| MAC | Message Authentication Code |
| ME | Mobile Equipment |
| MME | Mobility Management Entity |
| MS | Mobile Station |
| MSC | Mobile Switching Centre |
| MSIN | Mobile Station Identification Number |
| NAS | Non Access Stratum |
| NCCS | National Centre For Communication Security |
| NTP | Network Time Protocol |
| OS | Operating System |
| PLMN | Public Land Mobile Network |
| PTP | Precision Time Protocol |


NCCS
Securing Networks

# Annexure- II

**LIST OF UNDERTAKINGS TO BE FURNISHED BY THE OEM FOR S-GW SECURITY TESTING**

1. Source Code Security Assurance (against test case 3.3)
2. Known Malware and backdoor Check (against test case 3.4)
3. Avoidance of Unspecified Wireless Access (against test case 4.3)
4. Cryptographic Module Security Assurance (against test case 6.2)
5. Cryptographic Algorithms implementation Security Assurance (against test case 6.3)