सत्यमेव जयते

Indian Telecommunication Security Assurance Requirements (ITSAR)

PACKET DATA NETWORK GATEWAY (P-GW/PDN GW)

Release Date: Version: 1.0.0

Enforcement Date:

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

About NCCS

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

Disclaimer: This document purely focusses on the security related technical requirements of the P-GW. The regulations regarding Remote Access, Lawful Interceptions are not part of this ITSAR.

Document History

Sl. No	ITSAR Reference	Title	Remarks
1			

Contents

A) Overview:

This document defines the security requirements of Packet Data Network(PDN) Gateway, abbreviated as P-GW, which is an important logical functional entity in the core part of the Evolved Packet System(4G). It provides connectivity between the user equipment and the external packet data networks by acting through the interface between the EPS Core network and external packet network. Its main functions include IP address Allocation, Policy & charging enforcement and lawful interception.

The objective of this document is to present a comprehensive, country specific security requirements for the P-GW. There are various International standardization bodies/associations working on the security aspects related to communication products. 3GPP, ETSI, GSMA, CC are few among them. The specifications produced by these bodies along with the country specific security requirements are the basis for this document.

This document commences with a brief description of P-GW, its various interfaces, the logical entities associated with it and then proceeds to address the common and entity specific security requirements of P-GW.

B) Scope:

This document targets on the security requirements of P-GW in a non-virtualized environment. GTP based mobility management (not PMIP -Proxy Mobile IP) is discussed as it is the most prominent implementation. This document does not cover the security requirements at equipment vendor’s facility, operator facility and organization’s security policy. The requirements specified here are binding both on operators and network equipment providers.

C) References:

1. TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0: "Catalogue of General Security Assurance Requirements".
2. TSDSI STD T1.3GPP 33.250-14.0.0 V.1.0.0:Security Assurance Specification for the PGW network product class.
3. TSDSI STD T1.3GPP 33.210 14.0.0 V.1.0.0:Network Domain Security (NDS)/IP Network Layer Security.
4. TSDSI STD T1.3GPP 33.401 14.5.0 V.1.0.0 : "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".
5. TSDSI STD T1.3GPP 33.926-14.0.0 V1.0.0 Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes.
6. 3GPP TS 23.203: "Policy and charging control architecture".
7. 3GPP TS 32.251: " Packet Switched (PS) domain charging”
8. NIST FIPS 140-2 specification.
9. Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0

D) Definitions and Acronyms

D.1 Definitions

1. AMBR: Aggregate Maximum Bit Rate. The same bearer may contain many IP flows and AMBR indicates the total maximum bit rate a UE may have for all bearers in the same PDN connection.

2. ARP: Allocation and Retention Priority indicates the priority of the bearer compared to other bearers. This provides the basis for admission control in bearer set-up, and further in a congestion situation if bearers need to be dropped.

3. Bearer: An information transmission path of defined capacity, delay and bit error value etc.

4. Charging Identifier: It uniquely identifies charging records generated by SGW and PDN GW.

5. Cryptanalysis: The process of deriving the plaintext from the ciphertext (breaking a code) without being in possession of the key or the system (also called as code breaking).

6. Cryptography: The enciphering and deciphering of messages into secret codes by means of various transformations of the plaintext.

7. DiffServ Code Point: A Differentiated Services Code Point (DSCP) is a packet header value that can be used to request (for example) high priority or best effort delivery for IP traffic.

8. E-UTRAN Node-B (eNodeB): eNodeB is the Radio Base Station which handles all radio related functions of E-UTRAN. It is the only node in the E-UTRAN and serves as a Layer 2 bridge between EPC and UE.

9. E-UTRAN: Evolved UTRAN is the radio part of EPS and handles the EPC's radio communication with UE.

10. Evolved Packet Core (EPC): It is a flat, all-IP based core network of EPS.

11. Evolved Packet System (EPS): EPS is the 3GPP name for UMTS evolution. It includes both EPC and E-UTRAN.

12. GBR: Guaranteed Bit Rate- the bit rate that can be guaranteed to the bearer.

13. GTP Tunnel: GTP tunnels are used between two nodes communicating over a GTP based interface, to separate traffic into different communication flows. A GTP tunnel is identified in each node with a TEID, an IP address and a UDP port number. The receiving end side of a GTP tunnel locally assigns the TEID value the transmitting side has to use. The TEID values are exchanged between tunnel endpoints using GTP-C or S1-MME messages.

14. IMSI: The international mobile subscriber identity is a unique 15-digit number provided to the subscriber. It consists of the MCC, MNC, and MSIN.

15. IP-CAN bearer: An IP transmission path of defined capacity, delay and bit error rate, etc. for the definition of bearer.

16. IP-CAN: The collection of network entities and interfaces that provides the underlying IP transport connectivity between the UE and say, the IMS entities.

17. Long Term Evolution (LTE): Formally, the name of work item which developed radio access technology and E-UTRAN.

18. MBR: Maximum Bit Rate for the bearer.

19. Mobile Station (MS): It encompasses both mobile equipment and SIM card.

20. Mobility Management Entity (MME): MME is the main control plane element in the EPC.

21. MSISDN: The Mobile Station International Subscriber Directory Number is intended to convey the telephone number assigned to the subscriber for receiving calls on the phone. It has country code +National Destination Code + subscriber number format.

22. MTCTE: Mandatory Testing and Certification of Telecom Equipments. Department of Telecommunications, Ministry of Communications (the licensor) has notified “Indian Telegraph (Amendment) Rules” in Gazette of India vide G.S.R. 1131(E) PART XI" on 5th September 2017 which prescribes for Mandatory Testing and Certification of Telecommunication Equipment. Any telegraph which is used or capable of being used with any telegraph established, maintained or worked under the license granted by the Central Government in accordance with the provisions of section 4 of the Indian Telegraph Act, 1885 (hereinafter referred to as the said Act), shall have to undergo prior mandatory testing and certification in respect of parameters as determined by the telegraph authority from time to time.

23. Operator/Telecommunication Service Provider: An entity who has been granted with the license to provide telecommunication services in the country.

24. Original Equipment Manufacturer (OEM): Manufacturer of communication and its related products under whose brand, the products are sold or proposed to be sold to operators in the country. In case of telecommunication industry, OEMs are also called as Network Equipment Provider (NEP) or telecom gear makers/manufacturer.

25. Packet Filtering: It is a network security mechanism that controls the packets flow into and outside the network based on origin IP address, destination IP address, session and application layer protocols etc.

26. Packet flow: A specific user data flow from and /or to the UE.

27. Packet Screening: The packet screening function provides the network with the capability to check that the UE is using the exact IPv4- Address and/or IPv6-Prefix that was assigned to the UE.

28. Policy and Charging Resource Function (PCRF): PCRF is responsible for QoS handling and charging in EPC.

29. QCI: QoS Class Identifier. It is an index which references to a specific packet forwarding behavior related to QoS attributes like priority, delay and loss rate.

30. Rate (Traffic) Policing: It propagates the traffic bursts. When the traffic rate reaches the configured maximum rate, excess traffic is dropped (or remarked). The result is an output rate that appears as a saw-tooth with crests and troughs.

31. Rate (Traffic) Shaping: In contrast to policing, traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time. The result of traffic shaping is a smoothed packet output rate.

32. SDF: Service Data Flow. An aggregate set of packet flows carried through the PCEF that matches a service data flow template.

33. Service Architecture Evolution (SAE): SAE is a 3GPP work item for the evolution of 3G packet core. It is also referred as EPC.

34. Serving Gateway (S-GW): S-GW is the part of EPC and is responsible for routing and forwarding of user data packets to and from UE. It primarily serves as an anchor point for intra-LTE mobility.

35. SIM: Subscriber Identity Module. It is the ICC defined for 2G mobile communication (GSM). It has originally been specified as one physical and logical entity, not distinguishing platform and application. In 3G, the SIM may also be an application on the 3G UICC, then of course only represented by its logical characteristics. If the SIM application is active, the UICC is functionally identical to a 2G SIM. The SIM (or SIM application on a UICC) does only accept 2G commands.

36. TEID: A GTP tunnel endpoint is identified with a TEID, an IP address and a UDP port number. TEID unambiguously identifies a tunnel endpoint in scope of a path. (The TEID is a unique identifier within one IP address of a logical node)

37. (U)ICC platform: It includes security IC, card Operating System and related configuration data.

38. UICC: Universal Integrated Circuit card. It is a tamper resistant smart card hardware containing file and folder systems which can host more than one network application. SIM, USIM (Universal SIM), ISIM (IMS SIM), TSIM (Tetra SIM) and RUIM (Removeable User Identity Module -used for CDMA systems) are referred to as subscription containers of the UICC. The UICC is the physical and logical platform for the USIM. It does at least contain one USIM application and may additionally contain a SIM application. Further to that, the UICC may contain additional USIMs and other applications, e.g. for mobile banking or mobile commerce purposes, if these fit with the basic physical and logical characteristics of the UICC.

39. UMTS: Universal Mobile Telecommunication systems is the 3G evolution of GSM/GPRS network. UMTS standards are defined by 3GPP.

40. User Equipment (UE): Typically, a hand held device used by the end user for communication purpose. It encompasses both Terminal Equipment (TE) and USIM.

41. USIM: Universal SIM. It is a logical application residing on the UICC. It does only accept set of defined commands.

42. UTRAN: It is an acronym for UMTS Terrestrial Radio Access Network.

D.2 Acronyms

2G: Second Generation Technology

3G: Third Generation Technology

3GPP: 3rd Generation Participation Project

4G: Fourth Generation Technology

AES: Advanced Encryption Standards

AMBR: Aggregate Maximum Bit Rate

APDU: Application Protocol Data Unit

ARP: Allocation and Retention Policy

CGI: Common Gateway Interface

Charging Id: Charging Identifier

DHCP: Dynamic Host Configuration Protocol

DL: Downlink

EPC: Evolved Packet Core

EPS: Evolved Packet System

ETSI: European Telecommunication Standards Institute

GBT: Guaranteed Bit Rate

GSMA: GSM Association

GTP: GPRS Tunneling Protocol

IP-CAN: IP Connectivity Access Network

LEA: Law Enforcement Agencies

MBR: Maximum Bit Rate

MS: Mobile Station

OAM: Operation, Administration and Maintenance

OCS: Online Charging System

OFCS: Offline Charging System

OS: Operating System

PCC: Policy and Charging Control

PIN: Personal Identification Number

QCI: QoS Class Identifier

SCTP: Stream Control Transmission Protocol

SDF: Service Data Flow

SEG: Security Gateway

TEID: Tunnel End Point Identifier

TSTL: Telecom Security Testing Laboratory

UE: User Equipment

UL: Uplink

E) Conventions

1. Must or shall or required denotes absolute requirement of particular clause of ITSAR.

2. Must not or shall not denotes absolute prohibition of particular clause of ITSAR.

3. Should or Recommended denotes that the particular clause of ITSAR may be ignored under justifiable circumstances but after careful examination of its implications.

4. Should not or not Recommended denotes the opposite meaning of (3) above.

Chapter 1 - Introduction

The P-GW, a functional logical entity of 4G mobile Core system, acts as a point of interconnection with the external packet data networks. External packet data networks may include public internet, company intranet and operator's IMS. It acts as an Edge Router between external packet data networks and EPS. Along with S-GW, P-GW handles user plane traffic. It may also possible to implement both S-GW and P-GW in the same node. Policy and Charging Enforcement function (PCEF) which resides inside P-GW is used by PCRF for policy and charging enforcement. P-GW plays significant role in providing QoS to end user services.

In addition, P-GW is a mobility anchor for non-3GPP radio access technologies like WLAN, Wi MAX, 3GPP2 etc. During Home Routed roaming scenario, home P-GW is involved for connection establishment.

The P-GW functions include

a) UE IP address allocation (IPv4 & IPv6).
b) Per-user based packet filtering. (e.g. deep packet inspection for virus signature detection)
c) Lawful Interception through appropriate interface to LEAs.
d) Transport level packet marking in the uplink and downlink, e.g. setting the DiffServ Code Point, based on the QCI, and optionally the ARP priority level, of the associated EPS bearer.
e) Accounting for inter-operator charging: for home routed roaming, the P-GW shall collect and report the uplink and downlink data volume (per EPS bearer) as received from and sent to the serving node.
f) UL and DL service level charging (based on the SDFs defined by the PCRF or based on deep packet inspection defined by local policy)
g) UL and DL service level gating control (based on filters like source IP, destination IP, ports, protocol the flow of IP packets is allowed or denied)
h) UL and DL service level rate enforcement (the amount of IP packets flowing through the node is kept within the applicable limits. Methods to achieve this are rate policing (may lead to dropping of packets) and shaping (e.g. short time buffering), per individual Service Data Flow.
i) UL and DL rate enforcement based on APN-AMBR (applies to all SDFs of the same APN that are associated with Non-Guaranteed bit rate QCIs).
j) DL rate enforcement based on the accumulated MBRs of the aggregate of SDFs with the same GBR QCI.

k) DHCPv4 (server and client) and DHCPv6 (client and server) functions for IP address allocation or IP parameter configuration.

l) Packet screening.

m) Interfacing OFCS and OCS.

n) Sending of one or more "end marker" to the source SGW immediately after switching the path during SGW change.

o) UL and DL bearer binding (this is the procedure that associates a service data flow defined in a PCC and QoS rule based on a service data flow template, to the EPS bearer deemed to transport the service data flow)

p) UL bearer binding verification (this is a cross check of the network, if the UE has applied correct uplink bearer binding).

q) Functionality as defined in RFC 4861(IP neighbourhood detection functionality: the PDN GW sends Router Advertisements, handles Router Solicitations received from the UEs and handles Neighbour Solicitations. In other words, the PDN GW acts as the access IP router for the UE, terminating the virtual link provided by the GTP-U tunnel)

r) Accounting per UE and bearer.

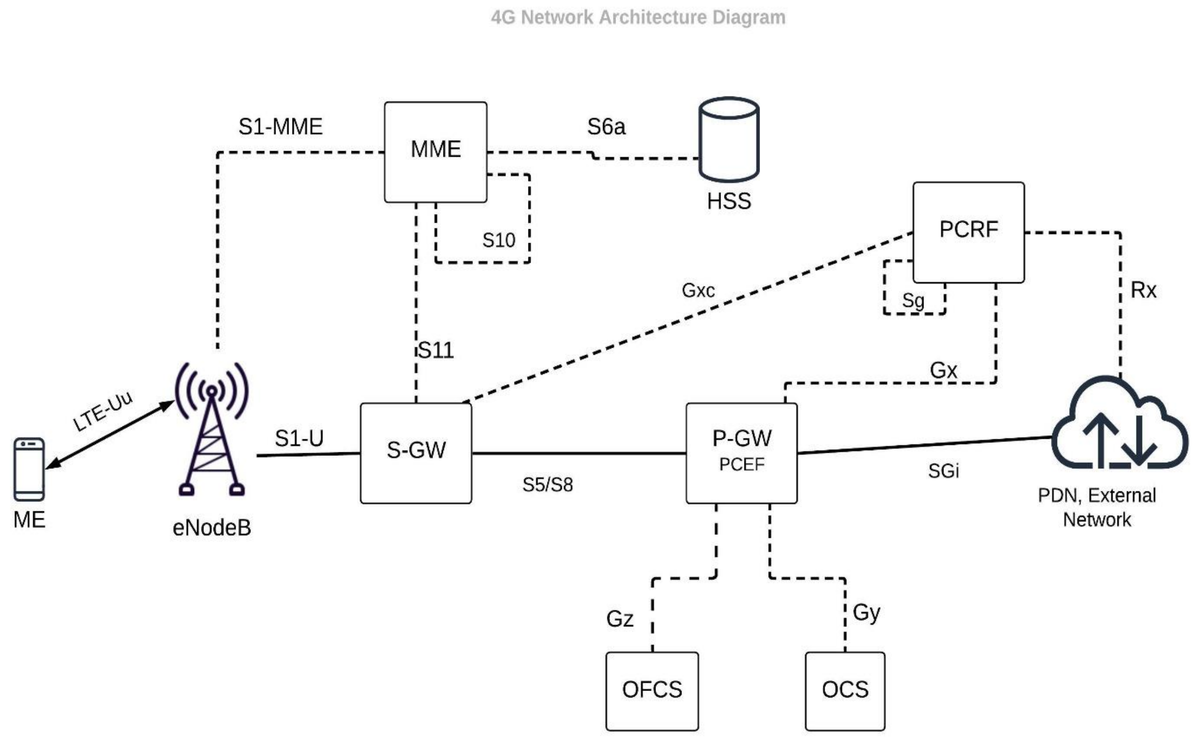

Fig 1 Architecture Overview of EPC with P-GW focus

The architectural overview of EPC with special focus on P-GW is shown in Fig 1.

Interfaces:

LTE-Uu: Radio Interface between UE and e-Node B; encompasses both control and user plane.

X2: point to point inter-eNode B interface and mainly used during handover; includes both control plane and user plane.

S1-MME: Reference point for the control plane protocol between E-UTRAN and MME; All control activities are performed over it, e.g. signalling for attachment, detachment, bearer establishment and modification, security procedures, etc. The protocol chosen for S1-MME is S1-AP, on top of SCTP.

S1-U: Reference point between E-UTRAN and Serving GW for the per bearer user plane tunnelling and inter eNodeB path switching during handover; uses GTP-U protocol.

S5: It provides user plane tunnelling and tunnel management between Serving GW and PDN GW. It is used for Serving GW relocation due to UE mobility and if the Serving GW needs to connect to a non-collocated PDN GW for the required PDN connectivity. It includes control and user planes. Two protocol variants are possible here, an evolved GPRS Tunnelling Protocol (GTP) and Proxy Mobile IP (PMIP).

S8: Inter-PLMN reference point providing user and control plane between the Serving GW in the VPLMN and the PDN GW in the HPLMN. S8 is the inter PLMN variant of S5.

S6a: It enables transfer of subscription and authentication data for authenticating /authorizing user access to the evolved system (AAA interface) between MME and HSS. It is based on the DIAMETER protocol.

S9: It provides transfer of (QoS) policy and charging control information between the Home PCRF and the Visited PCRF in order to support local breakout function.

S10: Reference point between MMEs for MME relocation and MME to MME information transfer. This reference point can be used intra-PLMN or inter-PLMN (e.g. in the case of Inter-PLMN HO). It is a pure control plane interface and an evolved GTP-C (GTP-C v2) protocol is used.

S11: Reference point for the control plane existing between MME and Serving GW; it employs the evolved GTP-C (GTP-C v2) protocol. The data bearer(s) between eNodeB and Serving GW are controlled via the concatenation of S1-MME and S11.

SGi: It is the reference point between the PDN GW and the packet data network. Here IETF based protocols for the user plane (i.e. IPv4 and IPv6 for packet forwarding) and control plane protocols like DHCP and RADIUS/DIAMETER for IP address/protocol configuration from external networks are employed.

Gx: the reference point for QoS policy, filter policy and charging control, between PCRF and PDN GW. It used to deliver filter and charging rules. The protocol used is DIAMETER.

Rx: defined between an Application Function (AF), located in a PDN, and PCRF for exchange of policy and charging information; it uses the DIAMETER protocol.

Gy interface connects PCEF to Online Charging System (OCS); uses DIAMETER protocol.

Gz interface is used in between PCEF and Charging Gateway Function (CGF).

Chapter 2 - Common Security Requirements

This section describes the common security requirements for P-GW.

Section 1: Access and Authorization

2.1.1 Management Protocols Mutual Authentication

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

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 P-GW management and maintenance.

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

Note: Any management protocol such as HTTP Over TLS 1.2 or later, IP Sec VPN are permitted. If TLS 1.2 is used, it should be patched up to date.

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

2.1.2 Management Traffic Protection

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

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

2.1.3 Role-Based access control

Requirement:
P-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.
P-GW shall support Role Based Access Control (RBAC) conforming to the globally accepted RBAC standard INCITS 359-2012(R2017), with minimum of 3 user roles , in particular, for OAM privilege management , for P-GW Management and Maintenance, including authorization of the operation for configuration data and software via the P-GW console interface.

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

2.1.4 User Authentication – Local/Remote

Requirement:

For remote user access , The various user accounts (other than system /admin accounts) on a system shall be protected from misuse. To this end, at least one authentication attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user in closed environment
Authentication attributes include
- Cryptographic keys
- Token
- Passwords

This means that authentication based on a parameter that can be spoofed is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker.

For remote user access , Minimum two of the above Authentication attributes shall be mandatorily combined to protect user accounts ((other than system /admin accounts) in open .environment (internet)

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

2.1.5 Remote login restrictions for privileged users

Requirement:

Login to eNodeB as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to eNodeB remotely i.e remote login access for root/admin/highest privileged users, by default shall be disabled permanently at the time of first installation.

This remote root user access restriction is also applicable to application software's / tools such as TeamViewer, desktop sharing which provide remote access to the eNodeB.
[Reference TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.6]

2.1.6 Authorization Policy

Requirement:
Only Role based authorization is permitted.
Bare minimum RBAC rights are to be assigned for the task to be performed.

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

2.1.7 Unambiguous identification of the user & group accounts removal
Requirement:
Users shall be identified unambiguously by the P-GW.
P-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.
P-GW shall also support assignment of specific ID for individual accounts per user as configured by administrator/root user. P-GW's all inactive users' accounts shall be locked / Disabled.

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

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

Section 2: Authentication Attribute Management

2.2.1 Authentication Policy

Requirement:

For local /Remote access , The various user accounts (other than system /admin accounts) on a PGW shall be protected from misuse. To this end, at least one authentication (Cryptographic keys or Token or Passwords) attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user in closed environment

For Local /Remote access, Minimum two of the Authentication attributes (Cryptographic Keys , Token , Passwords) shall be mandatorily combined to protect user accounts ((other than system /admin accounts) in open .environment (internet)

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.1.1]

2.2.2 Authentication Support – External

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

2.2.3 Protection against brute force and dictionary attacks

Requirement:
A protection against brute force and dictionary attacks that hinder authentication attribute guessing shall be implemented.
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.

In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by P-GW.

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

2.2.4 Enforce Strong Password

Requirement:
(a) The configuration setting shall be such that a P-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 P-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.
If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this sub-clause.
If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the P-GW.
When a user is changing a password or entering a new password, P-GW /central system checks and ensures that it meets the password requirements.
Password shall not be stored in clear text in the system; passwords shall be salted and hashed.

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

2.2.5 Inactive Session TimeouT

Requirement:
An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period ranging from 2 to 5 minutes.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.5.2]

2.2.6 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. P-GW shall support a configurable period for expiry of passwords.
Previously used passwords shall not be allowed upto a certain number (Password History).
The number of disallowed previously used passwords shall be:
□ Configurable;
□ Greater than 0;
□ And its minimum value shall be 3. This means that the P-GW shall store at least the three previously set passwords. The maximum number of passwords that the P-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.

This requirement shall be met either by P-GW itself or in combination with external authentication system.

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

2.2.7 Protected Authentication feedback

Requirement:

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

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

2.2.8 Removal of predefined or default authentication attributes

Requirement:
Predefined or default authentication attributes shall be deleted or disabled.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.2.3]

Section 3: Software Security

2.3.1 Secure Update

Requirement:

P-GW's system software updates shall be carried out strictly using the Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

P-GW shall allow updates only if code signing certificate is valid and not time expired.

Software update integrity shall be verified strictly using the Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

2.3.2 Secure Upgrade Requirement:

(i) P-GW Software package integrity shall be validated in the installation and upgrade stages strictly using the Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

(ii) P-GW shall allow upgrades only if code signing certificate is valid and not time expired. To this end, the P-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) Tampered software shall not be executed or installed if integrity check fails.

(iv) P-GW's software upgrades shall be carried out strictly using the Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

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

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

2.3.3 Source code security assurance

Requirement:
a) Vendor should follow best security practices including secure coding for software development and should be augmented with designated TSTL source code review duly supported by furnishing the Software Test Document (STD) generated while developing the P-GW.
b) Also, Vendor shall submit the undertaking as below:
(i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the P-GW Software which includes vendor developed code, third party software and open source code libraries used/embedded in the P-GW.
(ii)The P-GW software is free from all known security vulnerabilities, security weaknesses listed in the CVE and CWE databases as on the date of product release. Critical/severe, high and medium vulnerabilities based on CVSS (latest CWE database) for software weakness need to be patched during product release itself. For Low level vulnerabilities which are found during testing, vendor shall have remediation plan and patch them at the earliest

.

(iii) The binaries for P-GW and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

2.3.4 Known Malware and backdoor Check

Requirement:
Vendor shall submit an undertaking stating that P-GW is free from all known malware(CVE) and backdoors as on the date of product release and shall submit their internal Malware Test Document (MTD) of the P-GW to the designated TSTL.

2.3.5 No unused software
Requirement:
Software components / packages or parts of software packages which are not needed for operation or functionality of the P-GW shall not be present. Orphaned software components /packages shall not be present in P-GW.

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

2.3.6 Unnecessary Services Removal
Requirement:

P-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.

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

2.3.7 Restricting System Boot Source
Requirement:

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

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

2.3.8 Secure Time Synchronization
Requirement:

P-GW shall provide reliable time and date information provided manually by itself or through NTP/PTP server. P-GW shall establish secure communication channel with the NTP/PTP server.

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

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

2.3.9 Restricted reachability of services
Requirement:
The P-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.

2.3.10 Avoidance of Unspecified Wireless Access
Requirement:
An undertaking shall be given as follows: "The P-GW does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel"

2. 3.11. Disable Control + Alt +Del option Requirement: The P-GW Operating system may use option (Control + ALT +DEL) to forcibly to reboot, forcing the programs to stop. This feature may be misused by internal attackers. The same option shall be permanently disabled.

2.3.12. Disable USB stick detection Requirement: System shall restrict users from using USB stick to protect and secure data from stealing.

2.3.13. Lock Down Cron Jobs Requirement: Scheduling commands or tasks are called Cron Jobs. Cron Jobs are used for running scheduled backups, monitor disk space, and running system maintenance tasks. Running Cron Jobs should be restricted to specific users including administrator.

Section 4: System Secure Execution Environment

2.4.1 No unused functions

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

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

2.4.2 No unsupported components

Requirement:
Vendor to ensure that the P-GW shall not contain software and/or hardware components that are no longer supported by Vendor or its 3rd Parties including the open source communities, such as components that have reached end-of-life or end-of-support.

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

Section 5: User Audit

2.5.1 Audit trail storage and protection

Requirement: The security event log shall be access controlled using file access conditions such that only privilege users including the administrator have access to read the log files but not allowed to delete the log files.

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

2.5.2 Audit Event Generation

Requirement:
The P-GW shall log all important Security events with unique System Reference details as given in the Table below.
P-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
User Login including the Incorrect login attempts(Mandatory)	All use of Identification and authentication mechanism; Records any user login actions including the incorrect login attempts to the P-GW.	Username Source (IP address) if remote access Outcome of event (Success or failure) Date and Timestamp
Administrator access(Mandatory)	Records any access attempts to accounts that have system privileges.	Username, Date and Timestamp, Command given, Length of session, Outcome of event (Success or failure) Source (IP address) if remote access
Account administration(Mandatory)	Records all account administration activity, i.e. configure, delete, copy, enable, and disable along with the commands used for these activities	Administrator username, Administered account, Activity performed (configure, delete, enable and disable) Outcome of event (Success or failure) Date and Timestamp
Resource Usage (Mandatory)	Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period have exceeded their defined thresholds.	Value exceeded, Value reached (Here suitable threshold values shall be defined depending on the individual system.) Outcome of event (Threshold Exceeded) Date and Timestamp
Configuration change(Mandatory)	Changes to configuration of the network device	Change made Date and 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	Action performed (boot, reboot, shutdown, etc.) Username (for intentional actions)

	the network device has crashed.	Outcome of event (Success or failure)
		Date and Timestamp
Interface status change(Mandatory)	Change to the status of interfaces on the network device (e.g. shutdown)	Interface name and type
		Status (shutdown, down missing link, etc.)
		Outcome of event (Success or failure)
		Date and 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)
		Date and 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)
		Date and Timestamp
Services (Optional)	Starting and Stopping of Services (if applicable)	Service identity
		Activity performed (start, stop, etc.)
		Date and Timestamp
		Outcome of event (Success or failure)
X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Date and 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
		Date and Timestamp
		Outcome of event (Success or failure)
		Activity performed
Time change(Mandatory)	Change in time settings	old value of time
		new value of time
		Date and 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)
		Date and 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	Date and Timestamp
		Initiator identity (as applicable)
		Target identity (as applicable)
		User identity (in case of Remote administrator access)
		Type of event
		Outcome of event (Success or failure, as applicable)
Access to personal data (Mandatory)	All use of identification and authentication mechanism	user identity
		origin of attempt (e.g.IP address)
		Date and Timestamp
		Personal data in encrypted text(Optional)
		Outcome of event (Success or failure)
Audit data changes(Optional)	Changes to audit data including deletion of audit data	Date and Timestamp
		Type of event (audit data deletion, audit data modification)
		Outcome of event (Success or failure)
		Subject identity
		user identity
		origin of attempt to change time (e.g.IP address)
		Details of data deleted or modified

2.5.3 Secure Log Export

Requirement:
(I) (a) The P-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 P-GW.
(II) P-GW shall be able to store the generated audit data itself may be with limitations.
(III)P-GW shall alert administrator when its security log buffer reaches configured threshold limit.

(IV) In the absence of External system, P-GW shall stop its services when its own security event log buffer is full.

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

Section 6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirements:
P-GW shall Communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

Vendor shall submit to TSTL, the list of the connected entities with P-GW and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration and detailed procedure of establishing the communication with each entity.

2.6.2 Cryptographic Module Security Assurance

Requirement:

Cryptographic module embedded inside the P-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 Level 2.
Vendor shall also submit cryptographic module implementation testing document and the test results to designated TSTL for scrutiny.

2.6.3. Cryptographic Algorithms implementation Security Assurance

Requirement:

Cryptographic algorithms embedded in the crypto module of P-GW are implemented in compliance with respective FIPS standards (for the specific crypto algorithm.)
Vendor shall also submit cryptographic algorithm implementation testing document and the test results to designated TSTL for scrutiny.

2.6.4. Protecting data and information – Confidential System Internal Data

Requirement:

When P-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 text to users and administrators.
Access to maintenance mode shall be restricted only to authorised privileged user.

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

2.6.5. Protecting data and information in storage

Requirement:

For sensitive data (persistent or temporary), read access rights shall be restricted. Files of P-GW system that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” with appropriate non-repudiation controls.

In addition, the following rules apply for:

(i)Systems that need access to identification and authentication data in the clear/readable form e.g. in order to perform an activity/operation. Such systems shall not store this data in the clear/readable form, but scramble or encrypt it by implementation-specific means.
(ii)Systems that do not need access to sensitive data in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” only.
(iii)Stored files in the P-GW: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” only.

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

2.6.6 Protection against Copy of Data

Requirement:

P-GW shall not create a copy of data in use and/or data in transit.

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

2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement**:**

P-GW shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit. Establishment of outbound overt channels shall not be allowed if they are initiated by / originated automatically from the P-GW.

---

2. 6.8 Protection against Data Exfiltration - Covert Channel

Requirement:

P-GW shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.

Establishment of outbound covert channels and tunnels shall not be allowed if they are initiated by / originated automatically from the P-GW i.e the P-GW shall not have a session or process established/initiated without a configured user or a system user.

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

Section 7: Network Services

2.7.1: Traffic Filtering – Network Level Requirement: P-GW shall provide a mechanism to filter incoming IP packets on any IP interface.
(i) To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of the stack ISO/OSI.
(ii) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:

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

-Accept: the matching message is accepted.

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

This feature is useful to monitor traffic before its blocking.

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

(iv) To filter on the basis of the value(s) of any portion of the protocol header.

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

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

2.7.2: Traffic Separation

Requirement:

P-GW shall support physical and/or logical separation of management traffic and control plane traffic. See RFC 3871 for further information.

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

2.7.3: Traffic Protection –Anti-Spoofing: P-GW shall not process IP Packets if their source address is not reachable via the incoming interface.

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

Section 8: Attack Prevention Mechanisms

2.8.1 Network Level and application level DDoS

Requirement: P-GW shall have protection mechanism against network level and Application level DDoS attacks, supported by it self or supported in tandem by external firewall device.

P-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 include, but not limited to the following:
- Restricting of available RAM per application
- Restricting of maximum sessions for a Web application
- Defining the maximum size of a dataset
- Restricting CPU resources per process
- Prioritizing processes
- Limiting of amount or size of transactions of an user or from an IP address in a specific time range
- Limiting of amount or size of transactions to an IP address/Port Address in a specific time range

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

2. 8.2 Excessive Overload Protection
Requirement:

P-GW shall act in a predictable way if an overload situation cannot be prevented. P-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 P-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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.2.3.3.3]

Section 9: Vulnerability Testing Requirements

2.9.1 Fuzzing – Network and Application Level

Requirement:

P-GW shall respond with error messages , anomalous responses, Crash responses when receiving unexpected input request /Malformed input requests

Vendor should document the list of Protocol stacks supported by P-GW for all traffic planes (Management ,Control , Data plane and Service /Application plane)

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

2.9.2 Port Scanning

Requirement:

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

Any attempt to scan the network interface shall lead to triggering of logging of the appropriate parameters like Date & Time stamp, Source IP address, destination Port address etc.

The test for this requirement can be verified by using a suitable port scanning tool.

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

2.9.3 Vulnerability Scanning

Requirement:
It shall be ensured that there are no known vulnerabilities exist in the P-GW at the date of product release.

The purpose of vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans in place to mitigate them) on the P-GW that can be detected by means of automatic testing tools. The test for this requirement can be verified by using a suitable Vulnerability scanning tool.

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

Section 10: Operating System

2.10.1 Growing Content Handling

Requirements:

Growing or dynamic content 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 P-GW from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided.

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

2.10.2 Handling of ICMP

Requirement:

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

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

2.10.3 Authenticated Privilege Escalation only

Requirement:

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

2.10.4 System account identification

Requirement:

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

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

2.10.5 OS Hardening

Requirement:

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

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

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

2.10.6 No automatic launch of removable media

Requirement:

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

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

2.10.7 Protection from buffer overflows

Requirement:

P-GW shall support mechanisms for buffer overflow protection.

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

2.10.8 External file system mount restrictions

Requirement:

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in P-GW in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

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

2.10.9 File-system Authorization privileges

Requirement:

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

Section 11: Web Servers

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

2.11.1 HTTPS

Requirement:

The communication between Web client and Web server shall be protected strictly using the Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” only.

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

2.11.2 Webserver logging

Requirement:

Access to the P-GW webserver (for both successful as well as failed attempts) shall be logged by P-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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.2.1]

2.11.3 HTTPS input validation

Requirement:

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

2.11.4 No system privileges

Requirement:

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

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

2.11.5 No unused HTTPS methods

Requirement:

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

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

2.11.6 No unused add-ons

Requirement:

All optional add-ons and components of the web server shall be deactivated if they are not required for P-GW operation.
In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.

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

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

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

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

2.11.8 No CGI or other scripting for uploads

Requirement:

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

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

2.11.9 No execution of system commands with SSI

Requirement:

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

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

2.11.10 Access rights for web server configuration

Requirement:

Access rights for P-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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.8]

2.11.11 No default content

Requirement:

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

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

2.11.12 No directory listings

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

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

2.11.13 Web server information in HTTPS headers

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

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

2.11.14 Web server information in error pages

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

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

2.11.15 Minimized file type mappings

Requirement:

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

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

2.11.16 Restricted file access

Requirement:

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

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

2.11.17 Execute rights exclusive for CGI/Scripting directory

Requirement:

If CGI or other scripting technology is used, only the CGI/Scripting directory is configured with execute rights. Other directories used or meant for web content do not have execute rights.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.15]

Section 12: Other Security requirements

2.12.1 No System Password Recovery

Requirement:

In the event of P-GW system password reset with appropriate authentication and access control, the entire configuration of the P-GW shall be irretrievably deleted.

2.12.3 Secure System Software Revocation

Requirement:

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

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

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

2.12.4 Software Integrity Check –Installation

Requirement:

P-GW shall validate the software package integrity before the installation/upgrade stage strictly using the Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” only .

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

2.12.5 Software Integrity Check – Boot

Requirement:

The P-GW shall verify the integrity of a software component by comparing the result of a measurement of the component , typically a standard cryptographic hash generated strictly using the Secure cryptographic controls prescribed in Table1 of the document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" to the expected reference value.

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

2.12. 6 Unused Physical and Logical Interfaces Disabling

Requirement:

P-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.

2.12.7 No Default Profile

Requirement:

Predefined or default user accounts in P-GW shall be deleted or disabled.

2.12.8 Security Algorithm Modification

Requirement:

It shall not be possible to modify security algorithms supported by P-GW through unauthorized access, e.g. to perform a downgrade attack by deceiving the nodes to use a weaker algorithm.

Chapter 3 P-GW Specific Security requirements

Section 1: Generic Requirements

3.1.1 The OEM shall undertake that the hardware /software/firmware over which P-GW application is running shall be free of known weakness/vulnerability at the date of product release and the patch if any used for fixing the security vulnerabilities in these shall be as per clause 2.3.3 b(ii).

3.1.2 Core Network Security: All EPC nodes shall exist in the same security domain. If any nodes of the core are in different security domains, then the traffic between them shall be passed through a Security Gateway (SEG) using IPsec for encryption and Integrity Protection.

3.1.3 Roaming, 3rd party applications and Inter-operator Connectivity: The IP traffic, both control plane and user plane, meant for national and international roaming, 3rd party applications, inter operator connectivity shall be routed through SEG using IPsec for encryption and Integrity Protection.

Section 2. Threats specific to P-GW

3.2.1 Threats related to IP Address Allocation- IP Address Reallocation Continuously: If an IP address is reallocated to a UE immediately after released from another UE, then the network side might be mistaken that the same UE keeps using the IP address continuously. Consequently, some network functions (e.g. PCRF) will execute policies on the wrong target UE. And some mis-operations (e.g mis-charging) will be executed on UEs.

3.2.2 Packet Forwarding -Sending unauthorized packets to other UEs: If the destination address of uplink packets sent by a UE is other UE in the same PGW, the packets will not pass through the PGW and will be forwarded directly to the target UE. In this case mutual access between two UEs within the same PGW might be requested. If such access is enabled, an attacker can gain control a UE to send malicious packets (e.g. fraudulent information, malicious trojans, virus packs, etc.) directly to other UEs without security measures (e.g. firewall) at network side.

3.2.3 Emergency PDN Connection- Inactive Emergency PDN Connection Release: The PGW is expected to release all bearers corresponding to emergency inactive PDN connections after the configured timeout. If emergency bearers of inactive PDN connections are not released, it may lead to system resource exhaustion.

Section 3: Security Requirements specific to P-GW

The following security requirements are specific to P-GW:

3.3.1 Per-user based packet filtering: The PGW shall filter the packets per- user (deep packet inspection) according to the configured filtering policy.

[Reference: TSDSI STD T1.3GPP 33.250-14.0.0 V.1.0.0 Section 4.2.2.2]

3.3.2 Charging ID Uniqueness: Every IP-CAN bearer shall be assigned a unique identity number for billing purposes. (i.e. the Charging Id).

[Reference: TSDSI STD T1.3GPP 33.250-14.0.0 V.1.0.0 Section 4.2.2.3]

3.3.3 TEID Uniqueness: TEID generated for each new GTP tunnel shall be unique for both control and user plane.

[Reference: TSDSI STD T1.3GPP 33.250-14.0.0 V.1.0.0 Section 4.2.2.4]

3.3.4 Inactive emergency PDN connection release: P-GW shall initiate the deactivation of all bearers of the emergency PDN connection when it is inactive (i.e. not transferring any packets) for a configured period of time.

[Reference: TSDSI STD T1.3GPP 33.250-14.0.0 V.1.0.0 Section 4.2.2.6]

3.3.5 Unpredictable GTP TEID: The TEID created for usage in the GTP-C messages as well as in the GTP-U messages shall be unpredictable in order to prevent a hacker to inject GTP-U packets with a spoofed TEID into a user’s session (causing e.g. overbilling problems) or to send malicious GTP-C messages to delete an established session (and causing a DoS).

[Reference: TSDSI STD T1.3GPP 33.250-14.0.0 V.1.0.0 Section 4.2.3.5.1]

3.3.6 IP Address reallocation interval: The PGW shall support a mechanism to set an interval between an IP address reallocation.

[Reference: TSDSI STD T1.3GPP 33.250-14.0.0 V.1.0.0 Section 4.2.6.3]

3.3.7 MS/UE-Mutual Access Prevention: The PGW shall support a mechanism to prevent MS/UE-mutual access attacks (e.g. configure a filtering rule to drop all mutual access packets).

[Reference: TSDSI STD T1.3GPP 33.250-14.0.0 V.1.0.0 Section 4.2.6.4]

3.3.8 Traffic Separation: The PGW shall support physical or logical separation of O&M and control plane traffic, O&M and user plane traffic, control plane and user plane traffic respectively.

[Reference: TSDSI STD T1.3GPP 33.250-14.0.0 V.1.0.0 Section 4.3.5.1]

3.3.9 User Plane Traffic Differentiation: The PGW 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). This shall be applicable when EPS support simultaneous exchange of IP traffic to multiple PDNs through the use of separate PDN GWs or single PDN GW.

[Reference: TSDSI STD T1.3GPP 33.250-14.0.0 V.1.0.0 Section 4.3.5.2]

APPENDIX A

List of Undertakings/Submission

1. Source Code Security Assurance (against test case 2.3.3)
2. Known Malware and backdoor Check (against test case 2.3.4)
3. Avoidance of Unspecified Wireless Access (against test case 2.3.10)
4. Cryptographic Based Secure Communication (against test case 2.6.1)
5. Cryptographic Module Security Assurance (against test case2.6.2)
6. Cryptographic Algorithms implementation Security Assurance (against test case 2.6.3)
7. Hardware/Software/firmware - Absence of known vulnerability/security weakness (against test case 3.1.1)