ETSI TS 133 250 V15.1.0 (2019-10)

LTE;
Security assurance specification
for the PGW network product class
(3GPP TS 33.250 version 15.1.0 Release 15)

Reference
RTS/TSGS-0333250vf10

Keywords
LTE,SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document contains requirements and test cases that are specific to the PGW network product class. It refers to the Catalogue of General Security Assurance Requirements and formulates specific adaptions of the requirements and test cases given there, as well as specifying requirements and test cases unique to the PGW network product class.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 41.001: "GSM Release specifications".

[3] 3GPP TS 33.117: "Catalogue of General Security Assurance Requirements".

[4] 3GPP TR 33.916: "Security assurance scheme for 3GPP network products for 3GPP network product classes".

[5] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[6] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[7] 3GPP TS 33.102: "3G security; Security architecture".

[8] 3GPP TS 32.251: "Telecommunication management; Charging management; Packet Switched (PS) domain charging".

[9] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[10] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[11] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

4 PGW-specific security requirements and related test cases

4.1 Introduction

The structure of the present document is aligned with TS 33.117[3] such that the PGW-specific adaptation of a generic requirement in 33.117[3], clause 4, can be always found in clause 4 of present document.

The text on pre-requisites for testing in clause 4.1.2 of TS 33.117 [3] applies also to the present document.

4.2 PGW-specific security functional adaptations of requirements and related test cases

4.2.1 Introduction

4.2.2 Security functional requirements on the PGW deriving from 3GPP specifications and related test cases

4.2.2.1 Security functional requirements on the PGW deriving from 3GPP specifications – General approach

In addition to the requirements and test cases in TS 33.117[3], clause 4.2.2, a PGW shall satisfy the following:

It is assumed for the purpose of the present SCAS that a PGW conforms to all mandatory security-related provisions pertaining to a PGW in:

- 3GPP TS 33.401[5]: "EPS security architecture";
- other 3GPP specifications that make reference to TS 33.401[5] or are referred to from TS 33.401[5] (e.g. TS 23.401 [6], TS 23.060[9], etc.);
- 3GPP TS 32.251[8]: " Packet Switched (PS) domain charging".

Since the PDN GW is the gateway which terminates the SGi interface, the security procedures pertaining to the PGW are typically related to gateway functions. For example:

- Per-user based packet filtering (by e.g. deep packet inspection).
- Every IP-CAN bearer shall be assigned a unique identity number for billing purposes. (i.e. the Charging Id).
- The TEID is a unique identifier within one IP address of a logical node.

4.2.2.2 Per-user based packet filtering

Requirement Name: Per-user based packet filtering

Requirement Reference: TS 23.401 [6], clause 4.4.3.3

Requirement Description: This requirement is identical to per-user based packet filtering (by e.g. deep packet inspection) as specified in TS 23.401, clause 4.4.3.3.

Threat References: TR 33.926 [10], clause B.2.3.1 Failure to assign unique TEID or Charging ID for a session.

Test Case:

Purpose:

Verify that PGW supports a Per-user based packet filtering.

Pre-Conditions:

- The tester has a privilege to configure the filtering policy on the PGW to make the PGW can filter the packets per-user
- Some UE (e.g. UE1 and UE2) are registered on the PGW.
- The PGW can receive the packets from the UE1 and UE2.
- A network traffic analyser on the PGW (e.g. tcpdump) is available.

Execution Steps

1) The tester configures the different filtering policy for the UE1and the UE2 on the PGW, e.g. the PGW forwards the packets from the UE1 to SGi and drops the packets from the UE2.
2) The tester sends the packets from the UE1 to the PGW.
3) The tester sends the packets from the UE2 to the PGW.
4) The tester checks the filtered packets using the network traffic analyser.

Expected Results:

The PGW can filter the packets per- user according the configured filtering policy, e.g. the PGW forwards the packets from the UE1 to SGi in the step 2 and drops the packets from the UE2 in the step 3.

Expected format of evidence:

Evidence suitable for the interface, e.g. screenshot contains the operation results, pcap file demonstrating that the UE2's packets are correctly received but unavailable on the SGi interface while the UE1's packets are correctly sent to SGi.

4.2.2.3 Charging ID Uniqueness

Requirement Name: Charging ID Uniqueness

Requirement Reference: TS 32.251 [8], clause 5.1.1

Requirement Description: "Every IP-CAN bearer shall be assigned a unique identity number for billing purposes. (i.e. the Charging Id)" as specified in 3GPP TS 32.251 [8], clause 5.1.1.

Note: A charging ID is not assigned to more than one active IP-CAN bearers at the same time. The reuse of Charging ID is possible after an IP-CAN session has been terminated and the Charging ID related to this IP-CAN session has been released.

Threat References: TR 33.926 [10], clause B.2.5.1 Failure to assign unique TEID or Charging ID for a session

Test Case:

Purpose:

Verify that the Charging ID value set in the Information Element Bearer Context within a CreateSessionResponse is unique.

Pre-Conditions:

Test environment with P-GW and S-GW, PCRF. PCRF and S-GW may be real nodes or simulated.

The tester is able to trace traffic between the P-GW and the S-GW (real or simulated)

Execution Step

1) The tester intercepts the traffic between the P-GW and the S-GW.
2) The tester trigger more than one (e.g. at least 10000) consecutive CreateSessionRequest for an Initial UE Attach towards the P-GW (using a real or a simulated S-GW) in order to setup a new IP-CAN bearer.
3) The P-GW creates a UE/S-GW context and communicates with the PCRF (real or simulated) for QOS and APN resolve. That procedures shall be successfully in order to permit to the P-GW to send back to the S-GW a CreateSessionResponse containing at least :
   a) A Success cause.
   b) The P-GW's F-TEID for control plane
   c) The PDN Address Allocation (PAA)
   d) A Bearer Contexts Created.
4) The tester verifies that the Charging ID within Bearer Contexts Created in each generated CreateSessionResponse are different.

Expected Results:

The Charging ID assigned to every IP-CAN bearer requested by different CreateSessionRequest is unique.

Expected format of evidence:

Files containing the triggered GTP messages (e.g. pcap trace).

4.2.2.4 TEID UNIQUENESS

Requirement Name: TEID Uniqueness

Requirement Reference: TS 23.060 [9], clause 14.6

Requirement Description: "The TEID is a unique identifier within one IP address of a logical node." as specified in TS 23.060 [9], clause 14.6.

Note: 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.

Threat References: TR 33.926 [10], clause B.2.5.1 Failure to assign unique TEID or Charging ID for a session

Test Case:

Purpose:

Verify that the TEID generated for each new GTP tunnel is unique for both control and user plane.

Pre-Conditions:

Test environment with P-GW and S-GW, PCRF. PCRF and S-GW may be real nodes or simulated.

The tester is able to trace traffic between the P-GW and the S-GW (real or simulated)

Execution Step

1) The tester intercepts the traffic between the P-GW and the S-GW.

2) The tester triggers more than one (e.g. at least 10000) consecutives CreateSessionRequest e.g. for an Initial UE Attach towards the P-GW (using a real or a simulated S-GW) with GTP header TEID set to 0 and F-TEID set to different values.

3) The P-GW creates a UE/S-GW context and communicates with the PCRF (real or simulated) for QOS and APN resolve. That procedures shall be successfully in order to permit to the P-GW to send back to the S-GW a CreateSessionResponse containing at least :

   a) A Success cause.

   b) The P-GW's F-TEID for control plane

   c) The PDN Address Allocation (PAA).

   d) A Bearer Contexts Created.

4) The tester verifies that the F-TEID created for each generated CreateSessionResponse is unique.

Expected Results:

The F-TEID set into each different CreateSessionResponse is unique.

Expected format of evidence:

Files containing the triggered GTP messages (e.g. pcap trace).

4.2.2.5 Mobility binding

Requirement Name: MN-HA authentication extension validation for mobility binding during trusted non-3GPP access

Requirement Reference: TS 33.402 [11], clause 9.2.1.1

Requirement Description: "The PDN-GW shall validate the MN-HA authentication extension" as specified in TS 33.402, clause 9.2.1.1.

Threat References: TBA

Test Case:

Test Name: TC_PGW_MIP-AUTH_Non-3GPP

Purpose: To test whether the PGW validates the MN-HA authentication extension correctly.

Pre-Condition:

The UE and PGW are connected in the test environment. UE is simulated.

The tester has access to the S6b interface between the 3GPP AAA Server and the PDN GW.

The tester has access to the MIPv4 FACoA based S2a interface between the PGW and UE.

Execution Steps:

The PGW (home agent for the UE) is active in a 3GPP access network.

The tester captures packets over S6b and S2a interfaces using any packet analyser.

The tester filters the MN-HA Key transported in the authentication and authorization information from the 3GPP AAA server to PGW over S6b interface.

The UE sends a Registration Request message to PGW via the trusted non-3GPP IP access network.

The tester filters the Registration Request sent by UE to PGW and Registration Reply sent by PGW to UE over the S2a interface.