ETSI TS 133 513 V17.2.0 (2023-07)

5G;
5G Security Assurance Specification (SCAS);
User Plane Function (UPF)
(3GPP TS 33.513 version 17.2.0 Release 17)

Reference
RTS/TSGS-0333513vh20

Keywords
5G

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

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 https://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

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 4
1 Scope 6
2 References 6
3 Definitions of terms, symbols and abbreviations 6
3.1 Terms 6
3.2 Symbols 6
3.3 Abbreviations 7
4 UPF-specific security requirements and related test cases 7
4.1 Introduction 7
4.2 UPF-specific security functional requirements and related test cases 7
4.2.1 Introduction 7
4.2.2 Security functional requirements on the UPF deriving from 3GPP specifications and related test cases 7
4.2.2.0 General 7
4.2.2.1 Confidentiality protection of user data transported over N3 interface. 7
4.2.2.2 Integrity protection of user data transported over N3 interface 8
4.2.2.3 Replay protection of user data transported over N3 interface 9
4.2.2.4 Protection of user data transported over N9 interface Within a PLMN 9
4.2.2.5 Signalling Data Protection 10
4.2.2.6 TEID uniqueness 11
4.2.2.7 IPUPS 12
4.2.2.8 Protection against malformed GTP-U messages 13
4.2.3 Technical baseline 13
4.2.3.1 Introduction 13
4.2.3.2 Protecting data and information 13
4.2.3.2.1 Protecting data and information – general 13
4.2.3.2.2 Protecting data and information – unauthorized viewing 14
4.2.3.2.3 Protecting data and information in storage 14
4.2.3.2.4 Protecting data and information in transfer 14
4.2.3.2.5 Logging access to personal data 14
4.2.3.3 Protecting availability and integrity 14
4.2.3.4 Authentication and authorization 14
4.2.3.5 Protecting sessions 14
4.2.3.6 Logging 14
4.2.4 Operating systems 14
4.2.5 Web Servers 14
4.2.6 Network Devices 14
4.3 UPF-specific adaptations of hardening requirements and related test cases 14
4.3.1 Introduction 14
4.3.2 Technical baseline 14
4.3.3 Operating systems 15
4.3.4 Web servers 15
4.3.5 Network devices 15
4.3.6 Network functions in service-based architecture 15
4.4 UPF-specific adaptations of basic vulnerability testing requirements and related test cases 15
Annex A (informative): Change history 16
History 17

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.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document contains requirements and test cases that are specific to the UPF network product class. It refers to the Catalogue of General Security Assurance Requirements and formulates specific adaptions of the requirements and test cases. It also specifies the requirements and test cases unique to the UPF 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 TS 33.501 (Release 15): "Security architecture and procedures for 5G system".

[3] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[4] 3GPP TS 23.501: "System Architecture for 5G system".

[5] 3GPP TS 29.281: "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U) ".

[6] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[7] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[8] 3GPP TS 33.501 (Release 16): "Security architecture and procedures for 5G system".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

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 Symbols

Void.

3.3 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].

Void.

4 UPF-specific security requirements and related test cases

4.1 Introduction

The present document describes the following security requirements and the related test cases for UPF:

- Security functional requirements and the related test cases (clause 4.2),
- Adaptations of hardening requirements and the related test cases (clause 4.3), and
- Adaptations of basic vulnerability testing requirements and the related test cases (clause 4.4).

The above categories are aligned with those specified in TS 33.117 [3]. 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 UPF-specific security functional requirements and related test cases

4.2.1 Introduction

The security functional requirements and the related test cases specific for UPF are described in the clause.

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

4.2.2.0 General

The general approach in TS 33.117 [3] clause 4.2.2.1 apply to the UPF network product class. The requirements and test cases in TS 33.117 [3] clause 4.2.2.2 related to SBA/SBI aspect are not applicable.

4.2.2.1 Confidentiality protection of user data transported over N3 interface.

Requirement Name: Confidentiality protection of user data transported over N3 interface.

Requirement Reference: TS 33.501 [2], Clause 9.3

Requirement Description: "The transported user data between gNB and UPF shall be confidentiality protected." As specified in TS 33.501 [2], clause 9.3.

Threat Reference: TR 33.926 [7], Clause L.2.2, "No protection or weak protection for user plane data ".

TEST CASE:

Test Name: TC_UP_DATA_CONF_UPF

Purpose:

Verify that the transported user data between gNB and UPF are confidentiality protected over N3 interface.

Procedure and execution steps:

Pre-Condition:

- UPF network product is connected in simulated/real network environment.
- The tunnel mode IPsec ESP and IKE certificate authentication is implemented.
- Tester shall have knowledge of the security parameters of tunnel for decrypting the ESP packets.
- Tester shall have access to the N3 interface between gNB and UPF.
- Tester shall have knowledge of the confidentiality algorithm and confidentiality protection keys used for encrypting the encapsulated payload.

Execution Steps:

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [3].

Expected Results:

The user data transported between gNB and UPF is confidentiality protected.

Expected format of evidence:

Evidence suitable for the interface, e.g., evidence can be presented in the form of screenshot/screen-capture.

4.2.2.2 Integrity protection of user data transported over N3 interface

Requirement Name: Integrity protection of user data transported over N3 interface.

Requirement Reference: TS 33.501 [2], Clause 9.3

Requirement Description: "The transported user data between gNB and UPF shall be integrity protected" as specified in TS 33.501 [2], clause 9.3.

Threat Reference: TR 33.926 [7], Clause L.2.2, "No protection or weak protection for user plane data"

TEST CASE:

Test Name: TC_UP_DATA_INT_UPF

Purpose:

Verify that the transported user data between gNB and UPF are integrity protected over N3 interface.

Procedure and execution steps:

Pre-Condition:

- UPF network product is connected in simulated/real network environment.
- The tunnel mode IPsec ESP and IKE certificate authentication is implemented.
- Tester shall have knowledge of the security parameters of tunnel for decrypting the Encapsulated Security Payload (ESP) packets.
- Tester shall have knowledge of the authentication algorithm (Hash Message Authentication Code) and the protection keys.

Execution Steps:

The requirement mentioned in this clause is tested in accordance to the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [3].

Expected Results:

The user data transported between gNB and UPF is integrity protected.

Expected format of evidence:

Evidence suitable for the interface, e.g., evidence can be presented in the form of screenshot/screen-capture.

4.2.2.3 Replay protection of user data transported over N3 interface

Requirement Name: Replay protection of user data transported over N3 interface

Requirement Reference: TS 33.501 [2], Clause 9.3

Requirement Description: "The transported user data between gNB and UPF shall be replay protected." As specified in TS 33.501, clause 9.3.

Threat Reference: TR 33.926 [7], Clause L.2.2, "No protection or weak protection for user plane data"

TEST CASE:

Test Name: TC_UP_DATA_REPLAY_UPF

Purpose:

Verify that the transported user data between gNB and UPF are replay protected.

Procedure and execution steps:

The following procedure is executed if UPF supports IPsec.

Pre-Condition:

- UPF network product is connected in simulated/real network environment.
- The tunnel mode IPsec ESP and IKE certificate authentication is implemented.
- Tester shall have knowledge of the security parameters of tunnel for decrypting the ESP packets.
- Tester shall have access to the original user data transported via N3 reference point between gNB and UPF.

Execution Steps:

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [3].

Expected Results:

The user data transported between UE and UPF is replay protected.

Expected format of evidence:

Evidence suitable for the interface, e.g., evidence can be presented in the form of screenshot/screen-capture.

4.2.2.4 Protection of user data transported over N9 interface Within a PLMN

Requirement Name: Protection of user data transported over N9 within a PLMN.

Requirement Reference: TS 33.501 [2], Clause 9.9