ETSI TS 133 513 V16.3.0 (2023-07)

5G;
5G Security Assurance Specification (SCAS);
User Plane Function (UPF)
(3GPP TS 33.513 version 16.3.0 Release 16)

Reference
RTS/TSGS-0333513vg30

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 6
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
4.2.3 Technical baseline 12
4.2.3.1 Introduction 12
4.2.3.2 Protecting data and information 12
4.2.3.2.1 Protecting data and information – general 12
4.2.3.2.2 Protecting data and information – unauthorized viewing 12
4.2.3.2.3 Protecting data and information in storage 12
4.2.3.2.4 Protecting data and information in transfer 12
4.2.3.2.5 Logging access to personal data 12
4.2.3.3 Protecting availability and integrity 12
4.2.3.4 Authentication and authorization 12
4.2.3.5 Protecting sessions 12
4.2.3.6 Logging 12
4.2.4 Operating systems 12
4.2.5 Web Servers 12
4.2.6 Network Devices 12
4.3 UPF-specific adaptations of hardening requirements and related test cases 13
4.3.1 Introduction 13
4.3.2 Technical baseline 13
4.3.3 Operating systems 13
4.3.4 Web servers 13
4.3.5 Network devices 13
4.3.6 Network functions in service-based architecture 13
4.4 UPF-specific adaptations of basic vulnerability testing requirements and related test cases 13
Annex A (informative): Change history 14
History 15

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".

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 9.3

Requirement Description: As specified in clause 9.9 in TS 33.501 [2], "Interfaces internal to the 5G Core can be used to transport signalling data as well as privacy sensitive material, such as user and subscription data, or other parameters, such as security keys. Therefore, confidentiality and integrity protection is required.

For the protection of the non-SBA internal interfaces, such as N4 and N9, NDS/IP shall be used as specified in [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_N9

Purpose:

Verify that the protection mechanism implemented for user data transport over N9 interface in a PLMN conforms to the selected security profile.

Procedure and execution steps:

Pre-Condition:

- UPF network products are 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 N9 interface between two UPFs within a PLMN.
- 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 on N9 within a PLMN is protected.

Expected format of evidence:

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

4.2.2.5 Signalling Data Protection

Requirement Name: Protection of signalling data transported over N4 interface.

Requirement Reference: TS 33.501 [2], Clause 9.9

Requirement Description: As specified in clause 9.9 in TS 33.501 [2], "Interfaces internal to the 5G Core can be used to transport signalling data as well as privacy sensitive material, such as user and subscription data, or other parameters, such as security keys. Therefore, confidentiality and integrity protection is required.

For the protection of the non-SBA internal interfaces, such as N4 and N9, NDS/IP shall be used as specified in [3]."

Threat Reference: TR 33.926 [7], Clause L.2.3, "No protection or weak protection for signalling data over N4 interface"

TEST CASE:

Test Name: TC_CP_DATA_CONF _UPF_N4

Purpose:

Verify that the protection mechanism implemented for signalling data transmitted over N4 conforms to selected security profile.

Procedure and execution steps:

Pre-Condition:

- UPF and SMF network products are 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 N4 interface between SMF 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 signalling data transported over N4 interface is protected.

Expected format of evidence:

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

4.2.2.6 TEID uniqueness

Requirement Name: TEID uniqueness.

Requirement Reference:

TS 23.501 [4], Clause 5.8.2.3.1; TS 29.281 [5], Clause 5.1; TS 23.060 [6], Clause 14.6

Requirement Description:

"Allocation and release of CN Tunnel Info is performed when a new PDU Session is established or released. This functionality is supported either by SMF or UPF, based on operator's configuration on the SMF" as specified in TS 23.501[4], clause 5.8.2.3.1.

"Tunnel Endpoint Identifier (TEID): This field unambiguously identifies a tunnel endpoint in the receiving GTP U protocol entity. The receiving end side of a GTP tunnel locally assigns the TEID value the transmitting side has to use" as specified in TS 29.281[5], clause 5.1.

"The TEID is a unique identifier within one IP address of a logical node." As specified in TS 23.060 [6], clause 14.6.

Threat Reference: TR 33.926 [7], Clause L.2.4, "Failure to assign unique TEID for a session"

TEST CASE:

Test Name: TC_TEID_ID_UNIQUENESS_UPF

Purpose:

Verify that the TEID generated by UPF under test for each new GTP tunnel is unique.

Pre-Conditions:

Test environment is set up with SMF, which may be real or simulated, and UPF under test. The tester is able to trace traffic between the UPF under test and the SMF (real or simulated). SMF configures UPF under test to generate the TEIDs.

Execution Steps:

1) The tester intercepts the traffic between the UPF under test and the SMF.

2) The tester triggers the maximum number of concurrent N4 session establishment requests.

3) The tester captures the N4 session establishment responses sent from UPF to SMF and verifies that the F-TEID created for each generated response is unique.

Expected Results:

The F-TEID set in each different N4 session establishment response is unique.

Expected format of evidence:

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

4.2.3 Technical baseline

4.2.3.1 Introduction

The present clause provides baseline technical requirements.

4.2.3.2 Protecting data and information

4.2.3.2.1 Protecting data and information – general

There are no UPF-specific additions to clause 4.2.3.2.1 of TS 33.117 [3].

4.2.3.2.2 Protecting data and information – unauthorized viewing

There are no UPF-specific additions to clause 4.2.3.2.2 of TS 33.117 [3].

4.2.3.2.3 Protecting data and information in storage

There are no UPF-specific additions to clause 4.2.3.2.3 of TS 33.117 [3].

4.2.3.2.4 Protecting data and information in transfer

There are no UPF-specific additions to clause 4.2.3.2.4 of TS 33.117 [3].

4.2.3.2.5 Logging access to personal data

There are no UPF-specific additions to clause 4.2.3.2.5 of TS 33.117 [3].

4.2.3.3 Protecting availability and integrity

There are no UPF-specific additions to clause 4.2.3.3 of TS 33.117 [3].

4.2.3.4 Authentication and authorization

There are no UPF-specific additions to clause 4.2.3.4 of TS 33.117 [3].

4.2.3.5 Protecting sessions

There are no UPF-specific additions to clause 4.2.3.5 of TS 33.117 [3].

4.2.3.6 Logging

There are no UPF-specific additions to clause 4.2.3.6 of TS 33.117 [3].

4.2.4 Operating systems

There are no UPF-specific additions to clause 4.2.4 of TS 33.117 [3].

4.2.5 Web Servers

There are no UPF-specific additions to clause 4.2.5 of TS 33.117 [3].

4.2.6 Network Devices

There are no UPF-specific additions to clause 4.2.6 in TS 33.117 [3].

4.3 UPF-specific adaptations of hardening requirements and related test cases

4.3.1 Introduction

This clause specifies the UPF-specific adaptations of hardening requirements and related test cases.

4.3.2 Technical baseline

There are no UPF-specific additions to clause 4.3.2 in TS 33.117 [3].

4.3.3 Operating systems

There are no UPF-specific additions to clause 4.3.3 in TS 33.117 [3].

4.3.4 Web servers

There are no UPF-specific additions to clause 4.3.4 in TS 33.117 [3].

4.3.5 Network devices

There are no UPF-specific additions to clause 4.3.5 in TS 33.117 [3].

4.3.6 Network functions in service-based architecture

There are no UPF-specific additions to clause 4.3.6 in TS 33.117 [3].

4.4 UPF-specific adaptations of basic vulnerability testing requirements and related test cases

There are no UPF-specific additions to clause 4.4 in TS 33.117 [3].

Annex A (informative): Change history

Change history							
Date	Meeting	Tdoc	CR	Rev	Cat	Subject/Comment	New version
2019-10						EditHelp review, editorial changes	16.0.1
2019-12	SA#86	SP-191138	0002	1	F	Corrections for clean-up and alignment	16.1.0
2020-12	SA#90e	SP-201004	0003	-	F	Reference of general SBA/SBI aspect in 33.513	16.2.0
2023-06	SA#100	SP-230615	0011	1	F	Correction of SBA test for UPF	16.3.0

History

Document history		
V16.1.0	October 2020	Publication
V16.2.0	January 2021	Publication
V16.3.0	July 2023	Publication