ETSI TS 133 514 V16.2.0 (2020-08)

5G;
5G Security Assurance Specification (SCAS)
for the Unified Data Management (UDM)
network product class
(3GPP TS 33.514 version 16.2.0 Release 16)

Reference
DTS/TSGS-0333514vg20

Keywords
5G,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

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.

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

[5] 3GPP TS 23.501: "System Architecture for the 5G System (5GS)".

[6] 3GPP TS 23.003: "Numbering, addressing and identification".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms 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].

Subscription Identifier: Defined in TS 23.501 [5] and in TS 23.003 [6].

Subscription Concealed Identifier: Defined in TS 33.501 [2].

Subscription Identifier De-concealing Function: Defined in TS 33.501 [2].

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].

5GS 5G System

AMF	Access and Mobility Management Function
AKA	Authentication and Key Agreement
ARPF	Authentication credential Repository and Processing Function
AUSF	Authentication Server Function
EAP	Extensible Authentication Protocol
SIDF	Subscription Identifier De-concealing Function
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
UDM	Unified Data Management
UDR	Unified Data Repository

4 UDM-specific security requirements and related test cases

4.1 Introduction

UDM specific security requirements include both requirements derived from UDM specific security functional requirements in relevant specifications as well as security requirements introduced in the present document derived from the threats specific to UDM as described in TR 33.926 [4].

4.2 UDM-specific security functional requirements and related test cases

4.2.1 User Privacy Procedure

4.2.1.1 De-concealment of SUPI from the SUCI based on the protection scheme used to generate the SUCI.

Requirement Name: De-concealment of SUPI from the SUCI based on the protection scheme used to generate the SUCI.

Requirement Reference: TS 33.501 [2], clause 5.8.2.

Requirement Description: "The SIDF shall resolve the SUPI from the SUCI based on the protection scheme used to generate the SUCI." as specified in TS 33.501 [2], clause 5.8.2.

Threat References: TR 33.926 [4], clause E.2.2.1, Incorrect SUCI de-concealment.

TEST CASE:

Test Name: TC_DE-CONCEAL_SUPI_from_SUCI_UDM

Purpose:

Verify that the SIDF De-conceals the SUPI from the SUCI based on the protection scheme used to generate the SUCI.

Procedure and execution steps:

Pre-Condition:

- UDM network product is connected in simulated/real network environment.
- Tester shall have access to the subscription data stored in UDR.
- Tester shall record the SUPI from the UE.

Execution Steps:

Test case:

Tester shall capture the entire authentication procedure between UE and AMF over N1, N12 and N13 interface using any network analyser.

1. Tester shall filter the Nudm_Authentication_Get Response message sent from UDM to AUSF over N13 interface containing the SUPI.
2. Tester shall compare the SUPI gotten from UE and the SUPI retrieved from Nudm_Authentication_Get Response message.

Expected Results:

SIDF resolves the SUPI from the SUCI based on the protection scheme used to generate the SUCI.

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 Authentication and key agreement procedure

4.2.2.1 Synchronization failure handling

Requirement Name: Synchronization failure handling

Requirement Reference: TS 33.501 [2], clause 6.1.3.3.2.

Requirement Description: "When the UDM/ARPF receives an Nudm_UEAuthentication_Get Request message with a "synchronisation failure indication" it acts as described in TS 33.102 [9], clause 6.3.5 where ARPF is mapped to HE/AuC. The UDM/ARPF sends an Nudm_UEAuthentication_Get Response message with a new authentication vector for either EAP-AKA' or 5G-AKA depending on the authentication method applicable for the user to the AUSF.as specified in TS 33.501 [2], clause 6.1.3.3.2.

Threat References: TR 33.926 [4], clause E.2.2.2, Synchronization failure.

Test Case:

Purpose:

Verify that synchronization failure is recovered correctly in the home network.

Pre-Conditions:

Test environment with AUSF. The AUSF may be simulated.

Execution Steps

1. The AUSF sends an Nudm_UEAuthentication_Get Request message to the UDM with a "synchronisation failure indication" and parameters *RAND* and *AUTS*.
2. The UDM/ARPF performs steps 1-5 as described in TS 33.102, clause 6.3.5.

Expected Results:

The UDM sends an Nudm_UEAuthentication_Get Response message with a new authentication vector to the AUSF.

4.2.2.2 Storing of authentication status of UE by UDM.

Requirement Name: Storing of authentication status of UE by UDM.

Requirement Reference: TS 33.501 [2], clause 6.1.4.1a

Requirement Description: "The UDM shall store the authentication status of the UE (SUPI, authentication result, timestamp, and the serving network name) after authentication" as specified in TS 33.501 [2], clause 6.1.4.1a.

Threat References: TR 33.926 [4], clause E.2.2.3, Failure to store of authentication status.

TEST CASE:

Test Name: TC_AUTH_STATUS_STORE_UDM

Purpose:

Verify that the UDM under test stores the authentication status of UE, which is identical to the UE authentication information sent to/from the AUSF and the AMF.

Procedure and execution steps:

Pre-Condition:

- UDM network product is connected with an AUSF in simulated/real network environment involving AMF, eNB.
- The tester shall have access to all the authentication specific data sent over N1 interface, N12 interface and N13 interface.
- The tester shall have access to the UDM under test.

Execution Steps:

1. The tester shall capture the entire authentication procedure and authentication confirmation procedure over N12 and N13 interface using any network analyser.
2. the tester shall filter the Nudm_UEAuthentication_Get Request message sent over the N13 interface to retrieve serving network name.
3. The ester shall filter the Nudm_Authentication_Get Response message sent over N13 interface to find the SUPI.
4. The tester shall filter the Nausf_UEAuthentication_Authenticate Response message sent over N12 interface to retrieve the Authentication result (EAP success/failure for EAP-AKA' or Result for 5G AKA).
5. The tester shall filter the Nudm_UEAuthentication_ResultConfirmation Request message to retrieve the authentication result and time of authentication procedure sent from the AUSF to the UDM over N13 interface.
6. The tester shall compare the serving network name stored in the UDM against the serving network name retrieved from the Nudm_Authentication_Get Request message and the serving network name retrieved from the Nudm_UEAuthentication_ResultConfirmation Request message.
7. The tester shall compare the authentication status stored in the UDM against the authentication result retrieved from N12 interface.
8. The tester shall compare the SUPI stored in the UDM against the SUPI retrieved from the Nudm_Authentication_Get Response message and the SUPI retrieved from the Nudm_UEAuthentication_ResultConfirmation Request message.
9. The tester shall compare the timestamp stored in the UDM against the time of authentication procedure retrieved from the Nudm_UEAuthentication_ResultConfirmation Request message.

Expected Results:

The storing of authentication status (SUPI, authentication result, timestamp, and the serving network name) of UE at the UDM is verified.

Expected format of evidence:

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

NOTE: this test case does not apply to the deployment scenario where the UDM and AUSF network products are collocated without an open N13 interface.

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 UDM-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 UDM-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 UDM-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 UDM-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 UDM-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 UDM-specific additions to clause 4.2.3.3 of TS 33.117 [3].

4.2.3.4 Authentication and authorization

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

4.2.3.5 Protecting sessions

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

4.2.3.6 Logging

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

4.2.4 Operating Systems

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

4.2.5 Web Servers

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

4.2.6 Network Devices

There are no UDM-specific additions to clause 4.2.6 of TS 33.117 [3].

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

4.3.1 Introduction

The present clause contains UDM-specific adaptations of hardening requirements and related test cases.

4.3.2 Technical baseline

There are no UDM-specific additions to clause 4.3.2 of TS 33.117 [3].

4.3.3 Operating systems

There are no UDM-specific additions to clause 4.3.3 of TS 33.117 [3].

4.3.4 Web servers

There are no UDM-specific additions to clause 4.3.4 of TS 33.117 [3].

4.3.5 Network devices

There are no UDM-specific additions to clause 4.3.5 of TS 33.117 [3].

4.3.6 Network functions in service-based architecture

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

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

There are no UDM-specific additions to clause 4.4 of TS 33.117 [3].

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2019-09	SA#85					Change control version	16.0.0
2019-10						EditHelp review	16.0.1
2019-12	SA#86	SP-191138	0001	-	F	Corrections for clean-up and alignment	16.1.0
2020-07	SA#88E	SP-200358	0002	-	F	Update to the test case of Storing of UE authentication status by UDM	16.2.0

History

Document history		
V16.2.0	August 2020	Publication