ETSI TS 133 514 V18.3.0 (2024-07)

5G;
5G Security Assurance Specification (SCAS)
for the Unified Data Management (UDM) network product class
(3GPP TS 33.514 version 18.3.0 Release 18)

Reference
RTS/TSGS-0333514vi30

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

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: "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".

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

[8] SECG SEC 1: Recommended Elliptic Curve Cryptography, Version 2.0, 2009. Available http://www.secg.org/sec1-v2.pdf

[9] 3GPP TS 29.503: "Unified Data Management Services".

[10] 3GPP TR 33.916: "Security Assurance Methodology (SECAM) for 3GPP network products".

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 33.501 [2] 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].

Network Function: As defined in TS 23.501 [5].

Network Product: As defined in TR 33.916 [10].

Network Product Class: As defined in TR 33.916 [10].

Pcap file: A file format used to store network packet data captured from a network interface.

Screenshot: A digital image that shows the contents of a display.

Vulnerability: As defined in TR 33.916 [10].

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
AV	Authentication Vector
EAP	Extensible Authentication Protocol
JSON	Javascript Object Notation
SBA	Service Based Architecture
SBI	Service Based Interfaces
SIDF	Subscription Identifier De-concealing Function
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TSC	Time Sensitive Communication
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 Security functional requirements on the UDM derived from 3GPP specifications and related test cases

4.2.0 General

The general approach in TS 33.117 [3] clause 4.2.2.1 and all the requirements and test cases in TS 33.117 [3] clause 4.2.2.2 related to SBA/SBI aspect apply to the UDM network product class.

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 resolves 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 including an AUSF and AMF.
- Tester shall have access to the subscription data stored in UDR.
- Tester shall record the SUPI from the UE.

Execution Steps:

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_UEAuthentication_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_UEAuthentication_Get Response message.

NOTE: The tester may filter the Nausf_UEAutentication_Authenticate Response message sent from the UDM/AUSF to the AMF over N12 interface containing the SUPI, if the UDM and AUSF network products are collocated without an open N13 interface.

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.

4.2.1.2 Rejection of SUCIs using an ECIES protection scheme with an invalid public key.

Requirement Name: Rejection of SUCIs using an ECIES protection scheme with an invalid public key.

Requirement Reference: TS 33.501 [2], clause C.3.3 with reference to SECG SEC 1 [8] clause 2.3.4.

Requirement Description: Output: An elliptic curve point P, or "invalid" as specified [8], clause 2.3.4.

Threat References: TR 33.926 [4], clause E.2.2.6, Invalid public key.

TEST CASE:

Test Name: TC_REJECT_SUCI_PROFILE_B_INVALID_PUBKEY_UDM

Purpose:

Verify that the SIDF rejects the SUCI if it uses an ECIES protection scheme and contains an invalid point as the UE's public key for Profile B.

Procedure and execution steps:

Pre-Condition:

- The tester has access to the public information of the SUCI profile (e.g., profile type, public key …) of theUDM/SIDF under test.
- The tester has configured the UDM to use Profile B.
- The tester has access to a SUPI of provisioned subscriber

Execution Steps

Test case:

1. The tester selects an invalid point (NOTE 1) and uses the point as a public key to encrypt the SUPI based on the encryption defined in Annex C of 33.501 [2] and SECG SEC 1 [8] (NOTE 2).
2. The tester sends the SUCI to the Nudm_UEAuthentication_Get service of the UDM/ SIDF under test.

NOTE 1: An example invalid point for Profile B (of order 47) is: 0x049af0190d4e237c462c94c447052c770f6d348866f1dbbe29a0ee889f18835d6a973457a6730323716ef2c8a3723793be64b54cec40eb86ab194057c95baf8cfe.

NOTE 2: An example SUCI encrypted with the invalid point (above) for the MCC|MNC (274012) and MSIN (001002086) for Profile B (Annex C of 33.501 [2]) is: suci-0-274-012-0-2-2-049af0190d4e237c462c94c447052c770f6d348866f1dbbe29a0ee889f18835d6a973457a6730323716ef2c8a3723793be64b54cec40eb86ab194057c95baf8cfe8cf9a0959454b74e31a331018b.

Expected Results:

The UDM/SIDF rejects the SUCI, and the UDM sends a Nudm_UEAuthentication_Get Response message with an HTTP status code "403 Forbidden" and may include additional error information in the response body (in "ProblemDetails" element) as specified in TS 29.503 [9], clause 5.4.2.2.2, 2b.

NOTE 3: Values for "ProblemDetails" may be AUTHENTICATION_REJECTED or INVALID_SCHEME_OUTPUT as specified in TS 29.503 [9], clause 6.3.3.2.4.2.2-2.

Expected format of evidence:

Evidence suitable for the interface, e.g., evidence can be presented in the form of packet trace (e.g., pcap file).

4.2.1.3 Rejection of SUCIs using an uncompressed point with Profile B.

Requirement Name: Rejection of SUCIs using an uncompressed point with Profile B.

Requirement Reference: TS 33.501 [2], clause C.3.4.0.

Requirement Description: Profile B shall use point compression to save overhead as specified in TS 33.501 [2], clause C.3.4.0.

Threat References: TR 33.926 [4], clause E.2.2.6, Invalid public key.

TEST CASE:

Test Name: TC_REJECT_SUCI_PROFILE_B_NO_COMPRESSION_UDM

Purpose:

Verify that the SIDF rejects the SUCI if it uses the ECIES Profile B protection scheme and contains an uncompressed point as the UE's public key.

Procedure and execution steps:

Pre-Condition:

- Tester shall have access to the HN’s public key for SUCI decryption with Profile B.

Execution Steps

Test case:1. The tester shall generate a SUCI for a registered SUPI with the protection scheme output for Profile B. Theephemeral public key of the UE should be in the uncompressed point format specified in [x] clause 2.3.3. The remaining parts of the protection scheme output retain their format [x].

NOTE 1: The uncompressed point format shall have a size of 65 bytes, and the most significant byte shall be 0x04. The compressed point format shall have a size of 33 bytes, with 0x02 or 0x03 as the most significant byte. Test data in TS 33.501 [2], clause C.4.4.1.

2. The tester shall send the SUCI to the Nudm_UEAuthentication_Get service of the UDM/ SIDF under test.

Expected Results:

The SIDF rejects the SUCI, and the UDM sends a Nudm_UEAuthentication_Get Response message with an HTTP status code "403 Forbidden" and may include additional error information in the response body (in "ProblemDetails" element) as specified in TS 29.503 [9], clause 5.4.2.2.2, 2b.

NOTE 2: Values for "ProblemDetails" may be AUTHENTICATION_REJECTED or INVALID_SCHEME_OUTPUT as specified in TS 29.503 [9], clause 6.3.3.2.4.2.2-2.

Expected format of evidence:

Evidence suitable for the interface, e.g., evidence can be presented in the form of packet trace (e.g., pcap file).

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 [7], 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:

Test Name: TC_SYNC_FAILURE_HANDLING_UDM

Purpose:

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

Pre-Conditions:

Test environment with an AUSF. The AUSF or AMF 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.

NOTE: The expected results would be that the UDM/AUSF sends an Nausf_UEAuthentication_Authenticate Response message with EAP Request/AKA'-Challenge for EAP AKA', or 5G SE AV for 5G AKA to the AMF, if the UDM and AUSF network products are collocated without an open N13 interface.

Expected format of evidence:

Evidence suitable for the interface, e.g., Screenshot, packet capture or application log containing the operational results.

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 stores 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_UEAuthentication_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_UEAuthentication_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_UEAuthentication_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].

4.2.7 User plane security procedures

4.2.7.1 UP Security enforcement configuration for TSC service

Requirement Name: UP security enforcement configuration

Requirement Reference: TS 33.501 [2], clause L.3, TS 23.501 [5], clause 5.10.3.

Requirement Description:

"After the 5GS TSC-enabled UE is authenticated and data connection is set up, any data received from a TSC bridge or another 5GS TSC-enabled UE shall be transported between DS-TT (in the UE) and NW-TT (in the UPF) in a protected way using the mechanisms for UP security as described in clause 6.6.

The UP security enforcement information shall be set to "required" for data transferred from gNB to a 5GS TSC-enabled UE. This is also applicable to the gPTP messages sent in the user plane."

as specified in TS 33.501 [2], clause L.3.

"The SMF determines at PDU session establishment a User Plane Security Enforcement information for the user plane of a PDU session based on:

- subscribed User Plane Security Policy which is part of SM subscription information received from UDM; and
- User Plane Security Policy locally configured per (DNN, S-NSSAI) in the SMF that is used when the UDM does not provide User Plane Security Policy information.
- The maximum supported data rate per UE for integrity protection for the DRBs, provided by the UE in the Integrity protection maximum data rate IE during PDU Session Establishment. The UE supporting NR as primary RAT, i.e. NG-RAN access via Standalone NR, shall set the Integrity protection maximum data rate IE for Uplink and Downlink to full rate at PDU Session Establishment as defined in TS 24.501 [47]."

as specified in TS 23.501 [5], clause 5.10.3.

Threat References: TR 33.926 [4].

NOTE: The test case below only applies to the UDMs which support the setting and providing of User Plane Security Policy for dedicated TSC service.

Test Case:

Test Name: TC_UP_SECURITY_ENFORCEMENT_CONFIGURATION

Purpose:

Verify that UP security enforcement information is set to "required" for dedicated TSC service.

Pre-Conditions:

Test environment with SMF. The SMF may be simulated.

A dedicated DNN/S-NSSAI combination is defined to identify the TSC service.

The security policy is configured in the UDM.

Execution Steps

1. During the PDU session establishment procedure, the SMF sends a Nudm_SDM_Get Request message to the UDM under test with a dedicated DNN/S-NSSAI combination.
2. The UDM under test sends the Nudm_SDM_Get Response back to the SMF with UP security enforcement information.

Expected Results:

The confidentiality and integrity protection requirements of the UP security enforcement information are set to "required".

Expected format of evidence:

Save the logs and the communication flow in a .pcap file.

4.2.8 User plane security procedures

4.2.8.1 UP security policy configuration for 5G LAN service

Requirement Name: UP security enforcement configuration

Requirement Reference: TS 33.501 [2], clause K.3, TS 23.501 [5], clause 5.10.3.

Requirement Description: "To reduce incremental complexity added by security, all PDU sessions associated with a specific 5G LAN group should have the same UP security policy. When generating the policy enforcement information, and to avoid the redundant double protection, the SMF may consider information by a DN-AAA about DN protection mechanisms already applied."

as specified in TS 33.501 [2], clause K.3.

"The SMF determines at PDU session establishment a User Plane Security Enforcement information for the user plane of a PDU session based on:

- subscribed User Plane Security Policy which is part of SM subscription information received from UDM; and
- User Plane Security Policy locally configured per (DNN, S-NSSAI) in the SMF that is used when the UDM does not provide User Plane Security Policy information.
- The maximum supported data rate per UE for integrity protection for the DRBs, provided by the UE in the Integrity protection maximum data rate IE during PDU Session Establishment. The UE supporting NR as primary RAT, i.e. NG-RAN access via Standalone NR, shall set the Integrity protection maximum data rate IE for Uplink and Downlink to full rate at PDU Session Establishment as defined in TS 24.501 [47]."

as specified in TS 23.501 [5], clause 5.10.3.

Threat References: TR 33.926 [4].

NOTE 1: The test case below only applies to the UDMs which support the setting and providing of User Plane Security Policy for 5G LAN service.

Test Case:

Test Name: TC_UP_SECURITY_ENFORCEMENT_CONFIGURATION_FOR_5G_LAN

Purpose:

Verify that UP security policy is set to the same for all the 5G LAN UEs.

Pre-Conditions:

Test environment with SMF. The SMF may be simulated.

A dedicated DNN/S-NSSAI combination is defined to identify the 5G LAN service.

The security policy of the 5G LAN service is configured in the UDM.

Execution Steps

1. During the PDU session establishment procedure initiated by the UE1, the SMF1 sends a Nudm_SDM_Get Request message to the UDM under test with a dedicated DNN/S-NSSAI combination, and SUPI1.
2. The UDM under test sends the Nudm_SDM_Get Response back to the SMF1 with UP security policy1.
3. During the PDU session establishment procedure initiated by the UE2, the SMF2 sends a Nudm_SDM_Get Request message to the UDM under test with a dedicated DNN/S-NSSAI combination, and SUPI2.
4. The UDM under test sends the Nudm_SDM_Get Response back to the SMF2 with UP security policy2.

NOTE 2: SMF1 and SMF2 could be the same network function.

Expected Results:

The confidentiality and integrity protection requirements of the UP security policy1 and UP security policy2 are the same.

Expected format of evidence:

Save the logs and the communication flow in a .pcap file.

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

4.4.1 Introduction

There are no UDM specific addtions to clause 4.4.1 of TS 33.117 [3].

4.4.2 Port scanning

There are no UDM specific addtions to clause 4.4.2 of TS 33.117 [3].

4.4.3 Vulnerability scanning

There are no UDM specific addtions to clause 4.4.3 of TS 33.117 [3].

4.4.4 Robustness and fuzz testing

The test cases under clause 4.4.4 of TS 33.117 [3] are applicable to UDM.

The interfaces defined for the UDM are in clause 4.2.3 of TS 23.501 [5].

According to clause 4.4.4 of TS 33.117 [3], the transport protocols available on the interfaces providing IP-based protocols need to be robustness tested. Following TCP/IP layer model and considering all the protocols over transport layer, for UDM, the following interface and protocols are in the scope of the testing:

- For Nudm: The TCP, TLS, HTTP2 and JSON protocols.

NOTE: There could be other interfaces and/or protocols requiring testing under clause 4.4.4 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
2020-09	SA#89E	SP-200703	0003	-	F	Clarification on the test cases if the UDM and AUSF are collocated	16.3.0
2020-12	SA#90e	SP-201004	0004	-	F	Reference of general SBA/SBI aspect in 33.514	16.4.0
2021-06	SA#92e	SP-210440	0005	-	B	CR to include R-16 feature of UDM to 33.514	17.0.0
2023-06	SA#100	SP-230604	0006	1	B	Robustness interfaces and protocols defined for UDM	18.0.0
2023-06	SA#100	SP-230604	0007	1	F	SCAS release reference corrections	18.0.0
2023-09	SA#101	SP-230904	0009	-	F	Correction of UDM service naming	18.1.0
2023-12	SA#102	SP-231339	0010	1	F	Added missing Test Name and Expected format of evidence	18.2.0
2023-12	SA#102	SP-231339	0011	2	F	Added UDM SCAS test cases for checking an invalid and uncompressed point in ECIES protection scheme for SUCI decryption	18.2.0
2024-06	SA#104	SP-240669	0018	1	A	Correction to terms	18.3.0
2024-06	SA#104	SP-240669	0021	-	A	Correction to abbreviations	18.3.0
2024-06	SA#104	SP-240669	0024	-	A	Correction to test names	18.3.0
2024-06	SA#104	SP-240668	0027	-	F	Editorial correction of TEST CASE	18.3.0
2024-06	SA#104	SP-240668	0030	-	F	Fuzz TLS	18.3.0

History

Document history		
V18.2.0	May 2024	Publication
V18.3.0	July 2024	Publication