ETSI TS 133 512 V17.3.0 (2022-05)

5G;
5G Security Assurance Specification (SCAS);
Access and Mobility management Function (AMF)
(3GPP TS 33.512 version 17.3.0 Release 17)

Reference
RTS/TSGS-0333512vh30

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 - 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 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 objectives, requirements and test cases that are specific to the AMF 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 AMF 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 23.003: "Numbering, addressing and identification".

[5] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[6] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[7] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[8] 3GPP TS 23.501: "System Architecture for the 5G System".

[9] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)".

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].

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].

4 AMF-specific security requirements and related test cases

4.1 Introduction

AMF specific security requirements include both requirements derived from AMF-specific security functional requirements in relevant specifications as well as security requirements introduced in the present document derived from the threats specific to AMF as described in TR 33.926 [6].

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

4.2.1 Introduction

The present clause describes the security functional requirements and the corresponding test cases for AMF network product class. The proposed security requirements are classified in two groups:

- Security functional requirements derived from TS 33.501 [2] and detailed in clause 4.2.2.
- General security functional requirements which include requirements not already addressed in TS 33.501 [2] but whose support is also important to ensure that AMF conforms to a common security baseline detailed in clause 4.2.3.

4.2.2 Security functional requirements on the AMF 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 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 AMF network product class.

4.2.2.1 Authentication and key agreement procedure

4.2.2.1.1 Synchronization failure handling

Requirement Name: Synchronization failure handling

Requirement Reference: TS 33.501 [7], clause 6.1.3.3.2

Requirement Description: "Upon receiving an authentication failure message *with synchronisation failure* (AUTS) from the UE, the SEAF sends an Nausf_UEAuthentication_Authenticate Request message with a "*synchronisation failure*

indication" to the AUSF and the AUSF sends an Nudm_UEAuthentication_Get Request message to the UDM/ARPF, together with the following parameters:

- *RAND* sent to the UE in the preceding Authentication Request, and
- *AUTS* received by the SEAF in the response from the UE to that request, as described in clause 6.1.3.2.0 and 6.1.3.3.1.

An SEAF will not react to unsolicited "synchronisation failure indication" messages from the UE.

The SEAF does not send new authentication requests to the UE before having received the response to its Nausf_UEAuthentication_Authenticate Request message with a "*synchronisation failure indication*" from the AUSF (or before it is timed out). "

as specified in TS 33.501[7], clause 6.1.3.3.2.

Threat References: TR 33.926 [6], clause K.2.2.1, Resynchronization

Test Case:

Test Name: TC_SYNC_FAIL_SEAF_AMF

Purpose:

Verify that synchronization failure is correctly handled by the SEAF/AMF.

Pre-Conditions:

- Test environment with UE and AUSF. The UE and the AUSF may be simulated.
- AMF network product is connected in emulated/real network environment.

Execution Steps

Test A:

1) The UE sends an authentication failure message to the SEAF/AMF with *synchronisation failure* (AUTS).
2) The SEAF/AMF sends a Nausf_UEAuthentication_Authenticate Request message with a "*synchronisation failure indication*" to the AUSF.
3) The AUSF sends a Nausf_UEAuthentication_Authenticate Response message to the SEAF/AMF immediately after receiving the request from the SEAF/AMF, to make sure the SEAF/AMF will receive the response before timeout.

Test B:

1) The UE sends an authentication failure message to the SEAF/AMF with *synchronisation failure* (AUTS).
2) The SEAF/AMF sends a Nausf_UEAuthentication_Authenticate Request message with a "*synchronisation failure indication*" to the AUSF.
3) The AUSF does not send a Nausf_UEAuthentication_Authenticate Response message to the SEAF/AMF before timeout.

Expected Results:

Before receiving Nausf_UEAuthentication_Authenticate Response message from the AUSF and before the timer for receiving Nausf_UEAuthentication_Authenticate Response message runs out,

For Test B, the SEAF/AMF does not send any new authentication request to the UE.

For Test A, the SEAF/AMF may initiate new authentication towards the UE.

Expected format of evidence:

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

4.2.2.1.2 RES* verification failure handling

Requirement Name: RES* verification failure handling

Requirement Reference: TS 33.501 [7], clause 6.1.3.2.2

Requirement Description:

"The SEAF shall proceed with step 10 in Figure 6.1.3.2-1 and after receiving the Nausf_UEAuthentication_Authenticate Request message from the AUSF in step 12 in Figure 6.1.3.2-1, proceed as described below:

- If the AUSF has indicated in the Nausf_UEAuthentication_Authenticate Response message to the SEAF that the verification of the RES* was not successful in the AUSF, or
- if the verification of the RES* was not successful in the SEAF,

then the SEAF shall either reject the authentication by sending an Authentication Reject to the UE if the SUCI was used by the UE in the initial NAS message or the SEAF/AMF shall initiate an Identification procedure with the UE if the 5G-GUTI was used by the UE in the initial NAS message to retrieve the SUCI and an additional authentication attempt may be initiated.

Also, if the SEAF does not receive any Nausf_UEAuthentication_Authenticate Request message from the AUSF as expected, then the SEAF shall either reject the authentication to the UE or initiate an Identification procedure with the UE."

As specified in TS 33.501 [7], clause 6.1.3.2.2.

Threat References: TR 33.926 [6], clause K.2.2.3, RES* verification failure

Test Case:

Test Name: TC_RES*_VERIFICATION_FAILURE

Purpose:

1) Verify that the SEAF/AMF correctly handles RES* verification failure detected in the SEAF/AMF or/and in the AUSF, when the SUCI is included in the initial NAS message.
2) Verify that the SEAF/AMF correctly handles RES* verification failure detected in the SEAF/AMF or/and in the AUSF, when the 5G-GUTI is included in the initial NAS message.

Procedure and execution steps:

Pre-Conditions:

Test environment with UE and AUSF. The UE and the AUSF may be simulated.

Execution Steps

A. Test Case 1

1) The UE sends RR with SUCI to the SEAF/AMF under test, to trigger the SEAF/AMF under test to initiate the authentication, i.e. to send Nausf_UEAuthentication_Authenticate Request to the AUSF.
2) The AUSF, after receiving the request from the SEAF/AMF under test, responds with a Nausf_UEAuthentication_Authenticate Response message with an authentication vector to the SEAF/AMF under test.
3) The UE, after receiving the Authentication Request message from the SEAF/AMF under test, returns an incorrect RES* to the SEAF/AMF under test in the NAS Authentication Response message, which will

trigger the AMF to compute HRES*, compare HRES* with HXRES* and send an authentication request to the AUSF. The tester captures the value of RES* in the request.

4) The AUSF returns to the AMF under test the indication of RES* verification failure.

B. Test Case 2

1) The UE sends RR with a 5G-GUTI to the SEAF/AMF under test, to trigger the SEAF/AMF under test to initiate the authentication, i.e. to send Nausf_UEAuthentication_Authenticate Request to the AUSF.

2) The AUSF, after receiving the request from the SEAF/AMF under test, responds with a Nausf_UEAuthentication_Authenticate Response message with an authentication vector to the SEAF/AMF under test.

3) The UE, after receiving the Authentication Request message from the SEAF/AMF under test, returns an incorrect RES* to the SEAF/AMF in the NAS Authentication Response message, which will trigger the AMF to compute HRES* and compare HRES* with HXRES*, and send an authentication request to the AUSF. The tester captures the value of RES* in the request.

4) The AUSF returns to the AMF under test an indication of RES* verification failure.

C. Test Case 3

1) The UE sends RR with SUCI to the SEAF/AMF under test, to trigger the SEAF/AMF under test to initiate the authentication, i.e. to send Nausf_UEAuthentication_Authenticate Request to the AUSF.

2) The AUSF, after receiving the request from the SEAF/AMF under test, responds with a Nausf_UEAuthentication_Authenticate Response message with an authentication vector to the SEAF/AMF under test.

3) The UE returns RES* to the SEAF/AMF under test in the NAS Authentication Response message, which will trigger the AMF to compute HRES*, compare HRES* with HXRES*, and send to the received RES* to the AUSF.

4) The AUSF returns to the AMF under test an indication of RES* verification failure.

D Test Case 4

1) The UE sends RR with 5G-GUTI to the SEAF/AMF under test, to trigger the SEAF/AMF under test to initiate the authentication, i.e. to send Nausf_UEAuthentication_Authenticate Request to the AUSF.

2) The AUSF, after receiving the request from the SEAF/AMF under test, responds with a Nausf_UEAuthentication_Authenticate Response message with an authentication vector to the SEAF/AMF under test.

3) The UE returns RES* to the SEAF/AMF under test in the NAS Authentication Response message, which will trigger the AMF to compute HRES*, compare HRES* with HXRES*, and send to the received RES* to the AUSF.

4) The AUSF returns to the AMF under test an indication of RES* verification failure.

Expected Results:

For test case 1 and 3, the SEAF/AMF rejects the authentication by sending an Authentication Reject to the UE.

For test case 2 and 4, the SEAF/AMF initiates an Identification procedure with the UE to retrieve the SUCI.

Expected format of evidence:

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

4.2.2.1.3 NAS based redirection from 5GS to EPS

Requirement Name: NAS based redirection from 5GS to EPS

Requirement Reference: TS 33.501 [7], clause 6.16.4. , TS 23.501 [8], clause 5.31.3.

Requirement Description: "When a UE initiates registration procedure with the AMF, the AMF may redirect the UE from 5GC to EPC by including a EMM cause indicating to the UE that it shall not use 5GC, as described in clause 5.31.3 in TS 23.501 [2]. The following requirements apply to Registration Reject message with an EMM cause which indicates to the UE that the UE shall not use 5GC:

- the AMF shall only send such a Registration Reject message once NAS security has been established between the AMF and the UE; and
- the UE shall only act upon such Registration Reject message if received integrity protected and if UE has verified the integrity of the Registration Reject message successfully.

NOTE 1: This solution does not apply to unauthenticated emergency calls.

" as specified in TS 33.501 [7], clause 6.16.4. "

"In networks that support CIoT features in both EPC and 5GC, the operator may steer UEs from a specific CN type due to operator policy, e.g. due to roaming agreements, Preferred and Supported Network Behaviour, load redistribution, etc. Operator policies in EPC and 5GC are assumed to avoid steering UEs back and forth between EPC and 5GC.

" as specified in TS 23.501 [8], clause 5.31.3".

Threat Reference: TBD

Test Name: TC_AMF_REDIRCTION_5GS_EPS

Purpose:

Verify that AMF under test does not send a Registration Reject message containing an EMM cause indicating to the UE that the UE shall not use 5GC , if NAS security is not established. .

NOTE 2: This test case only applies to the AMF under test which supports the security handling in CIoT.

Pre-Conditions:

- Test environment with UE. The UE may be simulated.
- AMF under test is connected in emulated/real network environment.

- Tester configures the operator policy of the AMF that all the UEs sending initial registration request should be redirected from 5GS to EPS.

Execution Steps

1. UE initiates initial registration procedure with the AMF.
2. The AMF under test determines that the UE shall not use 5GC, and needs to redirect the UE from 5GC to EPC.

3. The AMF under test sends a Registration Reject message with a 5GMM cause indicating to the UE that the UE shall not use 5GC.

Expected Results:

The NAS SMC is performed before sending the Registration Reject message.

Expected format of evidence:

Screenshot containing the operational results.

4.2.2.2 Void

4.2.2.3 Security mode command procedure

4.2.2.3.1 Replay protection of NAS signalling messages

Requirement Name: Replay protection of NAS signalling messages

Requirement Reference: TS 33.501 [7], clause 5.5.2.

Requirement Description: " The AMF shall support integrity protection and replay protection of NAS-signalling." as specified in TS 33.501 [2], clause 5.5.2.

Threat References: TR 33.926 [6], clause K.2.3.1, Bidding Down

Test case:

Test Name: TC_NAS_REPLAY_AMF

Purpose:

Verify that the NAS signalling messages are replay protected by AMF over N1 interface between UE and AMF.

Procedure and execution steps:

Pre-Condition:

- AMF network product is connected in emulated/real network environment.
- Tester shall have access to the NAS signalling packets sent between UE and AMF over N1 interface.
- Tester shall ensure that integrity protection algorithm other than NIA0 is used.

Execution Steps:

1. The tester shall capture the NAS SMC procedure taking place between UE and AMF over N1 interface using any network analyser.
2. The tester shall filter the NAS Security Mode Complete message by using a filter.
3. The tester shall check for the NAS SQN of filtered NAS Security Mode Complete message and using any packet crafting tool the tester shall create a NAS Security Mode Complete message containing same NAS SQN of the filtered NAS Security Mode Complete message or the tester shall replay the captured NAS signalling packets.
4. Tester shall check whether the replayed NAS signalling packets were processed by the AMF by capturing over N1interface to see if any corresponding response message is received from the AMF.
5. Tester shall confirm that AMF provides replay protection by dropping/ignoring the replayed packet if no corresponding response is sent by the AMF to the replayed packet.
6. Tester shall verify from the result that if the crafted NAS Security Mode Complete message or replayed NAS signalling messages are not processed by the AMF when the N1 interface is replay protected

Expected Results:

The NAS signalling messages sent between UE and AMF over N1 interface are replay protected.

Expected format of evidence:

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

4.2.2.3.2 NAS NULL integrity protection

Requirement Name: NAS NULL integrity protection

Requirement Reference: TS 33.501 [7], clause 5.5.2

Requirement Description: "NIA0 shall be disabled in AMF in the deployments where support of unauthenticated emergency session is not a regulatory requirement." as specified in TS 33.501 [7], clause 5.5.2

Threat References: TR 33.926 [6], clause K.2.3.3, NAS NULL integrity protection

Test Case:

Test Name: TC_NAS_NULL_INT_AMF

Purpose:

Verify that NAS NULL integrity protection algorithm is used correctly.

Pre-Conditions:

Test environment with a UE. The UE may be simulated.

The AMF under test is configured to initiate authentication for both emergency and non-emergency registrations.

Execution Steps

Test case A:

1. The UE initiates an emergency registration.
2. The AMF derives the K_{AMF} and NAS signalling keys after successful authentication of the UE.
3. The AMF sends the NAS Security Mode Command message to the UE containing the selected NAS algorithms.

Test case B:

1. The UE initiates a non-emergency registration.
2. The AMF derives the K_{AMF} and NAS signalling keys after successful authentication of the UE.
3. The AMF sends the NAS Security Mode Command message to the UE containing the selected NAS algorithms.

Expected Results:

In both emergency and non-emergency registrations, the UE was successfully authentication and the integrity algorithm selected by the AMF in NAS SMC message is different from NIA0.

The NAS Security Mode Command message is integrity protected by the AMF.

Expected format of evidence:

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

4.2.2.3.3 NAS integrity algorithm selection and use

Requirement Name: NAS integrity algorithm selection and use

Requirement Reference: TS 33.501 [7], clause 6.7.1

Requirement Description: "The AMF shall then initiate a NAS security mode command procedure, and include the chosen algorithm and UE security capabilities (to detect modification of the UE security capabilities by an attacker) in the message to the UE (see sub-clause 6.7.2 of the present document). The AMF shall select the NAS algorithm which have the highest priority according to the ordered lists." as specified in TS 33.501 [7], clause 5.5.2.

Threat References: TR 33.926 [6], clause K.2.3.2, NAS integrity selection and use

Test Case:

Test Name: TC_NAS_INT_SELECTION_USE_AMF

Purpose:

Verify that the AMF selects the NAS integrity algorithm which has the highest priority according to the ordered list of supported integrity algorithms and is contained in the 5G security capabilities supported by the UE.

Verify that the selected NAS security algorithm is being used.

Pre-Conditions:

Test environment with a UE containing its 5G security capabilities, AUSF and UDM. The UE, AUSF and UDM may be simulated.

The list of ordered NAS integrity algorithms are configured on the AMF under test.

Execution Steps:

1) The UE sends a Registration Request with Initial Registration type to the AMF unders test.

2) The tester filters the Security Mode Command and Security Mode Complete messages.

3) The tester examines the selected integrity algorithm in the SMC against the list of ordered NAS integrity algorithm and the 5G security capabilities supported by the UE. The tester examines the MAC verification of the Security Mode Complete at the AMF under test.

Expected Results:

The selected integrity algorithm has the highest priority according to the list of ordered NAS integrity algorithm and is contained in the UE 5G security capabilities.

The MAC verification of the Security Mode Complete message is successful.

Expected format of evidence:

Logs and communication flow saved in a .pcap file.

4.2.2.4 Security in intra-RAT mobility

4.2.2.4.1 Bidding down prevention in Xn-handover

Requirement Name: Bidding down prevention in Xn-handovers

Requirement Reference: TS 33.501 [7], clause 6.7.3.1

Requirement Description: "In the Path-Switch message, the target gNB/ng-eNB shall send the UE's 5G security capabilities received from the source gNB/ng-eNB to the AMF. The AMF shall verify that the UE's 5G security capabilities received from the target gNB/ng-eNB are the same as the UE's 5G security capabilities that the AMF has locally stored. If there is a mismatch, the AMF shall send its locally stored 5G security capabilities of the UE to the target gNB/ng-eNB in the Path-Switch Acknowledge message. The AMF shall support logging capabilities for this event and may take additional measures, such as raising an alarm."

as specified in TS 33.501 [7], clause 6.7.3.1.

Threat References: TR 33.926 [6], clause K.2.4.1, Bidding down on Xn-Handover

Test Case:

Test Name: TC_BIDDING_DOWN_XN_AMF

Purpose:

Verify that bidding down is prevented by the AMF under test in Xn handovers.

Pre-Conditions:

Test environment with (source and target) gNBs may be simulated.

The AMF under test is configured with the UE’s security context for the UE.

The AMF under test is configured to log UE security capability mismatch.

Execution Steps

The tester sends 5G security capabilities for the UE, different from the ones stored in the AMF, to the AMF under test using a Path-Switch message.

Expected Results:

The tester captures the Path-Switch Acknowledge message sent by AMF under test to the target gNB, which includes the locally stored 5G security capabilities in the AMF under test for that UE.

The tester verifies that a log entry showing the capability mismatch is logged.

Expected format of evidence

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

4.2.2.4.2 NAS protection algorithm selection in AMF change

Requirement Name: NAS protection algorithm selection in AMF change

Requirement Reference: TS 33.501 [7], clause 6.7.1.2

Requirement Description: "If the change of the AMF at N2-Handover or mobility registration update results in the change of algorithm to be used for establishing NAS security, the target AMF shall indicate the selected algorithm to the UE as defined in Clause 6.9.2.3.3 for N2-Handover (i.e., using NAS Container) and Clause 6.9.3 for mobility registration update (i.e., using NAS SMC). The AMF shall select the NAS algorithm which has the highest priority according to the ordered lists (see sub-clause 6.7.1.1 of the present document)."

as specified in TS 33.501 [7], clause 6.7.1.2.

Threat References: TR 33.926 [6], clause K.2.4.2, NAS integrity protection algorithm selection in AMF change

Test Case:

Test Name: TC_NAS_ALG_AMF_CHANGE _AMF

Purpose:

Verify that NAS protection algorithms are selected correctly.

Pre-Conditions:

Test environment with source gNB, target gNB and source AMF. Source and target gNBs and source AMF may be simulated.

Execution Steps

Test case 1: N2-Handover

> The AMF under test receives the UE security capabilities and the NAS algorithms used by the source AMF from the source AMF. The AMF under test selects the NAS algorithms which have the highest priority according to the ordered lists. The lists are configured such that the algorithms selected by the AMF under test are different from the ones received from the source AMF.

Test case 2: Mobility registration update

> The AMF under test receives the UE security capabilities and the NAS algorithms used by the source AMF from the source AMF. The AMF under test selects the NAS algorithms which have the highest priority according to the ordered lists. The lists are configured such that the algorithms selected by the AMF under test are different from the ones received from the source AMF.

Expected Results:

For Test case 1, the tester captures the NASC of the NGAP HANDOVER REQUEST message sent by the AMF under test to the gNB, which includes the chosen algorithm.

For Test case 2, the AMF under test initiates a NAS security mode command procedure and includes the chosen algorithms.

Expected format of evidence:

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

4.2.2.5 5G-GUTI allocation

4.2.2.5.1 5G-GUTI allocation

Requirement Name: 5G-GUTI allocation

Requirement Reference: TS 33.501 [7], clause 6.12.3

Requirement Description: "A new 5G-GUTI shall be sent to a UE only after a successful activation of NAS security. The 5G-GUTI is defined in TS 23.003 [19].

Upon receiving Registration Request message of type "initial registration" or "mobility registration update" from a UE, the AMF shall send a new 5G-GUTI to the UE during the registration procedure.

Upon receiving Registration Request message of type "periodic registration update" from a UE, the AMF should send a new 5G-GUTI to the UE during the registration procedure.

Upon receiving Service Request message sent by the UE in response to a Paging message, the AMF shall send a new 5G-GUTI to the UE. This new 5G-GUTI shall be sent before the current NAS signalling connection is released or the N1 NAS signalling connection is suspended.

Upon receiving an indication from the lower layers that the RRC connection has been resumed for a UE in 5GMM-IDLE mode with suspend indication in response to a Paging message, the AMF shall send a new 5G-GUTI to the UE. This new 5G-GUTI shall be sent before the current NAS signalling connection is released or the suspension of the N1 NAS signalling connection.NOTE 1: It is left to implementation to re-assign 5G-GUTI more frequently than in cases mentioned above, for example after a Service Request message from the UE not triggered by the network..

NOTE 2: It is left to implementation to generate 5G-GUTI containing 5G-TMSI that uniquely identifies the UE within the AMF."

as specified in TS 33.501 [7], clause 6.12.3.

Threat References: TR 33.926 [6], clause K.2.7.1, Failure to allocate new 5G-GUTI

Test Case:

Test Name: TC_5G_GUTI_ALLOCATION _AMF

Purpose:

Verify that a new 5G-GUTI is allocated by the AMF under test in these scenarios accordingly.

Pre-Conditions:

For the following test case 1, 2, and 3, the following pre-conditions apply.

Test environment with a UE. The UE may be simulated.

Tester has access to the NAS signalling packets sent over N1 interface.

Tester has the knowledge of the UE’s security context used for protecting the Registration Request of type "mobility registration update" and Service Request, including the old 5G-GUTI, ngKSI, UE NR security capability, NAS security context. And the tester shall configure the UE’s security context on the AMF under test.For the following test case 4, more pre-conditions are required. Both the UE and the AMF under test support UP CIoT 5GS Optimization. The UE has requested the use of UP CIoT 5GS Optimization during the registration procedure, and afterwards the UE has gone to CM Idle with Suspend Indicator.

Execution Steps

Test case 1:

Upon receiving Registration Request message of type "initial registration" from a UE, the AMF sends a new 5G-GUTI to the UE during the registration procedure.

Test case 2:

Upon receiving Registration Request message of type "mobility registration update" from a UE, the AMF sends a new 5G-GUTI to the UE during the registration procedure.

Test case 3:

Upon receiving Service Request message sent by the UE in response to a Paging message, the AMF sends a new 5G-GUTI to the UE.

Test case 4:

The AMF under test is triggered to page the UE in CM Idle with Suspend Indicator. After paging the UE in CM-Idle with Suspend indicator, the AMF shall send a new 5G-GUTI to the UE.

NOTE 1: Test case 4 is only applicable to AMF supporting UP CIoT 5GS Optimization.

Expected Results:

For Test case 1, 2, 3 and 4, the tester retrieves a new 5G-GUTI by accessing the NAS signalling packets sent by the AMF under test over N1 interface during registration procedure.

For Test case 1, 2, 3 and 4, the NAS message encapsulating the new 5G-GUTI is confidentiality and integrity protected by the AMF under test using the NAS security context, which is same as the UE's NAS security context.

The new 5G-GUTI is different from the old 5G-GUTI.

Expected format of evidence:

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

4.2.2.6 Security in registration procedure

4.2.2.6.1 Invalid or unacceptable UE security capabilities handling

Requirement Name: Invalid or unacceptable UE security capabilities handling

Requirement Reference: TS 24.501 [5], clause 5.5.1.2.8

Requirement Description:"

…

i) UE security capabilities invalid or unacceptable

If the REGISTRATION REQUEST message is received with invalid or unacceptable UE security capabilities (e.g. no 5GS encryption algorithms (all bits zero), no 5GS integrity algorithms (all bits zero), mandatory 5GS encryption algorithms not supported or mandatory 5GS integrity algorithms not supported, etc.), the AMF shall return a REGISTRATION REJECT message."

as specified in TS 24.501 [5], clause 5.5.1.2.8.

Threat References: TR 33.926 [6], clause K.2.6.1, Invalid or unacceptable UE security capabilities

Test Case:

Test Name: TC_UE_SEC_CAP_HANDLING_AMF

Purpose:

Verify that UE security capabilities invalid or unacceptable are not accepted by the AMF under test in registration procedure.

Pre-Conditions:

Test environment with (target) UE, which may be simulated.

The tester configures invalid/unacceptable UE security capabilities (no 5GS encryption algorithms (all bits zero), no 5GS integrity algorithms (all bits zero), mandatory 5GS encryption algorithms not supported or mandatory 5GS integrity algorithms not supported) on the UE.

Execution Steps

The UE sends UE security capabilities to the AMF under test using registration request message.

Expected Results:

The tester captures the Registration reject message sent by AMF under test to the UE.

Expected format of evidence

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

4.2.2.7 RRCRestablishment in Control Plane CIoT 5GS Optimization

Requirement Name: RRCRestablishment in Control Plane CIoT 5GS Optimization

Requirement Reference: TS 38.413 [9], clause 8.3.8.2

*Requirement Description: "*Upon receiving the RAN CP RELOCATION INDICATION message, the AMF shall authenticate the request using the NAS-level security information received in the UL CP Security Information IE and if the authentication is successful initiate the Connection Establishment Indication procedure including NAS-level security information in the DL CP Security Information IE.

In case the AMF cannot authenticate the UE's request, the CONNECTION ESTABLISHMENT INDICATION message does not contain security information, and the NG-RAN node shall fail the RRC Re-establishment.

In case of authentication failure, the NG-RAN node and the AMF should locally release the allocated NG resources, if any." as specified in TS 38.413 [9], clause 8.3.8.2.

Threat References: TR 33.926 [5], clause K.2.9.1 –Failed Verification of UE Identity during RRC Reestablishment Procedure for CP CIoT 5GS Optimization.

Test Case*:*

Test Name: TC_AMF_REEST_CP_CIOT

Purpose: To verify that the verification of RRC Reestablishment is applied correctly.

Pre-Condition:

Test environment with UE and ng-eNB, which may be simulated. The UE is using Control Plane CIoT 5GS Optimization.

-AMF

Capability:

Ability to support the CIoT senario.

Execution Steps:

A. Test Case 1

1) The UE sends the RRC Connection Reestablishment Request message to the ng-eNB.

2) The ng-eNB sends RAN CP RELOCATION INDICATION message to the AMF.

B. Test Case 2

1) The UE sends the RRC Connection Reestablishment Request message to the ng-eNB.

2) The ng-eNB sends RAN CP RELOCATION INDICATION message to the AMF. The ng-eNB modifies UL NAS MAC in UL CP Security Information

Expected Results:
For test case 1, the AMF sends CONNECTION ESTABLISHMENT INDICATION to the ng-eNB, and DL CP Security Information is included.

For test case 2, the AMF sends CONNECTION ESTABLISHMENT INDICATION to the ng-eNB, and DL CP Security Information is not included.

Expected format of evidence:

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

4.2.2.8 Security in PDU session establishment procedure

4.2.2.8.1 Validation of S-NSSAIs in PDU session establishment request

Requirement Name: validation of S-NSSAIs in PDU session establishment request

Requirement Reference: TS 24.501 [5], clause 5.4.5.2.5

Requirement Description:"

13) if the Request type IE is set to "initial request" and the S-NSSAI IE contains an S-NSSAI that is not allowed by the network, then the AMF shall send back to the UE the 5GSM message which was not forwarded as specified in subclause 5.4.5.3.1 case e) or case f);" as specified in TS 24.501 [5], clause 5.4.5.2.5.

Threat References: TR 33.926 [6], clause K.2.X, Incorrect Validation of S-NSSAIs

Test Case:

Test Name: TC_VALIDTATION_SNSSAI_IN_PDU_REQUEST

Purpose:

Verify that S-NSSAIs which are not within Allowed NSSAI list are not accepted by the AMF under test in PDU session establishment procedure.

Pre-Conditions:

Test environment with UE, UDM, SMF and NSSAAF, which may be simulated.

The tester configures UDM with an S-NSSAI that require Network Slice-Specific Authentication and Authorizationin in UE's subscription information.

-AMF

Capability:

Ability to support Network Slice Specific Authentication and Authorization scenario.

Execution Steps

A. Test Case 1

1) The UE sends the S-NSSAI that require NSSAA to the AMF under test using registration request message.

2) After receiving the NSSAA request from the AMF, the NSSAAF sends EAP success to AMF.

3) The UE sends PDU session establishment request to the AMF with the S-NSSAI.

B. Test Case 2

1) The UE sends the S-NSSAI that require NSSAA to the AMF under test using registration request message.

2) After receiving the NSSAA request from the AMF, the NSSAAF sends EAP failure to AMF.

3) The UE sends PDU session establishment request to the AMF with the S-NSSAI.

Expected Results:

For test case 1, the AMF continues the PDU session establishment procedure by sending a Nsmf_PDUSession_CreateSMContext Request to the SMF.

For test case 2, the AMF aborts the PDU session establishment procedure by sending back the 5GSM message to the UE.

Expected format of evidence

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

4.2.2.9 Network Slice Specific Authentication and Authorization

4.2.2.9.1 NSSAA revocation

Requirement Name: NSSAA revocation

Requirement Reference: TS 33.501 [7], clause 16.5

Requirement Description: " If no S-NSSAI is left in Allowed NSSAI for an access after the revocation, and no Default NSSAI can be provided to the UE in the Allowed NSSAI or a previous NSSAA failed for the Default NSSAI over this access, then the AMF shall execute the Network-initiated Deregistration procedure for the access as described in subclause 4.2.2.3.3 in TS 23.502 [8], and it shall include in the explicit De-Registration Request message the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value. "

as specified in TS 33.501[7], clause 16.5

Threat References: TR 33.926, clause K.2.X

Test Case:

Test Name: TC_NSSAA_REVOCATION

Purpose:

Verify that AMF deregisters UE when, after slice specific authorization revocation, there is no allowed NSSAI or Default NSSAI that can be used by UE.

Pre-Conditions:

Test environment with UE. The UE may be simulated.

The AMF under test is configured with one S-NSSAI in the Allowed NSSAI and no default S-NSSAI.

Execution Steps

A message requesting the AMF under test to revoke the authorization of the S-NSSAI in the Allowed NSSAI is simulated and sent the AMF under test.

Expected Results:

The Deregistration Request message is sent by the AMF under test to the UE.

Expected format of evidence:

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

NOTE 1: This test case is only applicable to AMF supporting Network Slice Specific Authentication and Authorization.

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

4.2.3.4 Authentication and authorization

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

4.2.3.5 Protecting sessions

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

4.2.3.6 Logging

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

4.2.4 Operating Systems

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

4.2.5 Web Servers

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

4.2.6 Network Devices

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

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

4.3.1 Introduction

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

4.3.2 Technical baseline

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

4.3.3 Operating systems

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

4.3.4 Web servers

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

4.3.5 Network devices

There are no AMF-specific additions to clause 4.3.6 of TS 33.117 [3].

4.3.6 Network functions in service-based architecture

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

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

There are no AMF-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	Fixing the message names	16.1.0
2019-12	SA#86	SP-191138	0004	1	F	Corrections for clean-up and alignment	16.1.0
2020-03	SA#87E	SP-200136	0005	1	B	New test case on NAS integrity protection	16.2.0
2020-07	SA#88E	SP-200358	0006	1	F	Clarification on the test case on synchronization failure handling	16.3.0
2020-07	SA#88E	SP-200358	0007	1	F	Clarification on the test case on RES verification failure handling	16.3.0
2020-12	SA#90e	SP-201004	0008	-	F	Reference of general SBA/SBI aspect in 33.512	16.4.0
2021-03	SA#91e	SP-210117	0009	-	F	Correction of incomplete test cases	16.5.0
2021-06	SA#92e	SP-210440	0010	-	B	CR to include R-16 feature of AMF to 33.512	17.0.0
2021-09	SA#93e	SP-210844	0013	-	F	Add reference to TS 33.512	17.1.0
2021-12	SA#94e	SP-211370	0015	-	A	AMF - Expected result for test case not defined in the specifications	17.2.0
2021-12	SA#94e	SP-211370	0017	-	A	AMF - NAS protection algorithm selection in AMF change	17.2.0
2021-12	SA#94e	SP-211370	0018	1	F	33.512 – Alignment with TS 33.501 Rel-17	17.2.0
2021-12	SA#94e	SP-211371	0019	-	F	AMF - NAS NULL integrity protection clarifications	17.2.0
2021-12	SA#94e	SP-211370	0021	-	A	AMF - precondition bidding down prevention in Xn-handover test	17.2.0
2022-03	SA#95e	SP-220217	0022	1	F	Clarification on origination of the Rel17 SCAS test cases in AMF	17.3.0

History

Document history		
V17.3.0	May 2022	Publication