**3GPP TSG-SA3 Meeting #111 *S3-23xxxx***

**Berlin, Germany, 22 - 26 May 2023**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.512** | **CR** | **XXXX** | **rev** | **-** | **Current version:** | **17.3.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | SCAS release reference corrections |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_Ph2 |  | ***Date:*** | 2023-05-22 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | SA3 has been adding the release numbers explicitly to any of the references pertaining to the network function targeted by the SCAS work, for example reference 2 in TS 33.511. This is because the SCAS work has always been one "release late" since it is challenging to develop the SCAS requirements and tests in parallel to targeted new features within the same release timeline. The references have not been regularly updated and some SCAS specifications include more than one reference to the same specification, for example references 2 and 7 in TS 33.512. This practice is neither future proof nor it is documented anywhere. Furthermore, for SCAS evaluation of network products, this dependency on previous releases in SCAS documents turned out to be not very useful anyway. This issue has been discussed several times in previous SA3 meetings and the proposed resolution is documented in [S3-231050](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_110_Athens/docs/S3-231050.zip). |
|  |  |
| ***Summary of change:*** | Removal of the release number from the relevant references and minor reformulations to avoid verbatim content copies from other specifications |
|  |  |
| ***Consequences if not approved:*** | Unnecessary dependencies on previous releases and risk for confusion on scope of SCAS specifications |
|  |  |
| ***Clauses affected:*** | 2, 4.2.2.1.1, 4.2.2.1.2, 4.2.2.1.3, 4.2.2.3.1, 4.2.2.3.2, 4.2.2.3.3, 4.2.2.4.1, 4.2.2.4.2, 4.2.2.5.1, 4.2.2.6.1, 4.2.2.7, 4.2.2.8.1, 4.2.2.9.1 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\* Start of Changes\*\*\*\*

# 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 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] void

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

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

\*\*\*\* Next Changes\*\*\*\*

##### 4.2.2.1.1 Synchronization failure handling

*Requirement Name*: Synchronization failure handling

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

*Requirement Description*: As specified in TS 33.501 [2] clause 6.1.3.3.2, 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 of TS 33.501 [2].

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).

*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.

\*\*\*\* Next Changes\*\*\*\*

##### 4.2.2.1.2 RES\* verification failure handling

*Requirement Name*: RES\* verification failure handling

*Requirement Reference:* TS 33.501 [2], clause 6.1.3.2.2

*Requirement Description*:

As specified in TS 33.501 [2], clause 6.1.3.2.2, the SEAF is expected to proceed with step 10 in Figure 6.1.3.2-1 of TS 33.501 [2] 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 is expected to 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 is expected to 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 is expected to either reject the authentication to the UE or initiate an Identification procedure with the UE.

*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.

\*\*\*\* Next Changes\*\*\*\*

##### 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 [2], clause 6.16.4. , TS 23.501 [8], clause 5.31.3.

*Requirement Description*: As specified in TS 33.501 [2], clause 6.16.4, 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 is expected to only send such a Registration Reject message once NAS security has been established between the AMF and the UE; and

- the UE is expected to only act upon such Registration Reject message if received integrity protected and if UE has verified the integrity of the Registration Reject message successfully.

In addition, 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.

*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.

\*\*\*\* Next Changes\*\*\*\*

##### 4.2.2.3.1 Replay protection of NAS signalling messages

*Requirement Name:* Replay protection of NAS signalling messages

*Requirement Reference:* TS 33.501 [2], clause 5.5.2.

*Requirement Description:* The AMF is expected to 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 NASsignalling 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.

\*\*\*\* Next Changes\*\*\*\*

##### 4.2.2.3.2 NAS NULL integrity protection

*Requirement Name*: NAS NULL integrity protection

*Requirement Reference:* TS 33.501 [2], clause 5.5.2

*Requirement Description*: NIA0 is expected to be disabled in AMF in the deployments where support of unauthenticated emergency session is not a regulatory requirement as specified in TS 33.501 [2], 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 KAMF 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 KAMF 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.

\*\*\*\* Next Changes\*\*\*\*

##### 4.2.2.3.3 NAS integrity algorithm selection and use

*Requirement Name*: NAS integrity algorithm selection and use

*Requirement Reference:* TS 33.501 [2], clause 6.7.1

*Requirement Description*: The AMF is expected to 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 TS 33.501 [2]). The AMF is expected to select the NAS algorithm which have the highest priority according to the ordered lists as specified in TS 33.501 [2], 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.

\*\*\*\* Next Changes\*\*\*\*

##### 4.2.2.4.1 Bidding down prevention in Xn-handover

*Requirement Name*: Bidding down prevention in Xn-handovers

*Requirement Reference:* TS 33.501 [2], clause 6.7.3.1

*Requirement Description*: In the Path-Switch message, the target gNB/ng-eNB is expected to send the UE's 5G security capabilities received from the source gNB/ng-eNB to the AMF. The AMF is expected to 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 is expected to send its locally stored 5G security capabilities of the UE to the target gNB/ng-eNB in the Path-Switch Acknowledge message. The AMF is expected to support logging capabilities for this event and may take additional measures, such as raising an alarm; as specified in TS 33.501 [2], 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.

\*\*\*\* Next Changes\*\*\*\*

##### 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 [2], 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 is expected to indicate the selected algorithm to the UE as defined in Clause 6.9.2.3.3 of TS 33.501 [2] for N2-Handover (i.e., using NAS Container) and Clause 6.9.3 of the same document 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 TS 33.501 [2]); as specified in TS 33.501 [2], 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.

\*\*\*\* Next Changes\*\*\*\*

##### 4.2.2.5.1 5G-GUTI allocation

*Requirement Name*: 5G-GUTI allocation

*Requirement Reference:* TS 33.501 [2], clause 6.12.3

*Requirement Description*: As specified in TS 33.501 [2], clause 6.12.3, a new 5G-GUTI is expected to 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 is recommended to 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 is expected to send a new 5G-GUTI to the UE. This new 5G-GUTI is expected to 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..

*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.

\*\*\*\* Next Changes\*\*\*\*

##### 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*: For the case where 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 is expected to 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.

\*\*\*\* Next Changes\*\*\*\*

#### 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 is expected to 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 is expected to fail the RRC Re-establishment.

In case of authentication failure, the NG-RAN node and the AMF is recommended to 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:** Toverify 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.

\*\*\*\* Next Changes\*\*\*\*

##### 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*: As specified in TS 24.501 [5], clause 5.4.5.2.5, 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 is expected to 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) of TS 24.501 [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.

\*\*\*\* Next Changes\*\*\*\*

##### 4.2.2.9.1 NSSAA revocation

*Requirement Name*: NSSAA revocation

*Requirement Reference:* TS 33.501 [2], 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 is expected to 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 is expected to 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[2], 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.

\*\*\*\* End of Changes\*\*\*\*