**3GPP TSG-SA3 Meeting #123 S3-253019**

Goteborg, Sweden, 25 – 29 August 2025

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.512** | **CR** | **Draft CR** | **rev** | **-** | **Current version:** | **19.0.0** |  |
|  | | | | | | | | |
| *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:*** | Living document TS 33.512 SCAS | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon, China Telecom, CAICT, BSI (DE), Montsecure | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2025-08-18 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-20 |
|  | *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 can be 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:*** | | S3-253032  According to GSMA NESASG review, several corrections to 33.512 are needed.  S3-252697-r1  The expected result for test A is :*For Test A, the SEAF/AMF may initiate new authentication towards the UE*.  "May" expresses that something is possible but not certain. It causes uncertainty in the expected result.  S3-252704  Test case C of TC\_SYNC\_FAIL\_SEAF\_AMF is ambiguous and does not indicate whether the Authentication Failure message should be sent with security protection enabled or not.  Additionally, the expected results section of TC\_SYNC\_FAIL\_SEAF\_AMF is ambiguous and does not allow for automated tests as it is hard to detect whether an AMF does not respond or process a message.  Furthermore, the specification states that the AUSF should initiate a new authentication procedure with the UE after receiving its response from the UDM instead of this being optional (applicable to test case A).  S3-253025  The requirement of the initial NAS message retransmission was not yet covered by any AMF SCAS test case. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | S3-253032  1.Complementing new references, terms, abbreviations, and missing sub-headings.  2.Replacing modal verbs with normative texts.  3.Correcting format and font issues.  4.Correcting the reference to the threat in TR 33.926.  S3-252697-r1  Remove "may" from the expected result for test A.  S3-252704  Split up test case C of TC\_SYNC\_FAIL\_SEAF\_AMF into two subtests of which one tests a security protected message and the other tests a plain message. Additionally, specific timeout values are added to the test case steps and expected results section of TC\_SYNC\_FAIL\_SEAF\_AMF such that this test case can be automated without having to check the behaviour of the AMF from the logs.  S3-253025  Adds a test case which verifies that the AMF requests and uses the retransmitted (and protected) initial NAS message. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | S3-253032  Low quality of SCAS documents.  S3-252697-r1  There is uncertainty in the expected result for test A.  S3-252704  The definition of TC\_SYNC\_FAIL\_SEAF\_AMF is loose and might cause different testers to execute the test differently (e.g. one tester execution the test with a security protected message while the other executes it with a plain message). This might lead to the test results being inconsistent depending on the implementation of the test case.  S3-253025  If the AMF does not use the retransmitted initial NAS message and simply proceeds with the registration procedure based on the original Registration Request, then the AMF could be vulnerable to Bidding Down attacks. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 3, 4.2.2.1.1, 4.2.2.1.3, 4.2.2.1.4, 4.2.2.3.1, 4.2.2.3.2, 4.2.2.3.3, 4.2.2.3.X(new), 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:*** | | The merge of S3-253032,S3-252697-r1, S3-252704, S3-253025 | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 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)".

[10] 3GPP TS 29.509: "5G System; Authentication Server Services".

[11] 3GPP TR 33.916: "Security Assurance Methodology (SECAM) for 3GPP network products".

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 1st CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 2nd CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 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].

**Network Function:** As defined in TS 23.501 [8].

**Network product:** As defined in TR 33.916 [11].

**Network product class:** As defined in TR 33.916 [11].

**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 [11].

## 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].

HTTP2 Hypertext Transfer Protocol Version 2

JSON JavaScript Object Notation

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 2nd CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 3rd CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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 tester triggers the UE to perform a registration procedure up until the point where the UE receives a NAS Authentication Request message from the network.

2) The tester configures the UE to send an Authentication Failure message to the SEAF/AMF with *synchronisation failure* (AUTS), after receiving the NAS authentication request message.

3) Immediately after sending the Authentication Failure message, the UE starts timer T3520 as specified in section 5.4.1.3.7 of TS 24.501.

4) The SEAF/AMF sends a Nausf\_UEAuthentication\_Authenticate Request message with a "*synchronisation failure indication*" to the AUSF.

5) 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 of T3520.

Test B:

1) The tester triggers the UE to perform a registration procedure up until the point where the UE receives a NAS Authentication Request message from the network.

2) The tester configures the UE to send an Authentication Failure message to the SEAF/AMF with *synchronisation failure* (AUTS), after receiving the NAS Authentication Request message.

3) Immediately after sending the Authentication Failure message, the UE starts timer T3520 as specified in section 5.4.1.3.7 of TS 24.501.

4) The SEAF/AMF sends a Nausf\_UEAuthentication\_Authenticate Request message with a "*synchronisation failure indication*" to the AUSF.

5) The tester configures the AUSF in a way, that it does not send a Nausf\_UEAuthentication\_Authenticate Response message to the SEAF/AMF before timeout of T3520.

Test C: (unsolicited synchronisation failure; not security protected)

1) The tester triggers a UE to perform a Registration Procedure. The tester keeps track of the RAND value sent by the SEAF/AMF to the UE in the Authentication Request during the procedure.

2) While the UE is registered, the tester sends an unsolicited Authentication Failure message with \_synchronisation failure indication\_ to the SEAF/AMF. The AUTS value in the synchronisation failure indication message is computed using the RAND value from step 1. The Authentication Failure message must not be security protected, e.g. it is sent in a plain 5GS NAS message.

3) Immediately after sending the Authentication Failure message, the UE starts timer T3520 as specified in section 5.4.1.3.7 of TS 24.501.

Test D: (unsolicited synchronisation failure; security protected)

1) The tester triggers a UE to perform a registration procedure. The tester keeps track of the RAND value sent by the SEAF/AMF to the UE in the Authentication Request during the procedure.

2) While the UE is registered, the tester sends an unsolicited Authentication Failure message with \_synchronisation failure indication\_ to the SEAF/AMF. The AUTS value in the synchronisation failure indication message is computed using the RAND value from step 1. The Authentication Failure message must be security protected, e.g. it is sent in a security protected 5GS NAS message using the security context set up in step 1.

3) Immediately after sending the Authentication Failure message, the UE starts timer T3520 as specified in section 5.4.1.3.7 of TS 24.501.

**Expected Results:**

Test A and Test B: 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 A, the SEAF/AMF initiates new authentication towards the UE before the timer T3520 runs out.

- For Test B, the SEAF/AMF does not send any new authentication request to the UE while timer T3520 is running.

Test C and Test D: The UE does not receive an Authentication Request from the SEAF/AMF while timer T3520 is running. Additionally, the SEAF/AMF does not send a Nausf\\_UEAuthentication\\_Authenticate Request message with a "\_synchronisation failure indication\_" to the AUSF.

**Expected format of evidence:**

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 3rd CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 4th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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 only sends such a Registration Reject message once NAS security has been established between the AMF and the UE; and

- the UE only acts upon such Registration Reject message if received integrity protected and if UE has verified the integrity of the Registration Reject message successfully.

NOTE 1: Void

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*: TR 33.926 [6], clause K.2.8, NAS based redirection from 5GS to EPS in 5G CIoT

*Test Case*:

**Test Name:** TC\_AMF\_REDIRECTION\_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: Void

**Procedure and execution steps:**

**Pre-Conditions:**

- AMF under test supports the security handling in CIoT.

- Test environment with a CIoT 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. The tester triggers the UE to initiate an 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:**

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

##### 4.2.2.1.4 NAS integrity failure

*Requirement Name*: NAS integrity failure

*Requirement Reference:* TS 33.501 [2] clause 6.4.3.3.

*Requirement Description*: In case of failed integrity check (i.e. faulty or missing NAS-MAC) is detected after the start of NAS integrity protection, the concerned message shall be discarded except for some NAS messages specified in TS 24.501.

*Threat Reference*: TBD

*Test Case*:

**Test Name:** TC\_AMF\_NAS\_INTEGRITY\_FAILURE

**Purpose:**

Verify that AMF under test drops messages in case the NAS integrity fails or is missing.

**Procedure and execution steps:**

**Pre-Conditions:**

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

- AMF under test is connected in emulated/real network environment.

- NAS Integrity algorithm different than NIA0 is used.

**Execution Steps**

**Test case 1 (wrong NAS-MAC):**

1. The tester triggers the UE to initiate an initial registration procedure with the AMF.

2. The AMF sends the Security Mode Complete message to the UE.

3. After the Security Mode Complete message, send a NAS message from the UE to the AMF with a wrong NAS-MAC. The message used shall not be an exception in TS 24.501 [5].

**Test case 2 (missing NAS-MAC):**

1. The tester triggers the UE to initiate an initial registration procedure with the AMF.

2. The AMF sends the Security Mode Complete message to the UE.

3. After the Security Mode Complete message, send a NAS message from the UE to the AMF removing the NAS-MAC field. The message used shall not be an exception in TS 24.501 [5].

**Expected Results:**

In both test cases, the AMF discards the NAS messages.

**Expected format of evidence:**

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 4th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 5th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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 supports 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 Security Mode Command 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 replay the captured NAS Security Mode Complete message.

4. The tester shall check whether the replayed NAS Security Mode Complete message was not processed by the AMF by capturing traffic over the N1 interface to see if no corresponding response message was sent by the AMF. If applicable, AMF application logs could be checked for the rejection of the replayed NAS Security Mode Complete message.

**Expected Results:**

The NASsignalling messages sent from the UE to the AMF over N1 interface are replay protected.

**Expected format of evidence:**

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 5th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 6th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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 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.

**Procedure and execution steps:**

**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 tester triggers the UE to initiate 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 tester triggers the UE to initiate 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 the 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, packet captures or application log files 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 [2], clause 6.7.1

*Requirement Description*: The AMF initiates 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 selects 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.

**Procedure and execution steps:**

**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 is configured on the AMF under test.

- The tester is able to configure the list of ordered NAS integrity algorithms on the AMF under test.

**Execution Steps:**

1) The tester triggers the UE to send a Registration Request with Initial Registration type to the AMF under 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.

4) The tester changes the default order of the list of ordered NAS integrity algorithms on the AMF to one other valid configuration and repeats step 1-3 once.

**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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 6th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 7th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.3.X NAS Protection of initial NAS message

*Requirement Name*: Protection of initial NAS message

*Requirement Reference:* TS 33.501 [2], clause 6.4.6

*Requirement Description*: The UE sends the NAS Security Mode Complete message to the network in response to a NAS Security Mode Command message. The NAS Security Mode Complete message is ciphered and integrity protected. Furthermore the NAS Security Mode Complete message includes the complete initial NAS message in a NAS Container if either requested by the AMF or the UE sent the initial NAS message unprotected. The AMF uses the complete initial NAS message that is in the NAS container as the message to respond to, as stated in TS 33.501, clause 6.4.6, step 4.

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

*Test Case:*

**Test Name:** TC\_AMF\_NAS\_INITIAL\_MESSAGE\_RETRANSMISSION

**Purpose:**

Verify that the AMF requests the security protected retransmission of the initial NAS message from the UE in the NAS Security Mode Complete message and does proceed with the registration procedure based on the retransmitted, protected NAS Registration Request message.

**Pre-Conditions:**

- AMF network product is connected in emulated/real network environment.

- UE does not have a 5G NAS security context

- The Tester is able to intercept and modify the NAS signalling packets sent between UE and AMF over the N1 interface.

**Execution Steps:**1. The tester triggers the UE to conduct an initial registration procedure.

2. The tester intercepts the unprotected Registration Request message sent from the UE to the AMF and modifies either the Requested NSSAI or Registration Type.

3. The AMF initiates the Security Mode Command Procedure after receiving the unprotected Registration Request (initial NAS message) from the UE. The AMF sets the RINMR bit (Retransmission of the initial NAS message requested) to 1 in the Security Mode Command message sent to the UE.

4. The UE sends a Security Mode Complete message with a retransmitted and protected Registration Request message to the AMF.

5. The tester observers the AMFs consecutive behaviour.

**Expected Results:**

The RINMR bit is set to 1 in the Security Mode Command message sent from the AMF to the UE.

The AMFs consecutive messages (e.g. NSSAI modified: Nnssf\_NSSelection\_Get or Nudm\_SDM\_Get; Registration Type modified: Nudm\_UECM\_Registration; for Emergency Registration: Nsmf\_PDUSession\_CreateSMContext) are based on the contents of the retransmitted and protected Registration Request message of the UE.

**Expected format of evidence:**

Evidence suitable for the interface, e.g., packet captures of the N1 interface or application log files of the AMF containing the operational results.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 7th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 8th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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 sends the UE's 5G security capabilities received from the source gNB/ng-eNB to the AMF. The AMF verifies 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 sends its locally stored 5G security capabilities of the UE to the target gNB/ng-eNB in the Path-Switch Acknowledge message. The AMF supports 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.

**Procedure and execution steps:**

**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**

1) 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.

2) The tester captures the Path-Switch Acknowledge message sent by AMF under test to the target gNB.

3) The tester examines the AMF log regarding the capability mismatch.

**Expected Results:**

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 log entry shows that the capability mismatch is logged.

**Expected format of evidence**

Evidence suitable for the interface, e.g., Screenshot, packet captures and application log file 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 [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 indicates 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.

**Procedure and execution steps:**

**Pre-Conditions:**

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

- The ordered lists of NAS algorithms are configured such that the algorithms selected by the AMF under test are different from the ones received from the source AMF.

**Execution Steps**

Test case 1: N2-Handover

1) 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.

2) The tester captures the NGAP HANDOVER REQUEST message containing the NASC IE (NAS Container) sent by the AMF under test to the gNB.

Test case 2: Mobility registration update

1) The AMF under test receives the UE security capabilities and the NAS algorithms used by the source AMF from the source AMF.

2) The AMF under test selects the NAS algorithms which have the highest priority according to the ordered lists.

**Expected Results:**

For Test case 1, the NASC IE of the captured NGAP HANDOVER REQUEST message sent by the AMF under test to the gNB 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, packet captures or application log files containing the operational results.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 8th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 9th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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 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 sends a new 5G-GUTI to the UE. This new 5G-GUTI is 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: Void

*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.

**Procedure and execution steps:**

**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 or perform a new Registration Procedure with the UE for each corresponding test case..

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 (triggered by the tester), 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 (triggered by the tester), 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 (triggered by the tester), the AMF sends a new 5G-GUTI to the UE.

Test case 4:

The AMF under test is triggered by the tester 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, packet captures or application log files containing the operational results.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 9th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 10th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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 returns 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.

**Procedure and execution steps:**

**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 tester triggers the UE to send the following sets of UE security capabilities to the AMF under test using registration request messages:

1) no 5GS encryption algorithms (all bits zero)

2) no 5GS integrity algorithms (all bits zero)

3) mandatory 5GS encryption algorithms not supported

4) mandatory 5GS integrity algorithms not supported

**Expected Results:**

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

**Expected format of evidence**

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 10h CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 11th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 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 fails 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:** Toverify that the verification of RRC Reestablishment is applied correctly.

**Procedure and execution steps:**

**Pre-Conditions:**

- AMF under test is able to support the CIoT scenario.

- 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:**

Test Case A

1) The tester triggers the UE to send the RRC Connection Reestablishment Request message to the ng-eNB.

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

Test Case B

1) The tester triggers the UE to send 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 A, the AMF sends CONNECTION ESTABLISHMENT INDICATION to the ng-eNB, and DL CP Security Information is included.

For test case B, 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, packet captures or application log files containing the operational results.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 11th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 12th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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 sends 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.2.10.1, Incorrect Validation of S-NSSAIs

*Test Case*:

**Test Name:** TC\_VALIDATION\_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.

**Procedure and execution steps:**

**Pre-Conditions:**

- AMF under test supports the Network Slice Specific Authentication and Authorization scenario.

- 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**

Test Case A

1) The tester triggers the UE to send 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.

Test Case B

1) The tester triggers the UE to send 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 A, the AMF continues the PDU session establishment procedure by sending a Nsmf\_PDUSession\_CreateSMContext Request to the SMF.

For test case B, 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, packet captures or application log files containing the operational results.

List of allowed S-NSSAIs.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 12th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 13th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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 executes the Network-initiated Deregistration procedure for the access as described in subclause 4.2.2.3.3 in TS 23.502 [8], and it includes 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 [6], clause K.2.10.X, Failure to deregister UE after NSSAA revocation

*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.

**Procedure and execution steps:**

**Pre-Conditions:**

- AMF under test supports Network Slice Specific Authentication and Authorization.

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

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

- The UE is registered at the AMF using the specific S-NSSAI configured in the AMF.

**Execution Steps**

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

**Expected Results:**

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

The Deregistration Request message includes the list of rejected S-NSSAIs, each of them with the appropriate rejection cause value.

**Expected format of evidence:**

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

NOTE 1: Void

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*