**3GPP TSG-SA3 Meeting #123 S3-253023**

Goteborg, Sweden, 25 – 29 August 2025

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.216** | **CR** | **Draft CR** | **rev** | **-** | **Current version:** | **19.1.0** |  |
|  |
| *For* ***HE******LP*** *on using this form: comprehensive instructions can be found at http://www.3gpp.org/Change-Requests.* |
|  |

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

|  |
| --- |
|  |
| ***Title:***  | Living document for TS 33.216 |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon,BSI (DE) |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5GA |  | ***Date:*** | 2025-07-29 |
|  | D |  |  |  |
| ***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 canbe found in 3GPP TR 21.900. | *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:*** | S3-253023Correction of double test case naming and correction of referencesRemoval of NIA0 and EIA0 to align with baselineS3-252702Including emergency calls in test steps according to requirement description |
|  |  |
| ***Summary of change:*** | S3-253023Correction of test naming and references Removal of NIA0 and EIA0 to align with baselineS3-252702Adapting test steps according to requirements |
|  |  |
| ***Consequences if not approved:*** | S3-253023Non-standard tests remain and test automation would be affectedS3-252702differing test steps from requirements could lead to wrong test results |
|  |  |
| ***Clauses affected:*** | 4.2.2.1.3, 4.2.2.1.7,4.2.2.1.9, 4.2.2.1.13, 4.2.2.1.16, 4.2.2.1.19 |
|  |  |
|  | **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 merger of S3-253023,S3-252702 |

\*\*\*\*\*\*\*\*\*\* START OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*

4.2.2.1.3 User plane data ciphering and deciphering at the eNB

*Requirement Name:* User plane data ciphering and deciphering at eNB

Requirement Reference: TS 33.401 [3], clause 5.3.4

*Requirement Description:* "The eNB shall cipher and decipher user plane packets between the Uu reference point and the S1/X2 reference points." as specified in TS 33.401 [3], clause 5.3.4.

*Threat References:* TR 33.926 [4], clause C.2.2.3 – User plane data ciphering and deciphering at eNB.

*Test Case:*

**Test Name:** TC-DATA-CIP-eNB-Uu

**Purpose:** Toverify that the user data packets are confidentiality protected over the air interface.

**Pre-Condition:**

- The eNB network product is connected in emulated/real network environments. UE and the MME may be simulated,

- The tester can capture the messages via the air interface.

- The tester enables the user plane ciphering protection and ensure EEA0 is not used.

**Execution Steps:**

1. The UE sends an attach request to the MME.

2. The MME sends a KeNB and the UE security capability to the eNB.

3. eNB selects an algorithm and sends AS SMC to the UE,

4. eNB receive AS SMP from the UE.

**Expected Results:**

User plane packets sent by the eNB after eNB sending AS SMC is ciphered.

**Expected format of evidence:**

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

\*\*\*\*\*\*\*\*\*\* END OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\* START OF 2nd CHANGE \*\*\*\*\*\*\*\*\*\*

4.2.2.1.7 The selection of EIA0

*Requirement Name*: The selection of EIA0

*Requirement Reference:* TS 33.401 [3], clause 5.1.4.2

*Requirement Description*: " EIA0 is only allowed for unauthenticated emergency calls " as specified in TS 33.401 [3], clause 5.1.4.2.

*Threat References*: TBA

*Test Case*:

**Test Name:** TC\_ENB\_SELECTION\_OF\_EIA0

**Purpose:**

Verify that AS NULL integrity algorithm is selected correctly.

**Pre-Conditions:**

* Test environment with a UE. The UE may be simulated.
* The vendor provides documentation describing how EIA0 is disabled or enabled. EIA0 is enabled at the eNB.

**Execution Steps**

Positive:

1) The tester triggers the UE to initiate an emergency registration.

2) The eNB receives a UE security capability only containing EIA0 from S1 context setup message.

3) The eNB sends AS SMC to the UE.

Negative:

1) The tester triggers the UE to initiate a non-emergency registration.

2) The eNB receives a UE security capability that contains EIA0 and other integrity algorithm(s).

3) The eNB sends AS SMC to the UE.

**Expected Results:**

EIA0 is only selected in the Positive test.

**Expected format of evidence:**

Sample copies of the log files. List of algorithms configured in eNB and UE.

\*\*\*\*\*\*\*\*\*\* END OF 2nd CHANGE \*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\* START OF 3rd CHANGE \*\*\*\*\*\*\*\*\*\*

4.2.2.1.9 AS Security Mode Command Procedure

*Requirement Name*: AS integrity algorithm selection

*Requirement Reference:* TS 33.401 [3], clause7.2.4.5

*Requirement Description*: The eNB shall protect the SECURITY MODE COMMAND message with the integrity algorithm, which has the highest priority according to the ordered lists.

*Threat References*: TBA

*Test Case*:

**Test Name:** TC\_ENB\_AS\_SMC\_INTEGRITY\_PROTECTION

**Purpose:**

Verify that AS integrity protection algorithm is selected and applied correctly.

**Pre-Conditions:**

Test environment with UE. UE may be simulated.

**Execution Steps:**

The eNB sends the SECURITY MODE COMMAND message. The UE replies with the SECURITY MODE COMPLETE message.

**Expected Results:**

1. The eNB has selected the integrity algorithm which has the highest priority according to the ordered lists and is contained in the UE EPS security capabilities. The eNB checks the message authentication code on the SECURITY MODE COMPLETE message.

2. The MAC in the SECURITY MODE COMPLETE is verified, and the AS integrity protection algorithm is selected and applied correctly.

**Expected format of evidence:**

Snapshots containing the result.

\*\*\*\*\*\*\*\*\*\* END OF 3rd CHANGE \*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\* START OF 4th CHANGE \*\*\*\*\*\*\*\*\*\*

4.2.2.1.13 Map a UE NR security capability

*Requirement Name:* Map a UE NR security capability

*Requirement Reference:* TS 33.401 [3], clause E.3.10.2

*Requirement Description:* " The MeNB that does not have the UE NR security capabilities shall create them as follow:

- Set the support of NEA0, 128-NEA1, 128-NEA2, 128-NEA3, 128-NIA1, 128-NIA2, 128-NIA3 to the same as EEA0, 128-EEA1, 128-EEA2, 128-EEA3, 128-EIA1, 128-EIA2, 128-EIA3 respectively; and

- Set the rest of the bits to 0." as specified in TS 33.401 [3], clause E.3.10.2.

*Threat References:* TBA

*Test Case:*

**Test Name:** TC\_MAP\_NR\_SEC\_CAP

**Purpose:** To verify that the eNB creates mapped UE NR security capabilities.

**Pre-Condition:**

- The eNB and gNB network products are connected in the test environment. The gNB may be simulated.

- Tester has access to trigger dual connection to a gNB.

- The Tester can access to the X2 interface.

**Execution Steps:**

1) The MeNB does not receive UE NR security capabilities from S1 Initial Context Setup Request message.

2) The MeNB sends SN Addition Request Message to the SgNB.

3) The tester checks if the NR security capabilities are included in SN Addition Request Message.

**Expected Results:**

The SN Addition Request Message contains UE NR security capabilities, i.e. NEA0, 128-NEA1, 128-NEA2, 128-NEA3, 128-NIA1, 128-NIA2, 128-NIA3

**Expected format of evidence:**

Evidence suitable for the interface, e.g. Screenshot contains the operation results.

\*\*\*\*\*\*\*\*\*\* END OF 4th CHANGE \*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\* START OF 5th CHANGE \*\*\*\*\*\*\*\*\*\*

4.2.2.1.16 Integrity protection of user data between the UE and the eNB

*Requirement Name:* Integrity protection of user data between the UE and the eNB.

*Requirement Reference:* TS 33.401 [3], clause 5.1.4.1

*Requirement Description:* *"*User plane packets between the eNB and the UE may be integrity protected on the Uu interface.*" in clause 5.1.4.1*

*Threat References:* TBD

*Test Case:*

**Test Name:** TC-UP-DATA-INT\_eNB

**Purpose:** Toverify that the user data packets are integrity protected over the Uu interface.

**Pre-Condition:**

- The eNB network product is connected in emulated/real network environments. UE may be simulated.

- The tester has knowledge of integrity algorithm and integrity protection keys.

- The tester can capture the message via the Uu interface, or can capture the message at the UE.

- The tester enables user plane integrity protection and ensure that EIA0 is disabled at the eNB.

**Execution Steps:**

1. The tester triggers the eNB to send a RRCConnectionReconfiguration message with integrity protection indication "on" to the UE.

2. The tester checks that any user data sent by eNB after sending the RRCConnectionReconfiguration message and while the UE is in active state is integrity protected.

\*\*\*\*\*\*\*\*\*\* END OF 5th CHANGE \*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\* START OF 6th CHANGE \*\*\*\*\*\*\*\*\*\*

4.2.2.1.19 UP IP policy selection in S1 Handover

*Requirement Name:* Select the right UP IP policy in S1 handover.

*Requirement Reference:* TS 33.401 [2] clause 7.3.3

*Requirement Description:* *"* *At an S1-handover, the source MME shall send the UE's UP integrity protection policy and the UE EPS security capability to the target eNB via the target MME. Besides, the source eNB shall also send the UE's UP integrity protection policy if received from the source MME to the target eNB in a source-to-target container. The target eNB shall use the UE capability indicating support of UP IP in EPS together with the UP integrity protection policy received from the MME and ignore the UP integrity protection received in the source-to-target container. If the target eNB does not receive the UP integrity protection policy from the MME, the target eNB shall use the UE capability indicating support of UP IP in EPS together with the UP integrity protection policy received from the source eNB. If both policies from MME and source eNB are absent, but EIA7 in the EPS security capability indicates that the UE supports use of user plane protection with EPC, the eNB shall use locally configured UP integrity protection policy.*" in clause 7.3.3

*Threat References:* TR 33.926 [4], clause C.2.2.6, UP integrity protection policy selection

*Test Case:*

**Test Name:** TC\_UP\_IP\_POLICY\_Selection\_S1\_Handover

**Purpose:** Toverify that the eNB has correct selection on UP IP policy in S1 handover

**Pre-Condition:**

- The target eNB network product is connected in emulated/real network environments. UE, source eNB and MME may be simulated.

- The target eNB locally UP IP is set to NOT NEEDED.

- The tester has knowledge of integrity algorithm and integrity protection keys.

- The tester can capture the message via the Uu interface, or can capture the message at the UE.

**Execution Steps:**

Test Case 1:

1) The tester triggers the source MME to send EPS security capability with EIA7 to the target eNB indicating the UP IP is supported by the UE. Furthermore, the tester triggers the source MME to send a UP IP policy with REQUIRED to the target eNB.

2) The source eNB sends UP IP policy with NOT NEEDED in the source-to-target container to the target eNB.

3) The target eNB sends a RRCConnectionReconfiguration message with integrity protection indication "on" to the UE.

4) The tester checks that any user data sent by the target eNB after sending the RRCConnectionReconfiguration message and before UE enters CM-Idle state is integrity protected.

Test Case 2:

1) The tester triggers the source MME to send EPS security capability with EIA7 to the target eNB indicating the UP IP is supported by the UE. Furthermore, the tester prepares the MME to not send a UP IP policy to the target eNB.

2) The source eNB sends UP IP policy with REQUIRED in the source-to-target container to the target eNB.

3) The target eNB sends a RRCConnectionReconfiguration message with integrity protection indication "on" to the UE.

4) The tester checks that any user data sent by eNB after sending the RRCConnectionReconfiguration message and before UE enters CM-Idle state is integrity protected.

Test Case 3:

1) The tester configures the target eNB to make sure the local UP IP is set to REQUIRED.

2) The tester triggers the source MME to send EPS security capability with EIA7 to the target eNB indicating the UP IP is supported by the UE. Furthermore, the tester prepares the MME to not send a UP IP policy to the target eNB.

3) The source eNB does not send UP IP policy in the source-to-target container to the target eNB.

4) The target eNB sends a RRCConnectionReconfiguration message with integrity protection indication "on" to the UE.

5) The tester checks that any user data sent by eNB after sending the RRCConnectionReconfiguration message and before UE enters CM-Idle state is integrity protected.

**Expected Results:**

For all test cases, any user plane packets sent between UE and eNB over the Uu interface after eNB sending the RRCConnectionReconfiguration message are integrity protected.

**Expected format of evidence:**

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

For each test case: Configuration of UP IP of target eNB, source eNB and UP IP policy sent by MME.

\*\*\*\*\*\*\*\*\*\* END OF CHANGES \*\*\*\*\*\*\*\*\*\*