**3GPP TSG-SA3 Meeting #98 *S3-200335***

**e-meeting, 2-6 March 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.216** | **CR** | **0013** | **rev** | **-** | **Current version:** | **16.2.0** |  |
|  | | | | | | | | |
| *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 | **X** | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Complete the test cases of key refresh at the eNB | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Telecom Italia, NTT DoCoMo | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI16, SCAS\_eNB | | | | |  | ***Date:*** | | | 2020-02-21 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | According to the threat description in paper S3-200188, key reuse at the eNB could be exploited by attackers under different conditions. The current test case in TS 33.216 clause 4.2.2.1.8 only covers one condition which is PDCP COUNT reuse with the same bearer identity and the same KeNB.  However, the other condition that is the RB identity reuse with PDCP COUNT being reset to 0 is not captured yet for testing. The requirement to avoid RB identity reuse was already captured in TS 36.331 clause 5.3.1.2, but a related test case was not defined yet. Hence it is proposed to add a sub-test case in TS 33.216 clause 4.2.2.1.8 to cover the requirement in TS 36.331 clause 5.3.1.2. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Added TS 36.331 in the reference list.  Added the requirement from TS 36.331 clause 5.3.1.2 in TS 33.216 clause 4.2.2.1.8.  Added a new sub-test case (test case 2) in TS 33.216 clause 4.2.2.1.8. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The current test case of key refresh at the eNB does not cover all scenarios which could be exploited by attackers. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 4.2.2.1.8 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **x** |  | Other core specifications | | | | TS/TR 33.926 CR .0031 | | |
| ***affected:*** | |  | **x** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **x** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | | This test is relevant from R8 for the eNB. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 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 TR 33.117 (Release 15): "Catalogue of general security assurance requirements".

[3] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[4] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[x] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.8 Key refresh at the eNB

*Requirement Name*: Key refresh at the eNB

*Requirement Reference:* TS 33.401 [3], clause 7.2.9.1; TS 36.331 [x], clause 5.3.1.2.

*Requirement Description*: "Key refresh shall be possible for KeNB, KRRC-enc, KRRC-int, KUP-int, and KUP-enc and shall be initiated by the eNB when a PDCP COUNTs is about to be re-used with the same Radio Bearer identity and with the same KeNB. " as specified in TS 33.401 [3], clause 7.2.9.1.

Moreover, "The eNB is responsible for avoiding reuse of the COUNT with the same RB identity and with the same KeNB, e.g. due to the transfer of large volumes of data, release and establishment of new RBs. In order to avoid such re-use, the eNB may e.g. use different RB identities for successive RB establishments, trigger an intra cell handover or by triggering a transition from RRC\_CONNECTED to RRC\_IDLE or RRC\_INACTIVE and then back to RRC\_CONNECTED." as specified in TS 36.331 [x], clause 5.3.1.2.

*Threat References*: TR 33.926[4], clause C.2.x.1 – Key reuse for eavesdropping

*Test Case 1*:

**Test Name:** TC\_ENB\_KEY\_REFRESH\_ PDCP\_COUNT

**Purpose:**

Verify that the eNB performs KeNB refresh when PDCP COUNTs are about to wrap around.

**Pre-Conditions:**

The UE may be simulated.

**Execution Steps**

1) The eNB sends AS Security Mode Command message to the UE, and the UE responds with the AS Security Mode Complete message.

2) The UE sends RRC messages or UP messages to the eNB with an increasing PDCP COUNT until the value wraps around.

**Expected Results:**

The eNB triggers an intra-cell handover and takes a new KeNB into use.

**Expected format of evidence:**

Part of log that shows the PDCP COUNT wraping around and the intra-cell handover. This part can be presented, for example, as a screenshot.

*Test Case 2:*

**Test Name:** TC\_ENB\_KEY\_REFRESH\_DRB\_ID

**Purpose:**

Verify that the eNB performs KeNB refresh when DRB-IDs are about to be reused under the following conditions:

* the successive Radio Bearer establishment uses the same RB identity while the PDCP COUNT is reset to 0, or
* the PDCP COUNT is reset to 0 but the RB identity is increased after multiple calls and wraps around.

**Pre-Conditions:**

The UE and MME may be simulated.

**Execution Steps**

1) The eNB sends the AS Security Mode Command message to the UE, and the UE responds with the AS Security Mode Complete message.

2) A DRB is set up.

3) DRB is set up and torn down for multiple times within one active radio connection without the UE going to idle (e.g. by the UE making multiple IMS calls, or by the MME requesting bearer setup and bearer deactivation), until the DRB ID is reused.

**Expected Results:**

Before DRB ID reuse, the eNB takes a new KeNB into use by e.g. triggering an intra-cell handover or triggering a transition from RRC\_CONNECTED to RRC\_IDLE or RRC\_INACTIVE and then back to RRC\_CONNECTED.

**Expected format of evidence:**

Part of log that shows all the DRB identities and the intra-cell handover or the transition from RRC\_CONNECTED to RRC\_IDLE or RRC\_INACTIVE and then back to RRC\_CONNECTED. This part can be presented, for example, as a screenshot.

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