**3GPP TSG-SA3 Meeting #108-e  *draft\_S3-221875-r1***

**e-meeting, 22 – 26 August 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.216** | **CR** | Draft CR | **rev** | **-** | **Current version:** | **16.7.0** |  |
|  | | | | | | | | |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm" \l "_blank)******[LP](http://www.3gpp.org/3G_Specs/CRs.htm" \l "_blank)*** *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 | **X** | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Add a test case in TS 33.216 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | ZTE | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_eNB | | | | |  | ***Date:*** | | | 2022-08-09 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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 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:*** | | As specified in TS 33.401 clause 7.2.4.2.2, in the path-switch message, the target eNB shall send the UE EPS security capabilities received from the source eNB to the MME. The MME shall verify that the UE EPS security capabilities received from the eNB are the same as the UE EPS security capabilities that the MME has stored. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The MME shall verify that the UE EPS security capabilities received from the eNB are the same as the UE EPS security capabilities that the MME has stored. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The bidding down prevention can not be tested correctly for R17 devices. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.2.1.X(new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* 1st CHANGE \*\*\*

##### 4.2.2.1.X Bidding down prevention in X2-handovers when MME store the UE EPS security capabilities

*Requirement Reference:* TS 33.401 [3], clause 7.2.4.2.2

*Requirement Description*: "In the path-switch message, the target eNB shall send the UE EPS security capabilities received from the source eNB to the MME.The MME shall verify that the UE EPS security capabilities received from the eNB are the same as the UE EPS security capabilities that the MME has stored. If there is a mismatch, the MME shall send its locally stored UE EPS security capabilities to the target eNB in the response to the path-switch message. In addition, the MME may log the event and may take additional measures, such as raising an alarm. If the target eNB receives UE EPS security capabilities from the MME, the target eNB shall update the AS security context of the UE with these UE EPS security capabilities." as specified in TS 33.401 [3], clause 7.2.4.2.2."

*Threat References*: TBA

*Test Case*:

**Purpose:**

Verify that bidding down is prevented in X2-handovers.

**Pre-Conditions:**

Test environment with source eNB and target eNB, and the MME may be simulated.

**Execution Steps:**

1).The target eNB sends the path-switch message to the MME with tampered UE's security capabilities.

2). The MME send its locally stored 5G security capabilities of the UE to the target eNB in the Path-Switch Acknowledge message.

3b). The target eNB receives UE's security capabilities from the MME in the Path-Switch Acknowledge message, the target eNB update the AS security context of the UE with security capabilities of the UE received from the MME.

**Expected Results:**

1. The UE EPS security capabilities are in the path-switch message.
2. The target eNB update the AS security context of the UE with security capabilities of the UE received from the MME.

**Expected format of evidence:**

Snapshots containing the result

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