**3GPP TSG-SA3 Meeting #98e *S3-200188***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.926** | **CR** | **0031** | **rev** | **1** | **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:*** | Adding a clause of "Threats related to key reuse" for 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:*** | | The threats related to key reuse are currently not considered in TR 33.926 clause 4.2.2.1.8 for the eNB. Hence it is proposed to add a new clause for such threats. A few editorials also need to be fixed in other clauses. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Added the threats related to key reuse in Annex C.2.  Minor editorial corrections in C.2.2.1, C.2.2.2, C.2.2.3 and C.2.2.4. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No threat reference for the existing test case in TS 33.216 clause 4.2.2.1.8. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | C.2.1, C.2.2.1, C.2.2.2, C.2.2.3, C.2.2.4, new clauses C.2.x, C.2.x.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 the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# C.2 Assets and threats specific to the eNB

# C.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the eNB to be protected are:

- eNB Application;

- Mobility Management data: e.g. subscriber's identities (e.g. IMSI), subscriber keys (i.e. KUPenc, KRRCenc, KRRCint, NH), authentication parameters, address of serving gateway, APN name, data related to mobility management like UE measurements, UE's IP address, etc., QoS and so on, etc.

- User plane data

- The interfaces of eNB to be protected and which are within SCAS scope: for example

- S1 interface

- X2 interface

- Console interface, for local access: local interface on eNB

- OAM interface, for remote access: interface between eNB and OAM system

NOTE 1: The detailed interfaces of the eNB class are described in clause 4, Network Product Class Description of the present document.

- eNB Software: binary code or executable code

NOTE 2: eNB files may be any file owned by a user (root user as well as non root uses), including User account data and credentials, Log data, configuration data, OS files, eNB application, Mobility Management data or eNB Software.

## C.2.2 Threats related to Control plane and User plane

### C.2.2.1 Control plane data confidentiality protection

***-*** *Threat name:* Control plane data confidentiality protection

***-*** *Threat Category:* Tampering data, Information Disclosure, Denial of Service, Masquerading attack.

***-*** *Threat Description:* If the eNB does not provide confidentiality protection for control plane packets on the S1/X2 reference points, then the control plane packets sent between eNBs (eg. inter-eNB handover) and from eNB to MME (eg. handover on MME change) can be manipulated and the eNB can be compromised by attackers to prevent service to legitimate users (eg. Handover failure). Moreover, the UE identifiers, security capabilities, the security algorithms and key materials exchanged between eNBs and eNB-MME can be accessed by the attackers leading to huge security breach. There, any active attacker can perform masquerading by making use of the legitimate users’ UE identifiers to gain access to the network. This threat scenario assumes that the S1, X2 reference points are not within the security environment

***-*** *Threatened Asset:* User account data and credential

### C.2.2.2 Control plane data integrity protection

***-*** *Threat name:* Control plane data integrity protection

***-*** *Threat Category:* Tampering data, Denial of Service

***-*** *Threat Description:* If the eNB does not provide integrity protection for control plane packets on S1/X2 reference points, the control plane packets between eNBs on X2-C and from eNB to MME on S1-MME interface risks being exposed and/or modified. The intruder manipulations on control plane packets will lead to denial of service to legitimate users. This threat scenario assumes that the S1, X2 reference points are not within the security environment

***-*** *Threatened Asset:* Sufficient Processing Capacity

### C.2.2.3 User plane data ciphering and deciphering at eNB

***-*** *Threat name:* User plane data ciphering and deciphering at eNB

***-*** *Threat Category:* Tampering data, Information Disclosure, User tracking, Denial of Service, Man-in-the-middle

***-*** *Threat Description:* If the eNB does not cipher and decipher user plane packets between the Uu reference point and the S1/X2 reference points, then the attackers can manipulate and compromise user packets on Uu, X2-U and S1-U interface to launch Denial of Service as well as Man-in-the middle attack. The attackers can gain access to user identifiers, IMSI, serving network identifiers, location information and can perform user tracking. This threat scenario assumes that the S1, X2 reference points are not within the security environment

***-*** *Threatened Asset:* User account data and credential

### C.2.2.4 User plane data integrity protection

***-*** *Threat name:* User plane data integrity protection

***-*** *Threat Category:* Tampering data, Denial of Service

***-*** *Threat Description:* If the eNB does not handle integrity protection for user plane packets for the S1/X2 reference points then all the uplink/downlink user plane packets over X2-U and S1-U can be attacked and/or manipulated by intruders to launch Denial of Service attack. This threat scenario assumes that the S1, X2 reference points are not within the security environment

***-*** *Threatened Asset:* Sufficient Processing Capacity

## C.2.x Threats related to key reuse

### C.2.x.1 Key reuse for eavesdropping

***-*** *Threat name:* Key reuse for eavesdropping

***-*** *Threat Category:* Information Disclosure

***-*** *Threat Description:* if the keys (KeNB, KRRC-enc, KRRC-int, and KUP-enc) are not refreshed at the eNB, the key stream could be reused by attackers, who can recover the keystream and decrypt the originally established call. The threat of key stream reuse occurs under the following conditions:

- when the PDCP COUNT wraps around and is reused with the same Radio Bearer (RB) identity and with the same KeNB, e.g. due to the transfer of large volumes of data.

- when the PDCP COUNT is reset to 0 but the RB identity and key stay the same (e.g. the successive Radio Bearer establishment uses the same RB identity and keys, or the RB identity is increased after multiple calls and wraps around).

***-*** *Threatened Asset:* User plane data, Mobility Management data

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*