**3GPP TSG-SA3 Meeting #108-e *S3-22XXX***

**e-meeting, 22 - 26 August 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.926** | **CR** | **XXXX** | **rev** | **-** | **Current version:** | **16.5.0** |  |
|  |
| *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:***  | Proposed correction to Annex D on gNB network product class |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G |  | ***Date:*** | 2022-08-25 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***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 canbe 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:*** | In D.1.2, the references number are incorrected.In D.2.2.1, the threat cateory and threat description mention tampering and DoS and description of these respsectively but those are integrity related threats, so should not be included.In D.2.2.2, the exposed threat is a confidentiality threat so should be removed.In D.2.2.3, some of the text relates to integrity based threats, so should be removed.In D.2.7, the test case(s) related to PDCP COUNT wrap were removed (see CR 0023 to TS 33.511) as not applicable and hence it is proposed to remove the threat.  |
|  |  |
| ***Summary of change:*** | Corrected the above issues |
|  |  |
| ***Consequences if not approved:*** | Specification contains error or inconsistencies. |
|  |  |
| ***Clauses affected:*** | D.1.2, D.2.2.1, D.2.2.2, D.2.2.3, D.2.2.7 |
|  |  |
|  | **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 CHANGES \*\*\*\***

D.1.2 Minimum set of functions defining the gNB network product class

As part of the gNB network product, it is expected that the gNB to contain gNB application, a set of running processes (typically more than one) executing the software package for the gNB functions and OAM functions that are specific to the gNB network product model. Functionalities specific to the gNB network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.511 [6].

Note: For the purposes of the present document, this common set is defined to be the list of gNB functions contained in 3GPP TS 38.300, [7], 3GPP TS 38.323, [9], 3GPP TS 38.322, [10], and TS 23.501 [8].

**\*\*\*\* NEXT CHANGE \*\*\*\***

D.2.2.1 Control plane data confidentiality protection

***-*** *Threat name:* gNB control plane data confidentiality protection.

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

***-*** *Threat Description:* If the gNB does not provide confidentiality protection for control plane packets on the N2/Xn reference points, then the control plane packets sent between gNBs (e.g. inter-gNB handover) and from gNB to AMF (e.g. handover on AMF change) can be intercepted by attackers and hence, the UE identifiers, security capabilities, the security algorithms and key materials exchanged between gNBs and gNB-AMF can be accessed by the attackers leading to huge security breach. This threat scenario assumes that the N2, Xn reference points are not within the security environment.

***-*** *Threatened Asset:* User account data and credentials, Mobility Management data.

D.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 gNB does not provide integrity protection for control plane packets on N2/Xn reference points, the control plane packets between gNBs on Xn-C and from gNB to AMF on N2 interface risk being modified. The intruder manipulations on control plane packets can lead to denial of service to legitimate users. This threat scenario assumes that the N2, Xn reference points are not within the security environment.

***-*** *Threatened Asset:* Sufficient Processing Capacity, user account data and credentials, Mobility Management data.

D.2.2.3 User plane data confidentiality protection at gNB

***-*** *Threat name:* User plane data confidentiality protection at gNB.

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

***-*** *Threat Description:* If the gNB does not cipher and decipher user plane packets between the Uu reference point and the N3/Xn reference points, then the attackers can compromise user packets on Uu, Xn-U, and N3interface. The attackers can gain access to user identifiers, serving network identifiers, location information and can perform user tracking. This threat scenario assumes that the N3, Xn reference points are not within the security environment.

***-*** *Threatened Asset:* user plane data.

**\*\*\*\* NEXT CHANGE \*\*\*\***

D.2.2.7 Key Reuse

*- Threat name:* Key Reuse.

*- Threat Category*: Information Disclosure.

*- Threat Description*: If AS keys are not refreshed by the gNB when PDCP COUNTs is about to be re-used with the same Radio Bearer identity and with the same KgNB, key stream reuse is possible. This can result in information disclosure of AS signalling and user plane data. The threat of key stream reuse occurs under the following conditions 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 CHANGES \*\*\*\***