**3GPP TSG-SA3 Meeting #117 S3-243438**

Maastricht, Netherlands 19 - 23 August 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.926** | **CR** | **DraftCR** | **rev** | **-** | **Current version:** | **19.1.0** |  |
|  | | | | | | | | |
| *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 |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Addition of a new threat on peer certificate checking at gNB | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei; HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G\_Maint | | | | |  | ***Date:*** | | | 2024-08-17 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-19 |
|  | *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:*** | | Addition of a new threat related to a potential failure or lack of support of peer certificate checking at gNB.  Addition of a new threat on the potential lack of certificate checking at the gNB. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Addition of a new threat for the gNB network product class on peer certificate checking at gNB.  Addition of a new threat for the gNB network product class. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete SCAS coverage of the certificate related functionality. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | D.2.2.x(new), D.2.2.y(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 of Change\*\*\*\*\*\*\*\*\*\*\*\*\*

### D.2.2.X Peer certificate validity checking

*- Threat name:* Peer certificate checking

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

*- Threat Description*: If the gNB does not have the capability to check the validity of peer certificate, the gNB may mislead to establish a connection with any peer potentially with malicious intent and using invalid certificates that could have been already revoked or expired, etc.

*- Threatened Asset*: User Plane Data, Control Plane Data, Sufficient Processing Capability.

\*\*\*\*\*\*\*\*\*\*\*\*\* End 1st of Change\*\*\*\*\*\*\*\*\*\*\*\*\*

 \*\*\*\*\*\*\*\*\*\*\*\*\* 2nd of Change\*\*\*\*\*\*\*\*\*\*\*\*\*

### D.2.2.Y Certificate expiry checking

*- Threat name:* Certificate expiry checking at gNB

*- Threat Category*: Denial of Service.

*- Threat Description*: If the gNB does not have the capability to check for certificate expiry and to expose such issue (for example by raising an alarm or logging) should the certificate be about to expire, then this may result in the peer (for example, the UPF or the AMF) rejecting the connection with the gNB. Such a late failure and all the corresponding signalling exchange with the peer are completely unnecessary. Furthermore, such issue could remain unnoticed.

*- Threatened Asset*: Sufficient Processing Capability.

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