**3GPP TSG-SA3 Meeting #107-e *S3-220692***

**e-meeting, 16 - 20 May 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *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 | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | New threat for confidentiality, integrity and replay between AAnF and AF/NEF | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Keysight Technologies | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2022-05-05 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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:*** | | New threat detected for AAnF | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Added new threat to cover the confidentiality, integrity and replay between AAnF and AF/NEF | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Threat not covered in the TR | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex X | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | pCR S3-220691 depends of this threat to be approved. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | * r1: Added revision marks in the document as MCC comments | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## Annex X. Aspects specific to the network product class AAnF

X.1 Threats related to Control plane

## X.1.Y Control plane data protection with AF/NEF

***-*** *Threat name:*  Control plane data protection with AF/NEF.

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

***-*** *Threat Description:* Control plane traffic is transported between the AAnF and the AF/NEF via SBA interface. If the control plane data transported over the interface is not confidentiality protected, it can be subject to eavesdropping. Information is leaked to unauthorized parties. If the control plane traffic is not integrity protected, attackers can tamper with user traffic at will. If the control plane traffic is not replay protected, attackers can insert historical legitimate values into the AAnF or to the AF/NEF. This can lead to denial of service to legitimate users.

If the protection implemented for the control plane transported over the SBA interface uses the wrong security profile, which may contain weak security algorithms or protocol versions known to be vulnerable, the level of the security of the user plane data may be degraded and fail to fulfil the required security.

***-*** *Threatened Asset:* SUPI.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*