**3GPP TSG-SA3 Meeting #102-e S3-210379-r1**

**e-meeting, 18 – 29 January 2021, Online**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.926** | **CR** | 0039 | **rev** |  | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
| *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 | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarification on exposure of confidential IEs in N32-f message in TR 33.926 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, Hisilicon, Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G | | | | |  | ***Date:*** | | | 2020-12-29 |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | In SA3 #101e meeting, it was agreed to align the JSON format on encryption IE with CT4. Hence, the test case on the confidential IEs replacement handling in original N32-f message should be updated accordingly.  According to TS 29.573, the SEPP replaces the cleartext representations of information elements requiring encryption with the value "encBlockIdx", rather then the “NULL”. Hence, the threat shall be updated accordingly. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Change the “NULL” to “encBlockIdx” as defined in TS 29.573. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Not align with the procedure defined in TS 29.573. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.2.5, 2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | | **X** |  | Test specifications | | | | TR 33.926 CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\* BEGIN CHANGES \*\*\*

### G.2.4.2 Exposure of confidential IEs in N32-f message

*- Threat name:* Exposure of confidential IEs in N32-f message.

*- Threat Category*: Information Disclosure.

*- Threat Description*: the following behaviours may lead to exposure of confidential IEs in N32-message, which can result in information disclosure:

- ▪ if the SEPP does not correctly replace the cleartext representations of information elements requiring encryption with the value " encBlockIdx ", there is the threat that the sensitive information in original N32-f messages may be exposed to IPX providers in the path or any other parties eavesdropping on the connection between roaming partners.

- ▪ if the SEPP does not correctly apply the basic validation rule and verify that an intermediate IPX has not inserted an IE requiring encryption at a different location in a JSON object, there is the threat that a misbehaving or compromised intermediate IPX can copy the encrypted IE into a cleartext IE in a request. Then the receiving SEPP decrypts the encrypted IE and puts its value into the cleartext IE field, resulting in the confidential IEs in N32-f message being exposed in the clear.

*- Threatened Asset*: SEPP Application, Service Messages to be sent/received over N32.

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