**3GPP TSG-SA3 Meeting #100e *S3-201855***

**e-meeting, 17 -28 Aug 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **TS 33.926** | **CR** | **DRAFT** | **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:*** | Threats specific of high-priority algorithm selection in the P-CSCF | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, Hisilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_IMS | | | | |  | ***Date:*** | | | 2020-7-16 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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 high-priority algorithm selection in the P-CSCF needs to be added. If the P-CSCF does not select the highest priority algorithm combination on its own list which is also supported by the UE to protect the messages between the P-CSCF and the UE, the new P-CSCF could end up using a weaker algorithm forcing the system into a lowered security level making the system easily attacked and/or compromised. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Adding threats related to high-priority algorithm selection in the P-CSCF | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No reference of threats related to high-priority algorithm selection in the P-CSCF | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | New Annex X.Y.Z | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## X.Y.Z Threats related to set-up of security associations

### X.Y.Z.1 High-priority algorithm selection

- Threat name: High-priority algorithm selection

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

- Threat Description: If the P‑CSCF does not select the highest priority algorithm combination on its own list which is also supported by the UE to protect the messages between the P‑CSCF and the UE, the P‑CSCF could end up using a weaker algorithm forcing the system into a lowered security level making the system easily attacked and/or compromised.

- Threatened Asset: IMS signalling

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