**3GPP TSG-SA3 Meeting #100e *S3-201857***

**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 bidding down on security association set-up |
|  |  |
| ***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 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-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 bidding down on security association set-up needs to be added. If the P-CSCF does not check whether the integrity and encryption algorithms list, SPI\_P and Port\_P received in SM7 is identical with the corresponding parameters sent in SM6, and check whether SPI\_U and Port\_U received in SM7 are identical with those received in SM1, the UE can force the system to reduce the security level by using weaker security algorithms or turning security off, making the system easily attacked and/or compromised. |
|  |  |
| ***Summary of change:*** | Adding threats related to bidding down on security association set-up |
|  |  |
| ***Consequences if not approved:*** | No reference of threats related to bidding down on security association set-up |
|  |  |
| ***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 Bidding down on security association set-up

- Threat name: Bidding down on security association set-up

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

- Threat Description: If the P‑CSCF does not check whether the integrity and encryption algorithms list, SPI\_P and Port\_P received in SM7 is identical with the corresponding parameters sent in SM6, and check whether SPI\_U and Port\_U received in SM7 are identical with those received in SM1, the attacker can force the system to reduce the security level by tampering the integrity and encryption algorithms list. Then, weaker security algorithms may be selected, which will make the system easily attacked and/or compromised. Tampering the SPI will cause the the negotiated SA cannot be indexed. As a result, the following security association fails to be established or Denial of Service occurs. The port number is generally used to identify different applications. Tampering the Port\_P number by the attacker will cause messages to be sent to the UE or P-CSCF through the Tampered port. These messages including some sensitive parameters may be leaked to another application, which is not intended to receive this message.

- Threatened Asset: IMS signalling, security data

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