**3GPP TSG-SA3 Meeting #116 *S3-242402***

Jeju, South Korea, 20th - 24th May 2024

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **33.926** |  **CR** | **draftCR** | **rev** | **-** | **Current version:** | **19.0.0** |  |
|  |
| *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:***  |  Security Assurance Specification (SCAS) threats specific to SMSF |
|  |  |
| ***Source to WG:*** | Indian Institute of Technology Bombay |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_SMSF |  | ***Date:*** | 13-05-2024 |
|  |  |  |  |  |
| ***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 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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | New clauses identifying threats on the Diameter SGd interface of the SMSF |
|  |  |
| ***Summary of change:*** | Clauses identifying threats related to the SGd interface of the SMSF are added, along with a figure depicting interfaces between the SMSF and other network entities in the critical assets clause |
|  |  |
| ***Consequences if not approved:*** | Legacy interfaces assets if not protected, could lead to security breach and network attacks |
|  |  |
| ***Clauses affected:*** |  |
|  |  |
|  | **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 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##

# Y.2 Assets and threats specific to the SMSF

## Y.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the TS 33.926 [7] document, the critical assets specific to the SMSF to be protected are:

- SMSF Application;

- NF and User Data: e.g. NF capabilities and events, network and user sensitive information (e.g., UeSMSContextData like supi, gpsi, ueLocation etc.), data retrieved from UDM, etc.

- The interfaces of SMSF to be protected and which are within SECAM scope (Figure Y.2-1 depicts the different interfaces between SMSF and other network entities):

- Service based interface for providing services to AMF, SMS-GMSC, IP-SM-GW, SMS-Router

- Service based interface for consuming services from AMF, UDM

- Reference point interface SGd (Diameter-based) with IP-SM-GW, SMS-GMSC, SMS- router

- MAP-based SS7 interface with IP-SM-GW/GMSC/SMS- router

- Console interface, for local access: local interface on SMSF

- OAM interface, for remote access: interface between SMSF and OAM system

- SMSF Software: binary code or executable code

NOTE 2: SMSF files may be any file owned by a user (root user as well as non-root uses), including User account data and credentials, Log data, configuration data, OS files, SMSF application, NF and User data, or SMSF Software.



Figure Y.2-1: Interface connections between SMSF and other network entities

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

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

## Y.2.x Threats related to Diameter-based SGd interface

### Y.2.x.y Diameter filtering

***-*** *Threat name:*  Diameter filtering

***-*** *Threat Category:* Denial of service.

***-*** *Threat Description:*

If filtering is not applied at the Diameter SGd interface of SMSF, the SMSF may receive incoming messages that have been manipulated by an attacker. This could potentially lead to interface hijacking and, consequently, denial of service.

***-*** *Threatened Asset:* SMSF application and Reference point interface SGd.

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## Y.2.x Threats related to Diameter-based SGd interface

### Y.2.x.y Diameter session information disclosure

***-*** *Threat name:*  Diameter session information disclosure

***-*** *Threat Category:* Information disclosure, denial of service.

***-*** *Threat Description:*

If the Diameter session is not an implicitly terminated session, it can possibly lead to session hijacking and consequently denial of service. Furthermore, if Diameter session IDs are not unique, then it can lead to unintended information disclosure due to incorrect session associations.

***-*** *Threatened Asset:* SMSF and user data.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*