**3GPP TSG-SA3 Meeting #100e *S3-20xxxx***

**e-meeting, 17 - 28 August 2020 *revision of S3-201997***

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.926** | **CR** | **DraftCR** | **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:***  | Critical Assets of SCP  |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_SECOP  |  | ***Date:*** | 07-08-2020 |
|  |  |  |  |  |
| ***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 work item of Security Assurance Specification for Service Communication Proxy (SCP) was approved at SA3#98e meeting. Before defining the test cases for security assurance, it is essential to first identify the critical assets of SCP which could become the targets of attackers and need to be protected. Therefore, it is proposed to add an Annex for the SCP network product class in TR 33.926 R17 for capturing its critical assets and the anaysis of potential threats. |
|  |  |
| ***Summary of change:*** | Added a new normative Annex for the SCP network product class in TR 33.926 R17. |
|  |  |
| ***Consequences if not approved:*** | Lack of to-be-protected objects for security assurance. |
|  |  |
| ***Clauses affected:*** | New Annex X, new clauses X.1, X1.1, X1.2, X2, X2.1 |
|  |  |
|  | **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 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 33.916: "Security Assurance Methodology for 3GPP network products classes".

[3] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[4] 3GPP TR 33.821: "Rationale and track of security decisions in Long Term Evolution (LTE) RAN/3GPP System Architecture Evolution (SAE)".

[5] 3GPP TS 33.116: "Security Assurance Specification for MME network product class".

[6] 3GPP TS 33.511: "5G Security Assurance Specification (SCAS); NR Node B (gNB)"

[7] 3GPP TS 38.300 v15: "NR; NR and NR-RAN Overall Description; Stage 2".

[8] 3GPP TS 23.501 v15: "System Architecture for 5G System; Stage 2".

[9] 3GPP TS 38.323 v15: "NR; Packet Data Convergence Protocol (PDCP) specification".

[10] 3GPP TS 38.322 v15: "NR; Radio Link Control (RLC) protocol specification".

[11] 3GPP TS 33.250: "Security assurance specification for the PGW network product class".

[12] 3GPP TS 33.516: "5G Security Assurance Specification (SCAS) for the AUSF network product class".

[13] 3GPP TS 33.517: "5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class".

[14] 3GPP TS 33.501 Release 15: "Security architecture and procedures for 5G system".

[15] 3GPP TS 33.518: "5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class".

[16] 3GPP TS 33.519: "5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class".

[17] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[18] 3GPP TS 33.513: "5G Security Assurance Specification (SCAS); User Plane Function (UPF)".

[19] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN);Overall description;Stage 2."

[20] 3GPP TS 33.216: "Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class."

[21] 3GPP TS 33.514: "5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class".

[22] 3GPP TS 33.512: "5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)".

[x] 3GPP TS 33.522: "5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP) ".

[y] 3GPP TS 23.501: "System Architecture for 5G System; Stage 2" (Release 16).

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

Annex X (normative):
Aspects specific to the network product class SCP

# X.1 Network product class description for the SCP

## X.1.1 Introduction

This annex captures the aspects specific to network product class SCP.

## X.1.2 Minimum set of functions defining the SCP network product class

According to TR 33.916 [2], a network product class is a class of products that all implement a common set of 3GPP-defined functionalities. Therefore, in order to define the SCP network product class, it is necessary to define the common set of 3GPP-defined functionalities that is constitutive for a SCP. As part of the SCP network product, it is expected that the SCP contains SCP application, a set of running processes (typically more than one) executing the software package for the SCP functions and OAM functions that is specific to the SCP network product model. Functionalities specific to the SCP network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.522 [x].

Note: For the purposes of the present document, this common set is defined to be the list of functions contained in clause 6.2.19 of 3GPP TS 23.501 [y].

# X.2 Assets and threats specific to the SCP

## X.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the SCP to be protected are:

- SCP Application;

- Service Messages forwarded/routed between NFs/NF services;

- Security data attached to service requests (e.g. Access Tokens, client credentials assertions);

- Data related to routing, selection, discovery (e.g. Routing and selection policies, Routing Binding Indication, Discovery and selection parameters (for communication model D));

- The interfaces of the SCP to be protected and which are within SECAM scope:

- Interfaces between the SCP and NFs

- Interfaces between the SCPs

- Internal interfaces of the SCP in a distributed model

- Console interface, for local access: local interface on the SCP.

- OAM interface, for remote access: interface between the SCP and OAM system.

NOTE 1: The detailed interfaces of the SCP network product class are described in clause 4.3.6 of the present document.

- SCP Software: binary code or executable code

NOTE 2: SCP files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, SCP application, access tokens, client credentials assertions, routing and selection policies, or SCP Software.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*