**3GPP TSG-SA3 Meeting #104-e *S3-212666-r1***

**e-meeting, 16 - 27 August 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.926** | **CR** | Draft CR | **rev** |  | **Current version:** | **17.1.0** |  |
|  | | | | | | | | |
| *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:*** | Adding description and critical assets for NSSAAF | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G\_NSSAAF | | | | |  | ***Date:*** | | | 2021-07-09 |
|  |  | | | |  | |  | | |  |
| ***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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The aspects on network product class description and critical assets specific for NSSAAF are missing in TR 33.926 [1]. This contribution proposes to add the missing aspects.  This contribution also proposes a correction in Annex F in TR 33.926. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Adding network product class description and critical assets specific to NSSAAF | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete spec | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex X (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 Change 1\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 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)".

[23] 3GPP TS 33.521: "Security Assurance Specification (SCAS) for the Network Data Analytics Function (NWDAF) network product class".

[24] 3GPP TS 23.288: " Architecture enhancements for 5G System (5GS) to support network data analytics services".

[25] 3GPP TS 33.226: "Security assurance for IP Multimedia Subsystem (IMS)".

[26] 3GPP TS 33.501: "Security architecture and procedures for 5G system" (Release 16).

[Y] 3GPP TS 33.326: "Security Assurance Specification (SCAS) for the Network Slice-Specific Authentication and Authorization Function (NSSAAF) network product class"

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

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

Annex X:   
Aspects specific to the network product class NSSAAF

# X.1 Network product class description for the NSSAAF

### X.1.1 Introduction

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

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

As part of the NSSAAF network product, it is expected that the NSSAAF to contain NSSAAF application, a set of running processes (typically more than one) executing the software package for the NSSAAF functions and OAM functions that is specific to the NSSAAF network product model. Functionalities specific to the NSSAAF network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.326 [Y].

Note:For the purposes of the present document, this common set is defined to be the list of NSSAAF functions contained in clause 6.2.23 of 3GPP TS 23.501 [8].

# X.2 Assets and threats specific to the NSSAAF

## 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 NSSAAF to be protected are:

- NSSAAF Application;

- User Data: e.g. subscriber's identities (e.g. GPSI), S-NSSAIs, EAP authentication parameters (e.g. EAP ID), etc.

- Slice information: e.g. the the (S-NSSAI, ENSI) mappings

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

- Service based interface, NNSSAAF, for providing services to AMF

- Service based interface for consuming services from UDM, and AMF

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

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

- AAA interface: interface betweeen NSSAAF and AAA-P or AAA-S

NOTE 1: The detailed interfaces of the NSSAAF class are described in clause 4, Network Product Class Description of the present document.

- NSSAAF Software: binary code or executable code

NOTE 2: NSSAAF 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, NSSAAF application, user data or NSSAAF Software.

NOTE X: The slice information is only applicable when AAA-S belongs to the 3rd party and the mapping of S-NSSAI to ENSI is needed.

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

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

# F.2 Assets and threats specific to the AUSF

## F.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 AUSF to be protected are:

- AUSF Application;

- User Data: e.g. subscriber's identities (e.g. SUPI), authentication parameters (e.g. Serving network name, authentication vectors, AUSF key), Routing indicator etc.

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

- Service based interface, Nausf, for providing services for AMF and UDM

- Service based interface for consuming services from UDM, and NRF

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

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

NOTE 1: The detailed interfaces of the AUSF class are described in clause 4, Network Product Class Description of the present document.

- AUSF Software: binary code or executable code

NOTE 2: AUSF 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, AUSF application, User data or AUSF Software.

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