**3GPP TSG-SA3 Meeting #107-e  *S3-224135***

**Toulouse, France, 14 - 18 November 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.926** | **CR** | **draft CR** | **rev** | **-** | **Current version:** | **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:***  | Living document for AAnF SCAS – draftCR to TR 33.926  |
|  |  |
| ***Source to WG:*** | China Mobile |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_AAnF |  | ***Date:*** | 2022-11-18 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** |  |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Adding a dedicated annex in 3GPP TR 33.926 including a network product class description with the corresponding critical assets and threats for thr product class of AKMA Anchor Function (AAnF). |
|  |  |
| ***Summary of change:*** | Addition of a new annex including the critical assets and threats pertaining to the AAnF network product class |
|  |  |
| ***Consequences if not approved:*** | Incomplete security assurance work for AAnF |
|  |  |
| ***Clauses affected:*** | 2, 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 draftCR's revision history:*** | SA3#107e: S3-220768, S3-221157, S3-221160, SA3#108e: S3-222369SA3#109: S3-223674 |

\*\*\* 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)".

[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).

[27] 3GPP TS 33.522: "5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP)".

[28] 3GPP TS 23.501: "System Architecture for 5G System; Stage 2" (Release 16).

[XX] 3GPP TS 33.537: "5G Security Assurance Specification (SCAS) for the Authentication and Key Management for Applications (AKMA) Anchor Function (AAnF)".

[YY] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)" (Release 17)".

\*\*\* Next CHANGE \*\*\*

# Annex X:

# Aspects specific to the network product class AAnF

# X.1 Network product class description for the AAnF

### X.1.1 Introduction

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

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

As part of the AAnF network product, it is expected that the AAnF to contain AAnF application, a set of running processes (typically more than one) executing the software package for the AAnF functions and OAM functions that is specific to the AAnF network product model. Functionalities specific to the AAnF network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.537 [XX].

Note:For the purposes of the present document, this common set is defined to be the list of AAnF functions contained in clause 4.2.1 of 3GPP TS 33.535 [YY].

\*\*\* Next CHANGE \*\*\*

# X.2 Assets and threats specific to the AAnF

## 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 AAnF to be protected are:

- AAnF Application;

- AKMA context Data: i.e. subscriber's identities (SUPI), AKMA Anchor Key (KAKMA) and AKMA Key IDentifier (A-KID).

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

- Service based interface, Naanf, for providing services for AUSF, NEF, AF

- Service based interface for consuming services from AUSF, NEF, AF, and NRF

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

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

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

- AAnF Software: binary code or executable code

NOTE 2: AAnF 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, AAnF application, AKMA context data or AAnF Software.

## X.2.2 Threats related to AAnF assets

## X.2.2.1 Control plane data protection with AUSF

***-*** *Threat name:*  Control plane data protection with AUSF.

***-*** *Threat Category:* Tampering,Information Disclosure, Denial of Service.

***-*** *Threat Description:* Control plane traffic is transported between the AAnF and the AUSF via SBA interface. If the control plane data transported over the interface is not confidentiality protected, it can be subject to eavesdropping. Information is leaked to unauthorized parties. If the control plane traffic is not integrity protected, attackers can tamper with user traffic at will. If the control plane traffic is not replay protected, attackers can insert historical legitimate values into the AAnF or to the AUSF. This can lead to denial of service to legitimate users.

 If the protection implemented for the control plane transported over the SBA interface uses the wrong security profile, which may contain weak security algorithms or protocol versions known to be vulnerable, the level of the security of the user plane data may be degraded and fail to fulfil the required security.

***-*** *Threatened Asset:* AKMA key material, SUPI.

## X.2.2.2 Control plane data protection with AF/NEF

***-*** *Threat name:*  Control plane data protection with AF/NEF.

***-*** *Threat Category:* Tampering,Information Disclosure, Denial of Service.

***-*** *Threat Description:* Control plane traffic is transported between the AAnF and the AF/NEF via SBA interface. If the control plane data transported over the interface is not confidentiality protected, it can be subject to eavesdropping. Information is leaked to unauthorized parties. If the control plane traffic is not integrity protected, attackers can tamper with user traffic at will. If the control plane traffic is not replay protected, attackers can insert historical legitimate values into the AAnF or to the AF/NEF. This can lead to denial of service to legitimate users.

 If the protection implemented for the control plane transported over the SBA interface uses the wrong security profile, which may contain weak security algorithms or protocol versions known to be vulnerable, the level of the security of the user plane data may be degraded and fail to fulfil the required security.

***-*** *Threatened Asset:* SUPI.

### X.2.2.3 AKMA key storage and update

- Threat name: AKMA key storage and update

- Threat Category: Elevation of Privilege

- Threat Description: If the AAnF does not maintain only the latest AKMA Context but also past ones, there is a possibility of an AKMA service failure.

- Threatened Asset: Sufficient Processing Capacity.

\*\*\* END OF CHANGES \*\*\*