**3GPP TSG-SA3 Meeting #104-e *draft\_S3-212873-r1***

**e-meeting, 16 - 27 August 2021** Revision of S3-20xxxx

**Source: Ericsson**

**Title: Solution to KI#1 (****Support of EAP-AKA’ authentication for NSWO) using credentials retrieved from UDM**

**Document for: Approval**

**Agenda Item: 5.22**

# 1 Decision/action requested

***It is proposed to add the following solution to the TR in [1]***

# 2 References

[1] 3GPP TR 33.881 “Study on non-seamless WLAN Offload in 5GS using 3GPP credentials”

# 3 Rationale

This contribution proposes a solution to KI #1.

# 4 Detailed proposal

\*\*\*\*\*\*BEGIN CHANGES\*\*\*\*\*

# 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".

[x] 3GPP TS 23.003: "Technical Specification Group Core Network and Terminals; Numbering, addressing and identification".

[y] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[z] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

\*\*\*\*\*\*NEXT CHANGES\*\*\*\*\*

## 6.Y Solution #Y: NSWO authentication using credentials retrieved from UDM/ARPF

### 6.Y.1 Introduction

This solution addresses key issue #1 (Support of EAP-AKA’ authentication for NSWO). This solution corresponds to a scenario where NSWO is executed for a user defined in a 5GC and the 5GC does not support interworking with EPC. This is, the home network of the user does not support HSS functionality.

### 6.Y.2 Solution Details

### 6.Y.2.1 Architecture Overview

The architecture proposed by this solution is similar to the existing one in EPC. The 3GPP AAA server fetches authentication vectors over Diameter interface SWx. However, since HSS is not present it is proposed that an AAA-IWF is deployed to relay authentication vectors requests and perform related protocol conversion between Diameter SWx and SBA services towards the UDM/ARPF in the 5GC. The AAA-IWF can be realized by the NSSAAF and use existing N59 reference point with the UDM/ARPF.

Additionally, this solution can also support SUPI privacy. This requires the 3GPP AAA to use updated SWx or new diameter interface, called SWx’ here, that includes the SUCI instead of an IMSI as UE ID.

The assumed architecture is described in Figure 6.Y.2.1-1.



Figure 6.Y.2.1‑1: NSWO access authentication using credentials retrieved from UDM/ARPF

### 6.Y.2.2 Flows

Figure 6.Y.1.2‑1: Non-3GPP access authentication in 5GC via UDM

0. The UE selects a WLAN access network and a PLMN for performing 3GPP based access authentication via this PLMN.

1. A layer-2 connection is established between the UE and the WLAN access network.

2. The EAP authenticator in the WLAN access network sends an EAP Request/Identity to the UE.

3. The UE sends an EAP Response/Identity message. The UE shall send its identity complying with Network Access Identifier (NAI) format specified in TS 23.003 [x]. In case of a 5G ME, the ME determines that 5G subscriber privacy should be used, the NAI contains either a pseudonym allocated to the UE in a previous run of the authentication procedure or, in the case of first authentication, the SUCI.

4. The message is routed towards the proper 3GPP AAA Server based on the realm part of the NAI as specified in TS 33.402 [y]. The routing path may include one or several AAA proxies. In such cases, NAI is formed in decorated NAI format as specified in TS 23.003 [z].

5. The 3GPP AAA Server receives the EAP Response/Identity message that contains the subscriber identity that is SUCI in NAI format. The 3GPP AAA decides to fetch IMSI and authentication vectors from the UDM/ARPF via SWx'.

In case the NAI received from step 4 does not contain a SUCI (i.e. contains an IMSI), the 3GPP AAA server gets IMSI from NAI and request authentication vectors using the existing SWx diameter MAR command.

Similarly, in case the NAI received from step 4 contains a SUCI protected with Null scheme, the 3GPP AAA server may retrieve the IMSI from the SUCI and request authentication vectors using the existing SWx diameter MAR command.

Editor’s Note: Support for NSI-based SUPI needs to be added.

6. The 3GPP AAA Server sends an Auth Vector request with SUCI or IMSI, and the access network identity received from step 4. The request is routed via an AAA-IWF/NSSAAF over SWx/SWx' and sent towards the UDM/ARPF of the 5GC via the AAA-IWF/NSSAAF. In the case that the SUCI is included in the request, this message could be an enhancement to SWx messages, e.g. Multimedia-Auth-Request/ Multimedia-Auth-Answer, as specified in TS 33.402 [y]. Otherwise, if IMSI can be used, the existing diameter SWx MAR commands could be used as defined.

7. The AAA-IWF/NSSAAF discovers and selects an UDM e.g. based on the routing identifier of the SUCI and sends an Auth Vector Request, e.g. Nudm\_UEAuthentication\_GetAaaAV, with the SUCI or SUPI, the access network identity and an indication for the requesting node is 3GPP AAA server.

NOTE: If AAA-IWF/NSSAAF receives IMSI from step 6, the AAA-IWF/NSSAAF derives SUPI from the IMSI.

8. The UDM de-conceals the SUPI from the SUCI. The UDM selects EAP-AKA' as authentication method, e.g. based on UE's subscription, the access network identity and an indication for the requesting node is 3GPP AAA server. The UDM/ARPF generates the AKA AV of EAP-AKA’.

9. The UDM sends the Auth Vector Response to the AAA-IWF/NSSAAF with the selected authentication method, AKA AV and SUPI if SUCI is received in step7.

10. The AAA-IWF/NSSAAF converts SUPI into IMSI and sends the Auth Vector Response to the 3GPP AAA server over SWx/SWx' with the selected authentication method, AKA AV and IMSI.

11. The 3GPP AAA server and the UE proceed with EAP AKA' procedure and derive key materials e.g. MSK/EMSK as specified in TS 33.402 [y].

12. The 3GPP AAA Server sends the EAP Success message and the MSK to the authenticator in the WLAN access network.

13. The authenticator in the WLAN access network informs the UE about the successful authentication with the EAP Success message.

14. The UE and the WLAN access network proceed with security establishment based on the share keying material. After successful authentication, the UE receives its IP configuration from the WLAN access network and can exchange IP data traffic directly via the WLAN, i.e. using NSWO.

### 6.Y.2.3 Subscriber Privacy

The UE determines whether 5G subscriber privacy should be used for NSWO traffic, based on the local configuration or the information provisioned by the home network that the home network supports 5G privacy for access authentication for NSWO.

Note: Depending on ME or USIM capability and UE's subscription, there could be cases that a 5G user can't apply SUCI for NSWO, e.g. the UE has 5G subscription defined in the home network but the terminal is pre-R15.

The UE follows the subscriber privacy for EAP-AKA' as specified in TS 33.501 [z] Annex F. In addition, the UE supports pseudonym NAI that are allocated to the UE by the 3GPP AAA server in a previous run of the authentication procedure, in response to EAP-Request/Identity or EAP-Request/AKA-Identity messages.

When the UE determines 5G subscriber privacy is not applicable for NSWO, the UE uses the NAIs specified in EPC for non-3GPP access interworking as in TS 33.402 [y].

### 6.Y.2.4 Key derivation

When deriving CK' and IK' then the KDF of TS 33.402 [11] clause A.2 is used.

When deriving MSK/EMSK for EAP-AKA' ( i.e. MK = PRF'(IK'|CK',"EAP-AKA'"|Identity)), the UE and the 3GPP AAA follows the Identity used for key derivation as specified in TS 33.501 [z] Annex F, in case the UE determines 5G subscriber privacy is applicable for NSWO, i.e. SUCI is used in NSWO access authentication.

### 6.Y.3 System impact

The solution has the following impacts on the different functions:

UE:

- Supports SUCI as EAP identity for NSWO authentication procedure

- Supports indication provisioned from the home Nework whether 5G privay is supported for NSWO.

3GPP AAA server:

- Support SUCI from access authentication for NSWO. Optionally, extract IMSI from SUCI protected with Null scheme.

- Support Diameter SWx' to retrieve IMSI and AV.

- Support Key derivation (MSK/ESMK) based on 5G EAP-AKA' profile

AAA-IWF/NSSAAF:

- Support protocol conversion between Diameter SWx/SWx' and corresponding SBA service operations with UDM

NOTE: NSSAAF already supports selection of UDM via NRF so this is not considered as an impact.

UDM:

- Support SUCI deconcealment and AV request from 3GPP AAA via AAA-IWF

### 6.Y.4 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

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