**3GPP TSG-SA3 Meeting #108adhoc-e *S3-222262***

**e-meeting, 10 – 14 October 2022**

**Source: Apple**

**Title: Solution – AKMA authentication in roaming scenario**

**Document for: Approval**

**Agenda Item: 5.6**

1 Decision/action requested

***It is proposed to add a new solution in AKMA TR 33.737.***

2 References

Null

3 Rationale

There are different scenarios on the deployment of AKMA roaming:

Arch #1. VPLMN doesn’t support AKMA, AF is in HPLMN

Arch #2. VPLMN doesn’t support AKMA, AF is in VPLMN/DN

Arch #3. VPLMN supports AKMA, AF is in HPLMN

Arch #4. VPLMN supports AKMA, AF is in VPLMN/DN

In the first 3 architectures, the current AKMA mechanism can be reused without enhancement and extra design. But for Arch#4, there is possibility there AF has multiple choices on whether it shall choose VAAnF or HAAnF for the performing AKMA. This pCR provides a solution on Arch#4.

4 Detailed proposal

**\*\*\*\*START OF CHANGES \*\*\***

6.X Solution #X: AKMA Authentication in roaming scenario

6.X.1 Introduction

This solution addresses the key issue #1: Support for AKMA roaming scenario.

6.X.2 Solution details

In this solution, it is assumed the VPLMN deployed AAnF (shown as VAAnF). There are 2 options for VAAnF to request KAF :

Option#1: VAAnF fetch KAF from HAAnF.

Option#2: VAAnF fetch KAKMA from HAUSF, and VAAnF generates KAF based on KAKMA.

6.X.2.1 Option#1 details



Fig 6.x.2-1 Authentication in roaming scenario – Option#1

Step 0: UE performs primary authentication with the network. Then KAUSF is shared between UE and AUSF in Home network.

Step 1.1: UE generates KAKMA and A-KID following AKMA procedure in TS 33.535 and stores them securely.

Step 1.2: AAnF generates KAKMA and A-KID following AKMA procedure in TS 33.535 and stores them securely.

Step 2: UE derives KAF following AKMA procedure in TS 33.535.

Step 3: AUSF selects the AAnF as defined in clause 6.7 in TS 33.535 and send the generated A-KID and KAKMA to the AAnF together with the SUPI of the UE using the Naanf\_AKMA\_KeyRegistration Request service operation.

Step 4: UE send Application session establishment request (A-KID) to AF.

Step 5: AF determines on whether to communicate with VAAnF or HAAnF.

NOTE: AF could contact HAAnF for fetch KAF, which is exactly the AKMA feature defined in R17 in TS 33.535. no need to repeat here. But AF may have local policy to decide which AAnF should it contact.

 Editor’s Note: How the AF selects the HAAnF when the UE is roaming is FFS

Step 6: AF sends Naanf\_AKMA\_ApplicationKey\_Get request(A-KID, AF\_ID) to VAAnF

Step 7: Based on the information provided in A-KID, VAAnF checked this is a roaming UE, so VAAnF sent Naanf\_AKMA\_ApplicationKey\_Get request (A-KID) to HAAnF.

Step 8: HAAnF derives KAF from KAKMA following TS 33.535.

Step 9: HAAnF sent Naanf\_AKMA\_ApplicationKey\_Get response (KAF , KAF expTime, SUPI) to VAAnF.

Step 10: VAAnF send Naanf\_AKMA\_ApplicationKey\_Get response (KAF , KAF expTime, SUPI) to AF.

6.X.2.2 Option#2 details

****

Fig 6.x.2-1 Authentication in roaming scenario – Option#2

Step 0: UE performs primary authentication with the network. Then KAUSF is shared between UE and AUSF in Home network.

Step 1.1: UE generates KAKMA and A-KID following AKMA procedure in TS 33.535 and stores them securely.

Step 1.2: AAnF generates KAKMA and A-KID following AKMA procedure in TS 33.535 and stores them securely.

Step 2: UE derives KAF following AKMA procedure in TS 33.535.

Step 3: AUSF selects the AAnF as defined in clause 6.7 in TS 33.535 and send the generated A-KID and KAKMA to the AAnF together with the SUPI of the UE using the Naanf\_AKMA\_KeyRegistration Request service operation.

Step 4: UE send Application session establishment request (A-KID) to AF.

Step 5: AF determines on whether to communicate with VAAnF or HAAnF.

 NOTE: AF could contact HAAnF for fetch KAF, which is exactly the AKMA feature defined in R17 in TS 33.535, thus no need to repeat here. But AF may have local policy to decide which AAnF should it contact.

 Editor’s Note: How the AF selects the HAAnF or VAAnF when the UE is roaming is FFS

Step 6: if AF determines to contact VAAnF in step 5, AF sends Naanf\_AKMA\_ApplicationKey\_Get request(A-KID, AF\_ID) to VAAnF

Step 7: Based on the information provided in A-KID, VAAnF checked this is a roaming UE, so VAAnF sent Nausf\_AKMA\_Key\_Get request (A-KID) to AUSF in HPLMN.

Step 8: AUSF response with Nausf\_AKMA\_Key\_Get response (KAKMA) to VAAnF.

Step 9: VAAnF derives KAF , KAF expTime based on KAKMA and AF\_ID following the key derivation function defined in A.4 in TS 33.535.

Step 10: VAAnF send Naanf\_AKMA\_ApplicationKey\_Get response (KAF , KAF expTime, SUPI) to AF.

6.X.2.2.1 New service: Nausf\_AKMA\_Key\_Get service operation

**Service operation name:** Nausf\_AKMA\_Key\_Get.

**Description:** The NF consumer requests AKMA Application Key and UE ID from the AUSF.

**Input, Required:** A-KID, AF\_ID

**Input, Optional:** None.

**Output, Required:** KAKMA

**Output, Optional:** None.

6.X.4 Evaluation

TBA.

**\*\*\*\*2nd 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".

[2] 3GPP TR 33.535: " Authentication and key management for applications based on 3GPP credential in 5G （AKMA）".

[3] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) ".

[x] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) ".

[y] 3GPP TS 33.210: "Generic AuthenticationNetwork Domain Security (NDS); IP network layer security".

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