Rel-18 AKMA proposals

China Mobile

2022.1

Two proposals

1. New SID on enhancement of AKMA
2. New WID on SCAS of AAnF

Proposal 1: New SID on enhancement of AKMA

Background & Motivation

AKMA roaming issues

- The AKMA feature has been used as a solution to protect the communication between the UE and the Application Function (AF) in the scenarios of ProSe, MSGin5G, MEC, etc.
- Considering the current AKMA use cases and the potential ones, the roaming aspects have to be considered and specified to support the use of AKMA in these use cases when roaming happens, which have not been addressed in Rel-17.
- As per S3i-200477, SA3 has to make sure the AKMA solutions comply with regulatory requirements.

Need for AKMA push

- GBA push is a mechanism to bootstrap the security between a NAF and a UE, without forcing the UE to contact the BSF to initiate the bootstrapping. With the GBA push, the NAF can share a secret key with the UE, and to push messages to UE securely.
- For AKMA, considering the scenarios where there is a need for the application function initiating the interaction, like when UE is unable to trigger the AKMA procedure in a broadcast scenario, it would be beneficial for AKMA to support the push mechanism.

Consideration of introducing Authentication Proxy in AKMA

- TS 33.222 specifies the use of Authentication Proxy in GBA, where an Authentication Proxy (AP) is a proxy resides between the UE and ASs. It helps to reduce the consumption of authentication vectors and/or to minimize SQN synchronization failures, and relieves the AS of security tasks.
- Whether introducing a similar proxy is feasible and helps with the use of AKMA in services could be studied.

Proposal 1: New SID on enhancement of AKMA

Scope

To study the following aspects:

1. Support of AKMA roaming
2. Investigate AKMA push mechanisms
3. Authentication Proxy

Proposal 1: New SID on enhancement of AKMA

Scope

To study the following aspects:

1. Support of AKMA roaming
2. Investigate AKMA push mechanisms
3. Authentication Proxy

- Identify AKMA roaming **architecture**;
- Investigate solutions **to meet LI requirements**. Specifically, based on the AKMA roaming architecture, to give suggestions to SA3-LI about the network function included within service function chains to support LI.

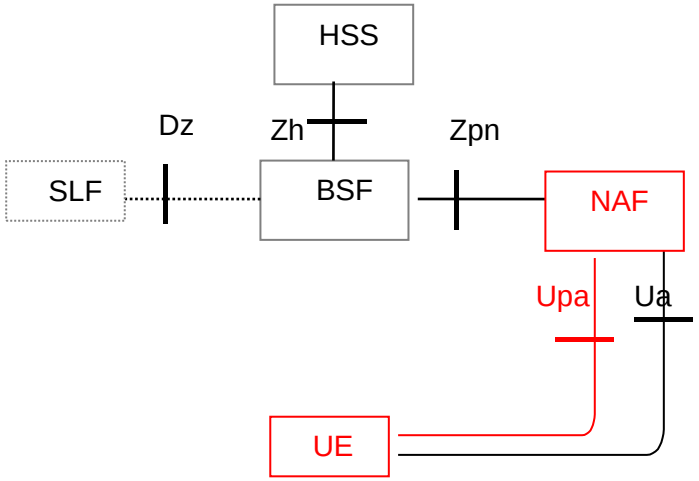
Proposal 1: New SID on enhancement of AKMA

Scope

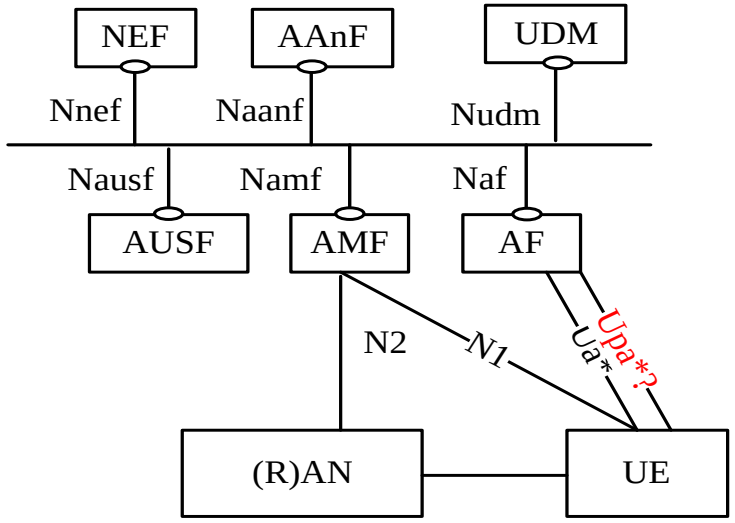
To study the following aspects:

1. Support of AKMA roaming
2. Investigate AKMA push mechanisms
3. Authentication Proxy

- Study the impact to the AKMA architecture
- Identify the AKMA push requirements on network functions
- Investigate AKMA push procedures



GBA push



AKMA push?

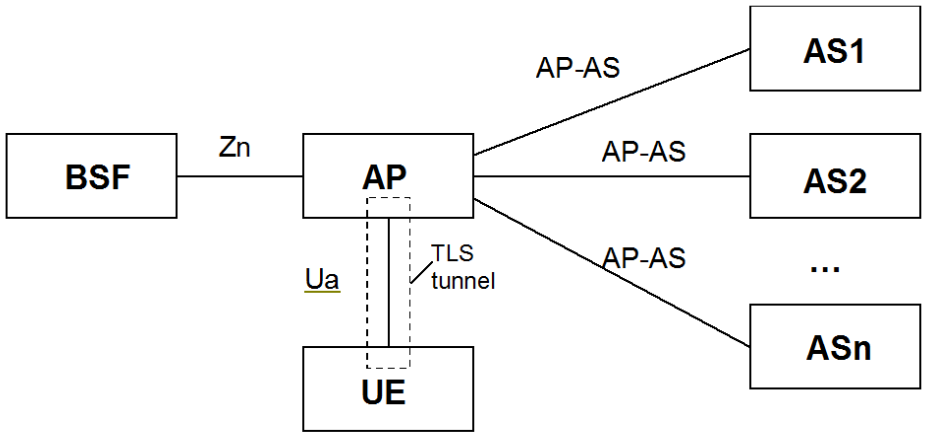
Proposal 1: New SID on enhancement of AKMA

Scope

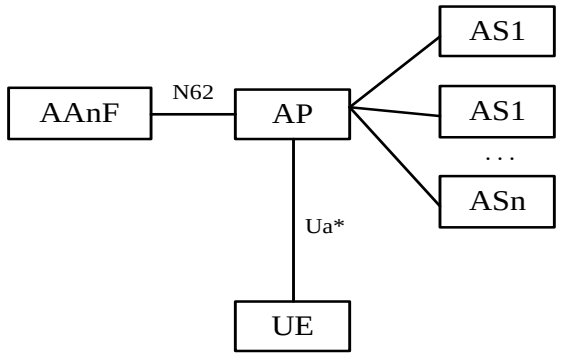
To study the following aspects:

1. Support of AKMA roaming
2. Investigate AKMA push mechanisms
3. Authentication Proxy

- Study the feasibility of introducing the AP into AKMA
- Investigate the architecture impacts and procedures of using the AP in AKMA



AP in GBA



AP in AKMA?

Proposal 2: New WID on SCAS of AAnF

Background & Motivation

- The AKMA feature has been introduced in Rel-17 with a new NF specified -AAnF.
- The AAnF is designed as the anchor function in the HPLMN, which stores the AKMA Anchor Key (K_{AKMA}) and the UE AKMA contexts for AKMA service, and also generates the key material to be used between the UE and the Application Function (AF).
- The Security Assurance Specifications (SCAS) work need to be expanded for AAnF, to identify and define security functional requirements and basic vulnerability requirements that need to be tested for security assurance of AAnF.

Objectives

- identify critical assets and threats of the AAnF not already identified in TR 33.926
- develop and/or adapt AAnF specific security functional requirements and related test cases
- develop and/or adapt AAnF specific basic vulnerability testing requirements and related test cases

Thank you!