Source: NEC
Title: K_{AUSF} desynchronization problem and solutions
Document for: Endorsement
Agenda Item:

1 Decision/action requested

Endorse the proposals of this discussion paper

2 References

[1] 3GPP TR 33.835 Study on Authentication and Key Management for Application based on 3GPP credentials in 5G

[2] S3-190640 Discussion on KAUSF synchronization

[3] 3GPP TS 24.501 Non-Access-Stratum (NAS) protocol for 5G System (5GS)

[4] 3GPP TS 33.501 Security architecture and procedures for 5G system (v15.3.1)

3 Introduction

During SA3#94AH, S3-190640 [2] was presented and discussed. The goal of that paper was to raise awareness about the issue of lack of synchronization between the UE and the AUSF with respect to the K_{AUSF}. The paper was presented for information purposes with the goal of coming back to this issue during the SA3#95 meeting.

Between the SA3#94AH and the SA3#95 meeting, further analysis has been performed. This paper presents the problem analysis and contains proposals for concrete ways forward.

4 Detailed description

4.1 Problem description and analysis

4.1.1 Generic

The K_{AUSF} is used in Steering of Roaming and UE Parameter Update procedures to provide AUSF to UE integrity protection. These procedures thereby implicitly rely on the fact that the K_{AUSF} in the UE and the AUSF are always the same. However, as explained in S3-160640 [2], it is possible for the serving network to launch attacks which cause the K_{AUSF} in the UE and the AUSF to be out of sync. The main reason for this is that there is no security context establishment between the UE and the AUSF, which can lead to situations where the K_{AUSF} handled differently at the UE and the AUSF.

Contrary to the paper S3-160640, which assumed malicious intend, this paper also shows scenarios where the K_{AUSF} is out of sync due to genuine behaviour. The genuine behaviour scenarios and the malicious / non standard behaviour are discussed in the following, but separate clauses.

4.1.2 Genuine behaviour scenarios

4.1.2.1 Introduction

In the following scenarios, the K_{AUSF} can be out of sync at the UE and the AUSF due to genuine behaviour:

- The serving network omits the NAS SMC. This is genuine behaviour because the serving network can always

- The UE is registered on 3GPP access and next authenticates on non-3GPP access. If the UE now detaches, the UE may delete all keys associated with the access, including the K_{AUSF};
- Handover from an EPC to a 5GC without authentication.

In the following paragraphs, the scenarios are discussed in more detail.

4.1.2.2 Not running NAS SMC

Not running NAS SMC by the network is a legitmate action of the network in case the network does not want to take the new security context into use. The steps are depicted below.

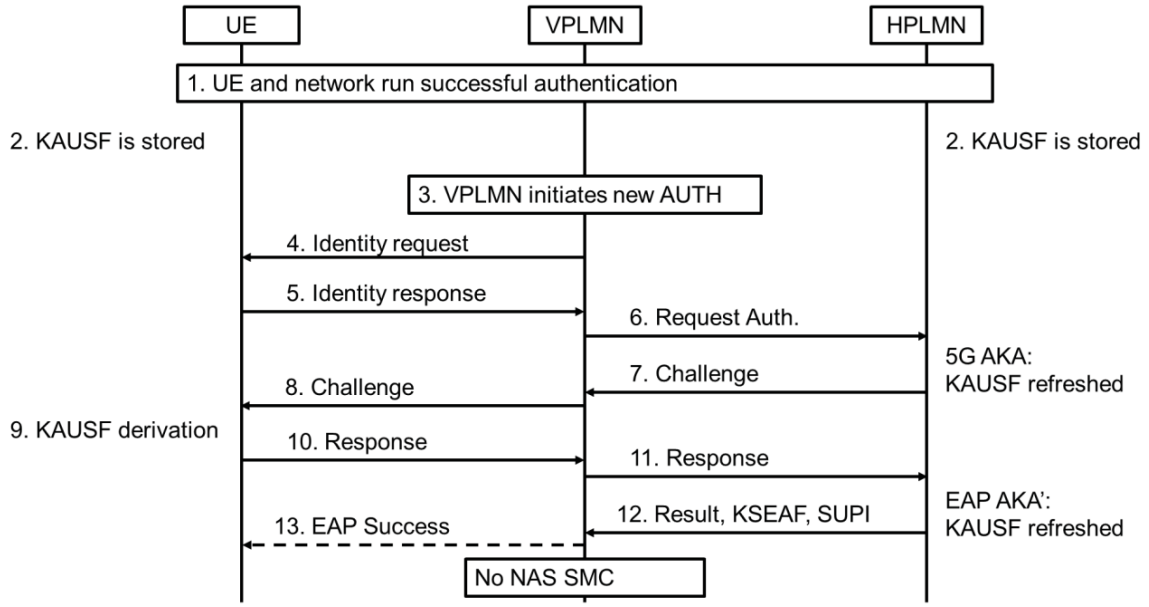

Figure 1: Flow for omitting NAS SMC procedure

For the description of steps 1-10, we refer to our description of the figure 1 in S3-190640 [2]. The description below only covers the steps 11, 12, 13, and the decision of the VPLMN not to initiate the NAS SMC. When arriving at step 11, the UE already has a non-current partial native security context (5G AKA) or a temporary security context (EAP AKA') without a mirror of this security context in the serving network. The steps 11 and further are as follows:

11. The VPLMN / AMF forwards the RES(*) to the Home network. As a result, the AUSF calculates the K_{AUSF} (see [4] clause 6.1.3.1 step 10) or checks whether the AV is expired ([4] clause 6.1.3.2.0 step 11 – nothing is said about what the AUSF should do to the K_{AUSF} if the AV was expired). The AUSF will also calculate K_{SEAF}.
12. In response to the RES(*) (if correct), the AUSF will provide the K_{SEAF} and SUPI and the authentication result to the AMF. If EAP AKA' was used for authentication, the result has the format of an EAP Success message which can be forwarded to the UE.
13. If EAP AKA' was used the AMF may forward the EAP Success message to the UE to inform the UE that it has been authenticated.

NOTE: In this text, we also consider the case where the AMF does not forward the EAP Success message to the UE.

The resulting situation is depicted in the figure below.

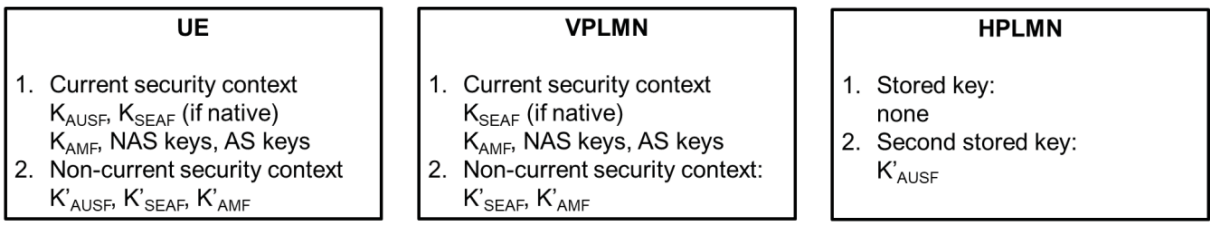

Figure 2: Situation before NAS SMC and after EAP Success in case of EAP AKA'. Note that if no EAP Success message was received, the non-current security context in the UE is a *temporary* security context.

The result of omitting the NAS SMC procedure is that the UE will have a non-current native security context (5G AKA

which will be deleted if no EAP Success or NAS SMC follows. It is not specified whether K_{AUSF} will be deleted as well in that case.

4.1.2.3 Multiple registrations

A UE that performs multiple registrations, i.e. one on 3GPP access and one on non-3GPP access, will have two independent security contexts. In such a case, the UE will first have established a security context with the first VPLMN over, e.g 3GPP access and will subsequently establish a security context with a second VPLMN over non-3GPP access. In the home network, however, the AUSF will delete the key resulting from the first authentication whenever the second authentication happens.

On the UE side, things are less clear. Both security contexts will have K_{AUSF} associated with it. However, it is unclear how this K_{AUSF} is handled by the UE when, e.g. whether

- The UE deletes the first K_{AUSF} whenever the second authentication is successful;
- The UE will delete the second K_{AUSF} whenever it deregisters from the non-3GPP access;
- Which K_{AUSF} the UE will use when for example SoR or UPU procedures are invoked.

4.1.2.4 Handover from EPC

A UE that gets handed over from EPC to 5GC can either use a previously established security context if it operates in dual registration mode or use a security context mapped from the EPC one in case it operates in single registration mode. In the second case, the UE nor the AUSF will have access to a K_{AUSF} to run subsequent procedures with.

This situation can only be resolved by running a new authentication, which is under control of the serving network. Said differently, how long this situation will continue to exist, depends on the serving network policy.

4.1.2.5 Summary and solution direction

In the above, three scenarios are detailed that show how the K_{AUSF} at the UE and the AUSF can be out of sync (or missing altogether). Such an out of sync scenario leads to problems with the security of steering of roaming, the security of UE Parameter Update and potentially AKMA if K_{AUSF} is reused for AKMA.

For the scenario where the UE operates in single registration mode and gets handed over from EPC. Four possible solutions are:

- Storing the a previous K_{AUSF} at both the UE and the AUSF, even if the UE is conntected to EPC;
- Mandate that the AMF always performs authentication whenever the UE gets handed over from EPC and a mapped security context is used;
- Allow the home network to signal the need for an authentication to refresh K_{AUSF}. Such would be a new message from the UDM to the AMF signalling that an authentication for a particular SUPI should be performed upon which the AMF initiates authentication.
- The UDM waits with subsequent procedures until an authentication is performed.

For the other two scenarios (not running NAS SMC and multiple registrations), the underlying problem is that the key cannot be identified and therefore, the UE and AUSF may end up using a different key for the same procedure. The simplest way forward is to add a key identifier to subsequent procedures. Such a key identifier could either be assigned by the network or simply be derived from K_{AUSF}. Apart from that, key handling may be further clarified in TS 33.501 [4].

4.1.3 Malicious / non standard behaviour

4.1.3.1 Introduction

In S3-190640, a number of malicious / non standard behaviour scenarios were discussed. In what follows, most of the text of S3-190640 is repeated with modifications. The following non standard behaviour scenarios are discussed:

- The serving network not completing authentication procedure.
- The serving network maliciously running multiple authentication procedures and not taking the keys into use;

4.1.3.2 VPLMN Not completing the authentication procedure

Aborting the authentication procedure by the serving network is done by not forwarding the RES to the home network. In what follows, the terms VPLMN and HPLMN are used to indicate the network elements AMF/SEAF (VPLMN) and AUSF/UDM (HPLMN). The attack is depicted in the the below figure and explained in the text that follows:

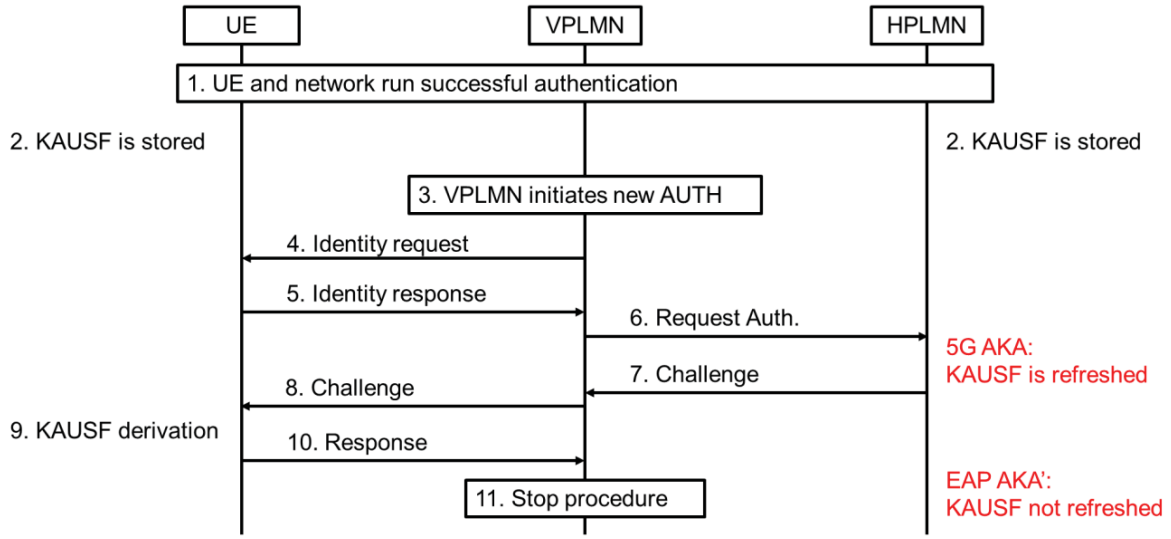

Figure 3: Flow for aborting authentication procedure

According to the following steps:

1. The assumption is that the UE is roaming and that the UE is successfully authenticated and receiving service.
2. As a result of the previous step, both the UE and the AUSF in the HPLMN store the KAUSF that resulted from the last authentication run.
3. At some point in time, the AMF (VPLMN) decides to initiate a new authentication with the UE.
4. The AMF sends an identity request to the UE
5. The UE responds with its identity set to SUCI
6. After receiving the UE's identity, the AMF sends an authentication request (Nausf_UEAuthentication_Authenticate Request) to the AUSF in the HPLMN, which forwards it to the UDM in order to initiate the authentication.

NOTE: For the following steps, the exact messages depend on whether 5G AKA or EAP AKA' is used. Therefore only the generic names are provided.

7. After reception of a 5G AV from the UDM, the AUSF will send the challenge to the AMF/SEAF in the VPLMN.
8. The AMF/SEAF will forward the challenge to the UE
9. The UE will verify the validity of the challenge and if successful, calculate the RES, the K_{AUSF}, K_{SEAF}, and K_{AMF}. What follows depends on which authentication method was used:

   5G AKA: The UE will store the K_{AUSF}, K_{SEAF}, and K_{AMF} in a non-current, partial security context. The UE now has two K_{AUSF}s of which one is different from the one that is stored in the HPLMN. The K_{AUSF} in the HPLMN may correspond to the one that is part of the active security context or may correspond to the one of the new authentication vector. (See [4], clause 6.1.3.2.0, step 3).

   EAP AKA': The UE may store the K_{AUSF}, K_{SEAF}, and K_{AMF} in a *temporary* security context (see [4] clause 6.1.3.1, step 11). The UE now has two K_{AUSF}s of which one is different from the one that is stored in the HPLMN. The one in the HPLMN corresponds to the one that is part of the active security context. (See [3] clause 5.4.1.2.2.3 and [4] clause 6.1.3.1 step 10)

10. The UE returns the the RES to the AMF/SEAF in the VPLMN.
11. The VPLMN / AMF does not forward the RES to the Home network. As a result, the AUSF does not calculate K_{AUSF} (see [4] clause 6.1.3.1 step 10) or expires the AV (see [4] clause 6.1.4.1 step 11)

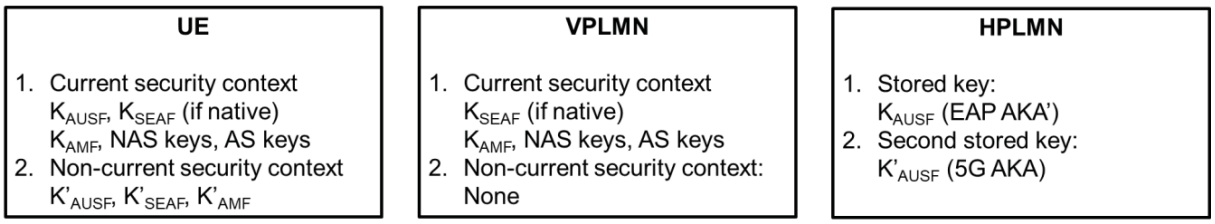

Figure 4: Situation after aborting authentication procedure. Note that on the UE side only the 5G AKA case is shown. For EAP AKA' a *temporary* security context is created instead of a non-current security context.

The result of aborting the procedure is that the UE will have non-current native security context (indicated by the primes) if 5G AKA was used and a temporary security context if EAP AKA' is used. A temporary security context will either be deleted or turned into a current security context or non-current security context upon instruction of the network using EAP Success or NAS SMC.

Proposal 1: A first problem to be solved is the inconsistent behavior between 5G AKA and EAP AKA'. By aligning how the two work, a solution can be found irrespective of which authentication procedure is used. It is proposed to defer storing the key in the AUSF after the AUSF has received the authentication confirmation message from the serving network. This change is proposed in a companion CR.

Proposal 2: After implementation of the above change, the attack can mostly be mitigated by mandating the inclusion of a key identifier for the K_{AUSF} in procedures that use the K_{AUSF}. As can be seen from the figure 4, the UE will have two K_{AUSF}s after authentication and needs to know which one is used. Similarly, the AUSF should be augmented to store two K_{AUSF}s in case UE initiated procedures that also use K_{AUSF} are introduced. One possible example being AKMA. Concrete proposal is to store a key identifier together with the K_{AUSF} and use this key identifier in subsequent procedures. Furthermore, the AUSF should always use the latest K_{AUSF} in SoR and UPU and only move to the older one if the latest one fails. The UE may use either, given that the AUSF stores both.

4.1.3.3 Continuously running authentications

In section 4.1.2.2 it was discussed that the NAS SMC procedure can be omitted by a network for genuine reasons. A network could also behave such with malicious intend in stead. In such a case, the network could run the authentication just for the reason to keep the KAUSF out of sync.

At SA3#94AH it was decided that this type of attack would not be considered because MNOs also have different means to solve such attacks. Therefore, it is not necessary to consider additional measures within the scope of 3GPP for these types of attacks.

4.1.3.4 Summary and solution direction

In the above two scenarios are discussed. The second one was not considered relevant for 3GPP because MNOs have other means at their disposal to deal with such attacks. For the first one, two proposals are done:

- Align the behaviour of the AUSF with respect to storing the K_{AUSF} after receiving the correct RES from the UE;
- Store two K_{AUSF}s in the UE (when a K_{AUSF} is associated with the non-current security context) and always store two K_{AUSF}s in the AUSF;
- Include a key identifier for K_{AUSF} in any procedures using K_{AUSF}.
- Mandate that the AUSF uses the latest K_{AUSF} when using it for AUSF initiated and that the UE may pick either

4.2 Summary

In the above, a number of scenarios and attacks are shown which can cause the K_{AUSF} in the UE and the AUSF to be out of sync. In order to combat these, it is necessary that the UE stores the K_{AUSF} associated with the current and non-current security context, that the AUSF stores two K_{AUSF}s for each UE, and that a key identifier is used in subsequent procedures that involve the K_{AUSF}. In addition a change to 5G AKA is necessary to make sure that EAP AKA' and 5G AKA behave similarly when it comes to storing and refreshing K_{AUSF} at the AUSF side.

Despite these measures, exceptionally malicious behavior of the VPLMN is not fully mitigated because MNOs have other means at their disposal to deal with such attacks. It is proposed to not further consider such scenarios.

4.3 Alternatives to be considered

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.