3GPP TSG-SA WG3 Meeting #95
Reno (USA), 6-10 May 2019

S3-191204
revision of S3-19xabc

Source:	**NEC**
Title:	**K_{AUSF} desynchronization problem and solutions – updated version after conf call on 25 Apr.**
Document for:	**Endorsement**
Agenda Item:	**7.1.2**

1 Decision/action requested

This discussion tdoc reflects the outcome of conf call on 25th Apr and supersedes the original discussion tdoc in S3-191203. It is proposed to 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 (v15.4.0)

[5] S3-191205, CR 0564 (TS 33.501) "Aligning the storage timing of KAUSF in 5G AKA with EAP-AKA'"

[6] S3-191206, Draft CR (TS 33.501) "Synchronization of Kausf between AUSF and UE"

[7] S3-191208, Draft CR (TS 33.501) "UDM triggered authentication"

[8] S3-191209, Draft CR (TS 33.501) "Kausf key setting in EAP-AKA'"

[9] S3-191207, Draft CR (TS 33.501) "Using Key Identifiers between AUSF and UE for UPU and SoR"

[10] S3-191203, "KAUSF desynchronization problem and solutions", (discussion tdoc discussed during the conf call on 25 Apr. 2019)

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.

After SA3#94AH, a disscussion paper was shared over the email reflector with a more detailed analysis and a more concrete proposals. Based on comments received on that paper, a renewed version is presented here.

The paper that was shared over the email reflector is uploaded as S3-191203 [10]. In addition, we have uploaded one CR to immediately fix an issue in 5G AKA. We also provided several draft CRs to show in more detail how a normative solution would look. These are provided for discussion purposes.

4 Detailed description

4.1 Comments received on S3-191203

4.1.1 Association of the K_{AUSF} with the NAS SMC

One comment received on S3-191203 was that the K_{AUSF} has no association with the NAS SMC. Where the NAS SMC

This means that there is no ‘state’ of the K_{AUSF} in relation to the security context that is in use. The storage and usage of KAUSF therefore only depends on whether the authentication has been successful.

4.1.2 Association of the K_{AUSF} with access type

As per the comment on the association with the NAS SMC, the same comment also implied that the K_{AUSF} is not associated with the access type. In dual registration the UE only stores one K_{AUSF}, which is the one resulting from the latest authentication. When deregistering from the access type, the UE does not delete the K_{AUSF}.

4.1.3 Conclusions

The conclusion that should be drawn from the comments is that there is only one K_{AUSF} stored in the UE, which is the result of the latest authentication. The key is not associated with the state of the security context or the access type that is used and is also not deleted after the UE deregisters from a particular access.

4.1.4 Requested actions from SA3

NEC kindly requests SA3 to take the following actions:

Requested action 1: Confirm the conclusion for the UE;

Requested action 2: Confirm that the same conclusion holds for the AUSF.

If the above are confirmed, section 4.2 details the remaining K_{AUSF} desynchronization scenarios.

4.2 Remaining K_{AUSF} desynchronization scenarios

4.2.1 Handover from EPC

4.1.2.1 Problem

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.

4.1.2.1 Summary and solution direction

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

1) Storing the a previous K_{AUSF} at both the UE and the AUSF, even if the UE is conntected to EPC;

2) Mandate that the AMF always performs authentication whenever the UE gets handed over from EPC and a mapped security context is used;

3) 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; and

4) The UDM waits with subsequent procedures until an authentication is performed.

Of the above solutions, the 1) has impact on the UE and is therefore not be backwards compatible with a UE that is Release-15. Solution 2) requires changes to the serving network and may induce unnecessary signalling and authentication even if the home network does not need to use the KAUSF. Solution 3) introduces new signalling between the AMF and the K_{AUSF} and is therefore not backwards compatible with Release-15 networks, but it is backwards compatible with release-15 UE. The advantage of this solution, contrary to solution 2) is that it does not introduce unnecessary authentications because it is only used if the Home network needs it. Also, if the serving network is release-15, the UDM will know by discovery and can delay further procedures until a new authentication is performed. Solution 4) confirms the status quo and offers no advantages over the current situation.

Of these solutions, solution 3) is preferred because it solves the problem in a backwards compatible manner without UE

Proposal 1: Accept solution 3) that introduces a new signalling message from the UDM to the AMF to trigger an authentication of the UE. The solution is proposed in a companion CR S3-191208 [7].

4.2.2 VPLMN Not completing the authentication procedure

4.2.2.1 Introduction

The VPLMN can abort the authentication procedure at two points:

1) Right after when the challenge is received from the home network;

2) Right after when the response is received from the UE.

The two options are depicted in the figure below. In what follows, both options and solutions for both options are discussed.

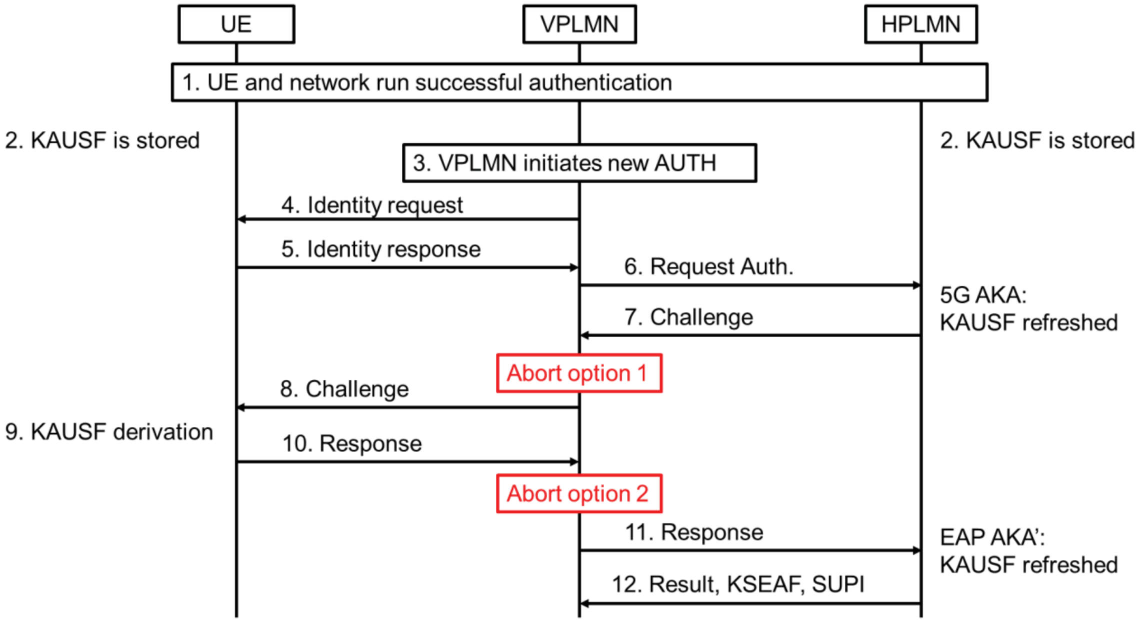


Figure 1: Flow for aborting authentication procedure according showing two options

4.2.2.2 Option 1

In this option, the VPLMN asks for an authentication vector, but never sends the challenge to the UE. The steps are as follows:

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 K_{AUSF} 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 (optional)

5. The UE responds with its identity (SUCI) to the AMF (dependent on step 4)

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 sends the challenge to the AMF/SEAF in the VPLMN.

   5G AKA: The AUSF overwrites the K_{AUSF} after which the UE and the AUSF have a different K_{AUSF}. (See [4], clause 6.1.3.2.0, step 3).

Further steps are not described.

This attack can be mitigated by delaying the derivation of the KAUSF in the AUSF which only leaves option 2 as an attack vector.

Proposal 2: Delay the derivation of KAUSF in the AUSF until after the RES has been received. This has the advantage of mitigating the attack of option 1, but also resolves 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 in the home network after the AUSF has received the authentication confirmation message from the serving network. This change is proposed in a companion CR in S3-191205 [5].

4.2.2.3 Option 2

The second way a VPLMN can abort the authentication procedure is 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:

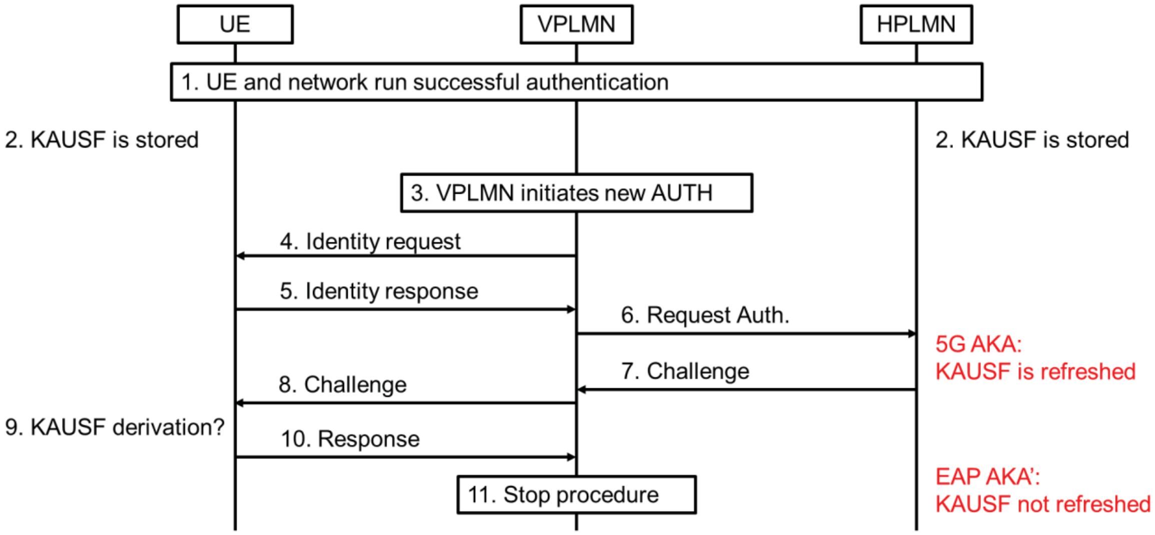


Figure 2: Flow for aborting authentication procedure according to option 2

According to the following steps:

1-7: Refer to figure 1.

8. The AMF/SEAF forward the challenge to the UE.

9. The UE verifies the validity of the challenge and if successful, may calculate the RES, the K_{AUSF}, K_{SEAF}, and K_{AMF}. The resulting situation follows depends on which authentication method was used:

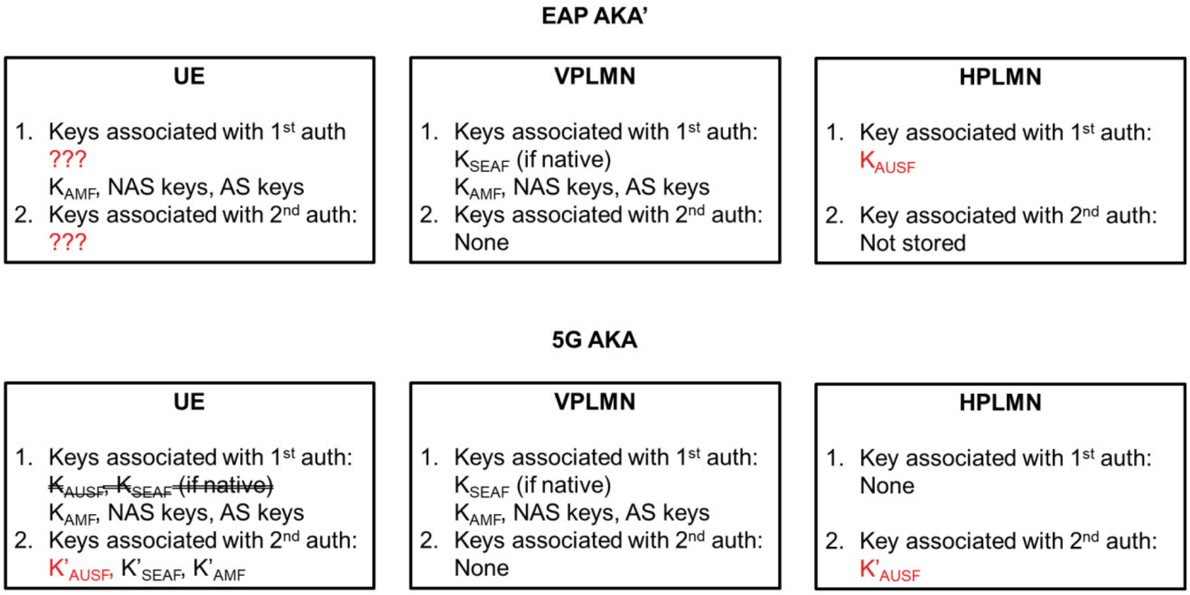
   5G AKA: The UE overwrites the K_{AUSF}. The UE now has a K_{AUSF}s of which is the same as the one stored at the AUSF. (See [4], clause 6.1.3.2.0, step 3).

   EAP AKA': According to TS 33.501 [4] clause 6.1.3.1, step 11, the UE overwrites the K_{AUSF} at this point in time. That would result in the UE having a new K_{AUSF}, which is different from the one that is stored in the HPLMN. (See TS 24.501 [3] clause 5.4.1.2.2.3 and TS 33.501 [4] clause 6.1.3.1 step 10). TS 24.501 [4] clause 5.4.1.2.2.3 and 5.4.1.2.2.8 on the contrary, also allows that the UE calculates the K_{AUSF} at a later point, namely after receiving the EAP Success message. This behaviour is also captured in NOTE 6 in TS 33.501 [4] clause 6.1.3.1. The UE behaviour is therefore rather uncertain.

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 in the home network 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).

The resulting situation is depicted in the figure below.



EAP AKA’

UE

1. Keys associated with 1st auth
???
K_{AMF}, NAS keys, AS keys
2. Keys associated with 2nd auth:
???

VPLMN

1. Keys associated with 1st auth:
K_{SEAF} (if native)
K_{AMF}, NAS keys, AS keys
2. Keys associated with 2nd auth:
None

HPLMN

1. Key associated with 1st auth:
K_{AUSF}
2. Key associated with 2nd auth:
Not stored

5G AKA

UE

1. Keys associated with 1st auth:
~~K_{AUSF}, K_{SEAF} (if native)~~
K_{AMF}, NAS keys, AS keys
2. Keys associated with 2nd auth:
K'_{AUSF}, K'_{SEAF}, K'_{AMF}

VPLMN

1. Keys associated with 1st auth:
K_{SEAF} (if native)
K_{AMF}, NAS keys, AS keys
2. Keys associated with 2nd auth:
None

HPLMN

1. Key associated with 1st auth:
None
2. Key associated with 2nd auth:
K'_{AUSF}

Figure 3: Situation after aborting authentication procedure at the VPLMN. Note that in case of EAP-AKA’ the keys may be desynchronized. In case of 5G AKA, there is no problem in this scenario.

The result of aborting the procedure at the VPLMN is that the UE, if EAP AKA’ is used, may be out of sync with the HPLMN depending on the implementation of EAP AKA’. The specification allows the procedure of EAP AKA’ to be left uncompleted (e.g. during AMF change) and also allows the derivation of the K_{AUSF} to be postponed until after the EAP Success message.

Proposal 2: (same as proposal 2 above): Delay the derivation of K_{AUSF} in the AUSF until after the RES has been received. This has the advantage of mitigating the attack of option 1, but also makes 5G AKA and EAP AKA’ more consistent. This change is proposed in a companion CR in S3-191205 [5].

4.2.2.4 Residual risk

By aligning the 5G AKA and EAP AKA’ behaviour the possible desynchronization if the authentication procedure is aborted remains. During some time window the UE and the HPLMN may remain unsynchronized because the authentication result is not provided to the home network.

The consequence of not providing the success to the home network are the following:

5G AKA: The UE has overwritten the K_{AUSF} and has stored a non-current security context, which the serving network does not have (it didn’t receive the K_{SEAF} because it didn’t send the authentication result to the home network). If the UE’s DM state changes to DM_DEREGISTERED, the UE will store the non-current security context and mark it as current, whereas the serving network will store the current security context. Therefore, a new authentication will be required whenever the UE’s state changes to DM_REGISTERED. However, it may take a long time before this state transition happens, which means that the desynchronized state may persist for a long time.

EAP AKA’: The specification is rather unclear at which point in time the UE overwrites the K_{AUSF} (see [4] clause 6.1.3.1, step 11). The UE and home network could therefore have the same, but also a different K_{AUSF}. In addition, the UE may have created a temporary security context, which will be deleted after some time-out. The exact value of the time out is not specified. It’s also not clear whether the UE will still calculate the K_{AUSF} even if the EAP Success message never arrives. The state is therefore uncertain.

Requested action 3: SA3 should decide whether the resulting possible desynchronization scenario should be solved.

4.2.2.5 Solutions

4.2.2.5.1 Introduction

In order to overcome the problems in the previous paragraphs, the following solutions are proposed in several separate CRs (numbering continues from section 4.1):

4) Storing multiple K_{AUSF}s in the UE and the AUSF and handling the deletetion and activation similar to how

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.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.