SA3/SA3-LI joint conf call on AKMA roaming LI requirements

7th September 3:00 PM - 4:30 PM (CEST)

AKMA roaming scenarios can be structured as followed:

Case 1: UE in VPLMN and accessing an internal HPLMN AF

Case 2: UE is in VPLMN and accessing an internal VPLMN AF

Case 3: UE is in VPLMN and accessing an AF in the Data Network (Internet)

**List of Questions for discussion:**

1. For Case 1, LI requires HPLMN to provide the means to decrypt the user services, e.g., the encryption key.

Note: Apart from the encryption key, other crucial information (e.g., nonces, counters, selected cipher algorithm) in order to decrypt are also obliged to be provided. For simplicity, we just focus on the encryption key in this doc for example.

1. If the encryption key is KAF, then KAF shall be provided. **Yes or No**?

Yes

1. If the encryption key is derived from KAF, e.g. in TLS profile, then the encryption key shall be provided, KAF is not needed to be provided. **Yes or No**?

Yes, either KAF and other parameters (cipher suites, …) used to derive the encryption key or the output of the derived key itself.

1. If the encryption key has nothing to do with KAF, e.g. KAF is only used for authentication, while the encryption key is established according to an application layer protocol, then the encryption key shall be provided, KAF is not needed to be provided. **Yes or No**?

Yes, either KAF and other parameters (cipher suites, …) used to derive the encryption key or the output of the derived key itself.

1. For Case 2, since the AF knows everything about the encryption key, LI requirements can be met by the AF without additional requirement to the HPLMN. **Yes or No?**

Yes

1. For Case 3, since the AF is external, the HPLMN has no knowledge of what KAF is used to do, e.g. for authentication only, for integrity protection, or for deriving the encryption keys, the HPLMN even doesn’t know the encryption key (unless the encryption key is KAF itself).
2. If KAF is used to establish the encryption key, then only KAF and related information which are known to HPLMN shall be provided to VPLMN. **Yes or No**? Having in mind that the HPLMN cannot force the external AF to provide the encryption keys.

Yes

Providing the information that are known to HPLMN

1. If AKMA/KAF is only used for authentication, similar as 1.c) above, AKMA has nothing to do with establishing keys by AF, **What is HPLMN obliged to do in this case?**

Providing the information that are known to HPLMN, e.g. Ua\* protocol identifier

**Minutes of the call:**

Xiaoting (rapporteur of AKMA) chaired the meeting, up to 52 people participated.

**Agenda 1: Presentation of slides from Mats (NDRE, SA3-LI participant)**

Xiaoting (CMCC): question for clarification, the requirements in the slides are only applicable to the use case that AF is an internal to the HPLMN right? For the external AF case, things will be difficult.

Mats (NDRE): Yes, the case for the external AF is a little bit on the side.

Saurabh (Nokia): For the external AF case, should the HPLMN somehow facilitate the AF to transfer the keys?

Mats (NDRE): The intention is right but where do we standardize the transfer protocol, it’s out of scope of 3GPP.

Alex (BT, SA3-LI chair): Currently LEA is concentrating on internal AF, for external AF, what we could probably do is to ringfence the external AF, if the external AF need some service policy control, not a cryptographic solution, that is down to the operator to have some roaming agreements about whether you allow this service to run.

Mats (NDRE): agree, but the issue is in the certain countries which does allow the AKMA keys to exposed the external AF, and if the AF uses the AKMA keys to do DH, then you still do not have full LI control. The DH keys are still outside the control of both PLMNs. In most jurisdictions, there are concerns of full LI plain text capabilities, they will always resort to don’t allow AKMA outside the VPLMN kind of policy.

Xiaoting (CMCC): for the external AF case, it’s difficult to handle at the moment, have listed it in the questions and we can look at it later on and write down some basic understandings as a way forward.

**Agenda 2: Discussion of list of questions**

Case 1:

Xiaoting (CMCC): presented the questions, thinks the answers to 1a) b) c) should be all Yes.

Mats (NDRE): agree.

Saurabh (Nokia): For internal AF, if the key is established outside the PLMN, the keys are obliged to be provided, correct?

Xiaoting (CMCC): Yes

Mats (NDRE): In those cases, agree that KAF is not needed to be provided, but it could be provided.

Varini(Samsung):question on 1 c), is this case similar to the home routed traffic, a roamer can connect to the AF in the HPLMN, don’t think in this case there are any keys provided to the VPLMN. Why in this case we are supposed to provide

Mats (NDRE): If you refer the solution to S8HR, the reasons that no keys are provided is GSMA roaming guidelines state in such cases, encryption shall not be used.

Andreas (Lenovo): question on 1 c), the encryption key is established at the application layer, how is the case different with the case of using HTTPS, why do we need to send the encryption key which is not derived from any of the 3GPP keys, why is this subject to LI?

Mats (NDRE): then why are you using AKMA if AKMA has no role in providing security for the UE. The point is in this case, AKMA is involved in establishing the keys, e.g., authentication between the client and the application server, the operator is actively assisting in establishing the keys hence the LI obligation applies.

Andreas (Lenovo): not sure we have that part in AKMA saying it is involved in authentication

Mats (NDRE): Maybe you could question if it’s an AKMA use case if AKMA is not involved.

Marcus (OPPO): considering the KAF refresh, which can rely on Ua\* protocol somehow as mentioned in SA3, once the KAF is refreshed, it’s different from the initial KAF, how would that be treated in LI?

Mats (NDRE): Anyhow the new KAF is established based on the previous AKMA context, AKMA is still the basis for the keys, the LI requirements still apply

Marcus (OPPO): So the LI requirement is to the AF, not to the core network, since the only place that the refreshed keys are known is AF.

Mats (NDRE): that doesn’t affect the LI requirements. Since AKMA is still to bootstrap.

Marcus (OPPO): just thinking whether the LI point would be AF or other elements.

Mats (NDRE): the transfer of the parameters has to involve the AF since it’s the one selecting the cipher suites, the point is the transfer from the HPLMN AF to VPLMN cannot be handled as an LI internal interface because it would break the principle of not having the inter PLMN LI interfaces, that transfer has need to be done by SBI. If there is a refresh, then the AF has to use the same interface to push the new key.

Mireille (Thales): In case of TLS, if the keys to establish TLS are not coming from operator, e.g. if it’s provisioned, the LI requirement do not apply, correct?

Mats (NDRE): If the operator key management in terms of UICC has no role, then yes, there are no LI requirements. But if the AF is internal to the HPLMN, then it doesn’t matter if the keys are coming from UICC or not, since HPLMN is providing encryption solutions somehow. Only the case the AF is external to all of the involved PLMNs, we don’t have LI that we are standardizing.

Vlasios (Ericsson): 1b) or 1c), the text saying KAF is not needed to be provided, do you have any suggestions on the actual wording of requirement, KAF may be provided or can be provided?

Mats (NDRE): The key and other parameters that are necessary to decrypt the traffic shall be provided, you could for example, if the key is directly derived from KAF, then you could either provide KAF and other parameters that are input to the derivation or the output the derived key itself.

Steven (?): Doesn’t this open a huge security vulnerability into AKMA? Any misuse, mishandling or compromise of the key transfer would break both integrity and confidentiality of the traffic.

Mats (NDRE): The integrity key and encryption key would be different, LI only targets the encryption key. For providing the encryption key, it has to be ensured that the minimum set of information is transferred.

Saurabh (Nokia): 1b), the new text, why do we need KAF then, think providing the encryption key is enough, if we provide the parent key, then KAKMA, KAUSF are going to be provided?

Mats (NDRE): the requirement is you either provide the final encryption key or KAF, etc., the point is you could provide KAF, but it may not be the best solution. Choose the approach that is much simpler.

Alex (BT, SA3-LI chair): It’s worth taking this question back in LI, whatever is the least revealing key that can be used to do and send a message to SA3. It’s for SA3 to figure out what is the minimum information set that need to be provided in order to fulfill the requirement. Regarding Steven’s question, maybe SA3 need to ensure that we specify key holding requirement, and how do we minimize the attack surface.

Mats (NDRE): If there are options of the keys being transferred, we may also need some flags identifying the keys that are transferred.

Case 2:

Xiaoting (CMCC): no additional requirement to HPLMN

Mats (NDRE): same understanding

Case3:

Mats (NDRE): this is a difficult case, assuming those AFs are authorized to obtain AKMA keys, they should have some connections with the HPLMNs, at least there are some agreements between AF and HPLMN, which may indicate some information about how the keys are used. Assuming the AF doesn’t cheat, then the HPLMN is assumed to know something. Then this will enable the VPLMN to do LI, but there is no guarantee. The only general solution is to promote operators only accept AFs that operators have agreement with on how to use the key.

Alf (Docomo): Do we have the same requirement for GBA? If we want to use GBA and AKMA for external entity. Don’t really see how this can work, especially if it’s used for TLS, after DH, everything goes out anyway.

Mats (NDRE): for GBA, the LI solutions in 33.107 and 33.108 are incomplete. Only handles the non-roaming case, doesn’t handle the case that NAF is in HPLMN and even external. Even for the non-roaming case, there are only stage 2 specs, no stage 3. We can’t use GBA LI solutions since it’s very complete.

The other part of the question, you might be right, if we are not going to provide an acceptable LI solution, we’ll end up in the same situation as S8HR. The roaming agreement will say that it’s forbidden for the encryption.

Alf (Docomo): for the internal AF, it’s ok. For the external one, it doesn’t matter that the roaming agreement is about encryption, external AF can do whatever they want, it’s not under control of the HPLMN. Don’t understand how would that work. What we could do is that we could say the same interface could be used, don’t see this will happen. It seems like we are doing more LI but less security when I do a facebook log, that’s not good.

Mats (NDRE): Agree that we have no control of the external AF, except for we have agreements that say how the AKMA keys are used, if the AF cheats, what HPLMN can do is to not provide keys anymore.

Saurabh (Nokia): Agree with Mats, there could be possible solutions we can work on. Also agree with Alf it’s challenging, but at least in standards we can define some procedures. 3GPP is exposing to 3rd party why can’t we provide the decrypt means back to the network.

Xiaoting (CMCC): asks whether do we exclude this case and say the LI requirements do not apply here or the LI requirements should be HPLMN providing the information that known to HPLMN.

Mats (NDRE): providing the information that are known to HPLMN, that’s the best we can do. The other sub-optimal solution, there could be an interface that the AF send back the actual encryption key.

Noamen (HW): Why couldn’t this be a problem to an application provider to provide the necessary information if they are subject to the same laws, why does this go to the operator.

Mats (NDRE): could be a legal intercept requirement to the 3rd party, but this is not helpful for the VPLMN operator. There are 3 jurisdictions involved, HPLMN, VPLMN and third party, the police authority can request information from the AF, that’s not helpful for the lawful enforcement in the VPLMN jurisdiction, unless they have some inter county agreement. The problem here is the LI in the VPLMN which is dependent on both HPLMN and external AF.

Saurabh (Nokia): the red line that added, does that mean HPLMN provide that information they know or they can try to get whatever they can then provide the encryption keys to VPLMN?

Xiaoting (CMCC): the former.

Mats (NDRE): Usually no requirements to acquire information in the LI standard.

Saurabh (Nokia): then there will be problems to decrypt the traffic if only KAF is provided.

Mats (NDRE): yes it may not be sufficient to only provide KAF, there’s guarantee

Xiaoting (CMCC): that’s all what the operator can do.

**Agenda 3: draft contribution on addressing the EN of KI#1 in TR 33.737**

Xiaoting (CMCC) presented the changes

Vlasios (Ericsson): the text “shall” means these text fit more into the security requirement part?

Andreas (Lenovo): change “shall” to “need to”?

Mireille (Thales): Are the added text exactly the security requirements or what is the intention of these texts? If these are actual security requirements to be met, they should be moved to the right place.

Xiaoting (CMCC): the reason not mandating them as the security requirements is that these need to be met only if SA3 decide the solutions are providing means to decrypt traffic. If SA3 leans towards disable the encryption as a solution, then these requirements are not applicable. So the texts are more like explaining the specific LI requirements.

Noamen (HW): the text may need refinements, will send out offline.

Xiaoting (CMCC): welcome any offline comments or modifications to the key issue before submission, and this version of the key issue is expected to be the basis for proposing solutions from the next SA3 meeting.