2021-07-26

Minutes of the second teleconference for AMF re-allocation for the SA3#104-e

--------------------------------------------------------------------------

--------------------------------------------------------------------------

Active participants:

Minpeng Qi (China Mobile, CMCC), Alf Zugenmaier (DOCOMO), Juan Deng (Huawei) , Sheeba Baskaran (Lenovo), Kundan Tiwari (NEC), Adrian Escott (Qualcomm Inc.), Rajavelsamy Rajadurai (Samsung), Taehyung Lim (Samsung), Vlasios Tsiatsis (Ericsson, organizer)

--------------------------------------------------------------------------

Agenda for this teleconference

Agenda

1) Discussion of input documents on [Directory Listing /ftp/Email\_Discussions/SA3/TSGS3\_104e/AMF-reallocation/teleconference2 (3gpp.org)](https://www.3gpp.org/ftp/Email_Discussions/SA3/TSGS3_104e/AMF-reallocation/teleconference2)

- Samsung: Proposed Way Forward

- Huawei:

 a) Discussion paper on the full registration request message to be rerouted

 b) Discussion paper on security context transfer via RAN

2) Discussion of the AMF re-allocation evaluation criteria document.

- Continue the discussion from teleconference #1 on the contents of the evaluation criteria paper

- Plan for submission for the evaluation criteria paper (who?, what?)

-> This was not discussed

3) AoB

--------------------------------------------------------------------------

--------------------------------------------------------------------------

Agenda item (1)

---

**- Input document from Samsung: Way Forward**

(Samsung) presented the discussion paper

(Lenovo) Question for Case 1. The context to be exchanged is defined to include 5G-GUTI, SUCI. What is the intention of this case ?

(Samsung) Case 1 is the case the initial AMF (iAMF) and the target AMF (tAMF) do not exchange any information at all including the SUCI or 5G-GUTI of the UE.

(Lenovo) SA2 has described the Registration Request (RR) transfer which includes 5G-GUTI or SUCI.

(NEC) Are these isolation cases based on SA2 criteria ?

(Samsung) We could check with SA2.

(NEC) Fine with sending an LS to SA2.

(Huawei) Case 1 and Case 2 are not much different

(Samsung) In Case 1 is there is no communication between AMFs. UE is the potential connecting point of the two AMFs. In Case 2 the RAN node is the connecting point of the two AMFs and the AMFs can perform via RAN rerouting. The via RAN rerouting is not much different from the direct rerouting.

(Qualcomm) Don't see the difference between case 1 and case 2 from a security perspective. All cases rely on the iAMF doing the right thing. Routing via RAN is an enabler.

(CMCC) For those 4 cases, it is ok but prefer to merge to 2 cases, i.e. without security context transfer and with security context transfer. I think that is enough.

(Huawei) We think that sharing the security context or not makes the difference.

(CMCC) For isolation, I want to point out that that is already discussed in SA2 since R15. They defined option A and option B. Option A can provide communications between AMFs, and that is already discussed and provide security solutions. For option B, that assumes AMF could not transfer, that is why we need to transfer sth. via RAN, and that is the case we need to solve here. So isolation is of course not the evaluation. It is precondition.

(Ericsson) We don't have any requirement from other groups e.g. SA1 about isolation that this makes the isolation discussion difficult.

(Samsung) Agree with Ericsson that we don't have SA1 requirements. Case 1 is about iAMF not trusting tAMF and the iAMF does not give anything tAMF.

(Ericsson) I believe that Case 1 is the main point of this discussion paper that we have not discussed before in the study.

(Qualcomm) What is the security threat when the iAMF does not give anything to the tAMF?

(Samsung) It is the other way around. If the iAMF does not provide anything to the tAMF what solution do we have in the study ?

(Lenovo) In Case 1 the UE related data are SUCI/5G-GUTI coming from the UE, cannot understand case 1. We cannot see the reason why the iAMF cannot send anything to the tAMF. What is the threat of Case 1?

(Samsung) In Case 1 the iAMF and tAMF are not allowed to exchange anything and this case needs to be captured.

(Ericsson) Just for my clarification. Is the Registration Request allowed to be exchanged between AMFs?

(Samsung) No RR forwarding is taking place in Case 1.

(Huawei) Case 1 breaks the user experience and operators will not accept it.

(Samsung) There is a case that the iAMF and tAMF cannot talk to each other and this scenario needs to be captured. We are trying to capture a requirement that does not exist.

(Ericsson) Let's move on to the next discussion paper.

**- Input document from Huawei: Discussion paper on the full registration request message to be rerouted**

(Huawei) presented the discussion paper.

(Ericsson) thank for the discussion paper. What is the intention of the discussion paper ?

(Huawei) The purpose is to bring a pCR to the TR 33.864, clause 4.3 to clarify this information.

(Qualcomm) Not clear about the purpose of the paper either. If the full RR (unencrypted) is transferred via RAN then the iAMF reveals to the RAN information elements (IEs) that are supposed to be protected.

(Huawei) Do you agree that the RR in the NAS SMC is plain NAS message?

(Qualcomm) Yes but what is the justification of breaking the security model ?

(Huawei) iAMF has the full RR in step 5.

(Qualcomm) The iAMF has the INITIAL UE message

(Ericsson) Is this discussion paper trying to address the potential discrepancy in 23.502 (stage 2) and NGAP (stage 3, 38.413) about the INITIAL UE MESSAGE?

(Qualcomm) I don't believe that we analyzed all the cases of the via RAN option.

Doing something like this we expose the Information Elements (IEs) that RAN does not need to have access to

(NEC) RR in step 1 is in the RRCComplete message in clear text. In Step 9a the RR is the same as in Step 1.

(Huawei) NEC talked about the 5G-GUTI case in step 1. For the 5G-GUTI case the RR in step 9a is the RR in the NAS container in Step 1.

(NEC) How does the tAMF perform integrity protection verification of the RR ?

(Huawei) the verification will fail

(Qualcomm) This is bringing a new thing in the specification.

(Ericsson) We should move on to the next discussion paper. All companies should consult their CT1, CT4 colleagues

(Huawei) These procedures are SA2 procedures and SA2 should be consulted.

(NEC) CT1 designs the UE messages and they should be consulted as well.

(Ericsson) Let's all consult internally our CT1 and SA2 colleagues for this discussion paper proposal and sort out unclear points.

**- Input document from Huawei: Discussion paper on security context transfer via RAN**

(Huawei) presented the discussion paper.

(Samsung) With respect to observation #3, why does solution #10 is indicated that exposes security context ?

(Huawei) NAS security context at the RAN node is a security risk

(Qualcomm) Why do you consider protected security context via RAN node a security risk ? Why does encrypted data become less secure if sent via RAN encrypted ?

(Ericsson) Is it considered a security threat if security context is stored encrypted on the RAN node ?

(Huawei) We don't want to compare solutions #2, #9, #10, we bring up the point of transferring security context via RAN.

(NEC) If a RAN node cannot read the security context what is the risk ?

(Huawei) An attacker can get the encrypted security context and could decrypt the message.

(DOCOMO) If the decryption key is not available to the RAN node the RAN node cannot decrypt. Unless the attacker has access to the keys to break the encryption what is the problem we are going to have here?

(Ericsson) The RAN node may not know what is sent via RAN.

(Lenovo) Would like to make the comment that the RAN node will know what is sent i.e. the information elements, since it would be specified if we chose to go with such a solution that transfers security context via RAN.

(Huawei) Security management is about threat probability times the cost of exploitation. What we are proposing is to minimize the threat of exposure of security context by not allowing it to be transferred via RAN.

(DOCOMO) If the security context is encrypted, what is the security context "exposed" ?

(NEC) There is a way for the RAN node not to know what is being transferred if there is a generic Information Element being used as a container in the message to the rerouted.

(Ericsson) In any case the RAN node may know what is being transferred so we should not probably focus on this aspect. Huawei is trying to make the point that no security context transferred, whether plain text of encrypted should be transferred via RAN. I don't fully agree with this principle since encrypted security context is not useful to a RAN node unless, as DOCOMO said the RAN node has access to the decryption key.

(Huawei) The risk is higher if the security context is passed via RAN. The security context in certain cases is passed encrypted between core network functions but the risk of this procedures is less than passing the security context encrypted via RAN.

(DOCOMO) We are making things complicated and I would prefer a simple solution for this issue (AMF re-allocation).