**FS\_eNPN\_SEC conf call 210413**

**Attendance:** Juan Deng (Huawei), Anand Palanigounder (QC), Thomas Pätzold (DT), Wei Lu (Xiaomi), Fei Li (Huawei), Mingpeng Qi (CMCC), Duckey Lee (Samsung), Ivy Guo (Apple), Helena Vahidi (Ericsson), Ru Yan (CMCC), Rong Wu (Huawei), Alf Zugenmaier (NTT DOCOMO), Mireille Pauliac (Thales), Huli (Huawei), Bo Zhang (Huawei), Yi-Hsueh Tsai (CSTI), Jun Shen, Hongjin Choi, He Li (Huawei), Longhua Guo (Huawei), Bo Bjerrum (Nokia), Christine Jost (Ericsson)

(attendance according to Teams meeting chat record, affiliation according to my knowledge)

**Agenda:**

* Conclusions to KI#1
* Authentication methods support in serving network
* Conclusions to KI#4
* LSes in from SA2

**S3-21bbbb**

Nokia: Don't see need for interworking function. What is the motivation for it?

QC: Optional proxy was included in previous version of conclusion. Reason: Depends on trust relationship between AUSF and external entity (CH). When there is no high level of trust, proxy can be used. Optional. Stateless proxy. Towards AUSF, uses AAA interfaces or SBA.

Ericsson: AUSF should be fully service-based. Interworking function is translation functionality. Can explain why we do not see security concerns with interworking function.

Nokia: Not so much about security concerns. Interworking function can be built into the AUSF. Security concerns: translation function translating radius increases trusted computing base. Also, see further functionality and complexity. Third: need TLS between the endpoints. Don't want man in the middle that we need to trust.

CMCC: On privacy concern with intermediate node, also deployment related issues. Do not want to expose system function to the outside. Need intermediate node.

QC: Minpeng explained it well, this was the motivation. Reply to Bo: It's up to deployment. These are all functions, can be in same box or different.

Ericsson: Try to make progress by keeping non-security aspects in SA2, discuss security aspects. Trusted computing base, complexity increases with both options. Whether new protocol is too complex is up to SA2. In 3GPP network, many NFs handle session keys, nothing new.

Nokia: To some parts Nokia disagrees with. Important part: not necessarily rooted in security concern. More an SA2-discussion.

**S3-21aaaa**

QC: some operators disagree with EAP-TTLS, so keep as separate discussion. Putting both together problem for progress. Already have EAP-TLS in informative Annex, could potentially enhance with EAP-TTLS. For progress, keep EAP-TTLS discussion separate from MSK discussion. Independent issue.

Huawei: Cosigns. EAP-TTLS should be separate topic for moving forward.

QC: Suggest to rapporteur to request early decision by chair, e.g. by Tuesday.

Ericsson (rapp): Good proposal.

**S3-210372**

Huawei: 33.501 for roaming, home UDM selects the authentication method based on UE IE. Does not consider authentication method supported by the serving PLMN. With SNPN, support of authentication methods is flexible. "may support 5G AKA, EAP-AKA' or any other generating key generating EAP-method". When SNPN is serving network, home network needs to consider what is supported by serving SNPN. If home UDM considers UE ID, serving SNPN may not support authentication method. Proposed solution is that supported authentication method is configured at home UDM. Different interpretations on requirements for SNPN.

QC: Our position is still the same. Both UE and PLMN support 5G AKA and EAP framework. For SNPN, the requirement was relaxed in Rel-16, because roaming was not considered. Either 5G AKA or EAP framework. Serving network consists of AMF, so main requirement from PLMN case still holds. Should be clarified. Otherwise the whole point of introducing EAP framework is gone. Suggestion to clarify in Annex to TS 33.501. Otherwise AMF would need to be upgraded when new requirements are brought. QC plans to bring a CR, hopefully to be shared in advance.

Nokia: Challenging part is the roaming case. Agree with QC. Nokia view is that AMF needs to be algorithm agnostic, just pass-through of all the parameters (RES, XRES). Impossible to update AMF with new authentication algorithm otherwise.

Ericsson: That's the beauty of EAP-framework, just need to support EAP at the AMF and all EAP-methods will be supported. Requirements from PLMN case translate to SNPN case. Would be good to see the CR.

Huawei: Not proposing to abandon EAP framework. Should proposing that SNPN should have the flexibility to support 5G AKA or EAP. UDM needs to consider what is supported in the SNPN.

QC: AMF should not need to care. Therefore support 5G AKA and EAP at AMF. That capability is already there. So that UDM can deploy whatever they want without caring about AMF. Relaxed requirement in SNPN, because factory may only want to support EAP. In the case of roaming, it's important that AMF supports both.

Huawei: For the serving network able to roam with home network, only requirement should be that one authentication method is common between serving and home network.

QC: Yes, only requirement is EAP and 5G-AKA. Relaxed requirement is for UDM, can deploy any key-generating EAP method. Flexibility not on AMF side. Will share CR and discuss offline.

**S3-21cccc**

QC: similar with our proposal from last meeting, so inline. Proposals to support other methods could be considered separately, on top of this.

Nokia: Cannot agree to having mutual authentication. Of course what is already there is supported. Provisioning protocol is out of scope, this protocol will have mutual authentication. For example OPC UA, it already has discovery service etc. No need to have additional complication. Of course, other methods proposed last meeting require mutual authentication. But do not overcomplicate cases that are already secure. E.g. AKMA has mutual authentication as prerequisite.

QC: All agree that existing primary authentication can be used. On top of this, legacy AAA from key issue 1, with mutual auth between UE and AAA. If Nokia thinks this needs to be supported, should be ok. The issue is whether there is agreement to support network-only authentication. Suggestion to agree on partial conclusion. Need partial progress or SA2 may drop the topic.

Huawei: Mutual authentication is necessary. Do not think one-way is secure enough. Risk with man in the middle attack before onboarding procedure.

Ericsson: Intention is to have minimal conclusion for progress. Only describes what can be done. Please drive additional conclusions separately.

Nokia: Currently not willing to accept this conclusion. Planning to come back with rephrased proposal.

**S2-2101077**

QC presents. Question is which procedure to use, UPU or SoR.

QC: Security-wise they are similar. Prefer UPU, because it is meant for updating parameters, while SoR is more for steering of roaming. SoR seems to be non extensible. Even from security pov SoR less extensible. Can extend to include parameter update without affecting serving network. SoR mainly done during registration, also in that perspective UPU more flexible.

Ericsson: prefer SoR, because it can be used during and after registration.

QC: any security concerns?

Ericsson: No, security-wise they are very similar. Leave to CT1 colleagues.

**S2-2101072**

QC presents.

QC: KI#2 no progress. Need to agree whether to specify provisioning protocol. According to SA2 it is out of scope. If to be specified, what will the right protocol for UPU? Mutual authentication e2e is usually required for provisioning protocols. Proposal: In Rel-17 provisioning will be out of scope for the sake of progress.

Ericsson: Should UPU be extended or new specified?

QC: Problem is it's not sure whether KI#2 is in scope? We have to answer whether CP provisioning is ok. With all these changes, not sure whether it will be UPU. Also dependent on authentication method (e.g. PAP/CHAP, certificates). Not sure whether this is feasible.

Ericsson: Action is to find a solution.

QC: It may not be possible to find a solution. Plan to provide discussion paper. Propose to drop CP provisioning in Rel-17. Would need to agree on authentication method first.

Nokia: Not in favor of CP-based provisioning. Industry that is going to adopt the functionality would like to bring their own existing functionality.

QC: agree with Nokia, industrial players would have their own provisioning protocols. If they have initial access, can use to run their own provisioning protocols. GSMA RSP, UPC UA, IETF and enterprise provisioning protocols. For Rel-17, progress on initial access should be sufficient.

**Next call:** Proposal to discuss WID