# eNPN security conf call 210119

**Agenda:**

**5.00 – 5.45  UTC**

|  |  |  |
| --- | --- | --- |
| [**S3-210494**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_102e/Docs/S3-210494.zip) | pCR: Security architecture conclusion for KI #1 | Qualcomm Incorporated |
| [**S3-210340**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_102e/Docs/S3-210340.zip) | High-level conclusions for KI#1 (Credentials owned by an external entity) | Ericsson |
| [**S3-210346**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_102e/Docs/S3-210346.zip) | High-level conclusions for KI#1 (Credentials owned by an external entity) | Ericsson |

|  |  |  |
| --- | --- | --- |
| [**S3-210343**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_102e/Docs/S3-210343.zip) | draft LS on Feedback on function supporting primary authentication and authorization of SNPN UEs that use credentials from the AAA Server | Ericsson |

The main goal is to try to find conclusions for our Key Issue #1 that help SA2 to progress their work.

**5.45 – 6.00 UTC**

|  |  |  |
| --- | --- | --- |
| [**S3-210406**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_102e/Docs/S3-210406.zip) | LS on Feedback on Key Issue #4 "UE onboarding and remote provisioning" | Ericsson |

The main goal is to start the discussion. Main goal for the later email discussion is to try to identify agreements that help SA2 to progress their work.

**Attendees:** (according to Teams meeting chat, in order of joining the meeting)

Helena Vahidi (Ericsson), Christine Jost (Ericsson), Baruch Pinto (Allot), Lu Fei (Huawei?), Bo Bjerrum (Nokia), Nivedya (Samsung), Rong Wu (Huawei), Huli (Huawei), Bo Zhang (Huawei), Ivy Guo (Apple), Anand Palanigounder (Qualcomm), Abhijeet Kolekar (Intel), Alf Zugenmaier (NTT DOCOMO), Mireille Pauliac (Thales), Rajavel (Samsung), Rohini (Samsung), Xiaobo Yu (Alibaba), Chunhui Zhu (?), Minpeng Qi (CMCC), SungDuck (LGE), Wei Lu (Xiaomi), Yi Zhang (?), Duckey Lee (Samsung)

**Notes:**

**S3-210494 (QC)**

In case that the external entity is 5GS aware (i.e., capable of deriving 5G key hierarchy after a successful primary authentication), it is concluded that the existing 5GS roaming architecture is reused.

[QC] Can use existing 5G roaming architecture, nothing new.

[Eri(HV)] "Home network" has AUSF and UDM?

[QC] Yes

[QC] Is this agreeable?

[Eri(CJ)] Silence, so it seems to be agreeable.

[DCM] Roaming architecture refers to only key hierarchy?

[QC] whole security architecture

[Eri(HV)] clarification?

[QC] Existing security architecture in 33.501, serving network and home network split. There may not be roaming depending on the relation between SNPN and external entity.

[DCM] Also other policies? Integrity protection policy?

[QC] Which integrity protection, SBI?

[DCM] UPIP deployed, PCRF?

[QC] UPIP is already mandatory, no reason to relax. Also policies don't change.

[DCM] complete access to UDM?

[QC] If I am not mistaken, this is SA2 conclusion.

[DCM] interconnect?

[QC] not in our scope, but SA2 has concluded to re-use Rel-16. They just wait for us to conclude on external entity.

[DCM] Is SNPN still standalone then?

[QC] In some sense, but uses PLMN. Serving SNPN and home SNPN/PLMN.

[DCM] what is the difference between serving SNPN and serving PLMN.

[QC] There are four different deployment options now. Only case not possible in Rel-16 is non-5GS aware AAA.

[DCM] What does it mean for interconnect security?

[Eri(CJ)] We note that interconnect security needs further discussion.

In case that the external entity is non-5GS aware (legacy AAA server), the following is concluded:

* The SNPN access with a credential owned by an external entity is performed via an AUSF proxy function (AUSFp) in the SNPN.

[QC] Proposal is to use AUSF and enhance with necessary functionality. In the solution it is called AUSF\*. If the credentials hosting functionality is 5GS aware, the AUSF\* would not do any functionality, KAUSF can be derived by 5GS aware network.

* The AUSFp transports EAP authentication messages between the UE and legacy AAA server and creates the necessary 5G keys (e.g., derives KAUSF and KSEAF) based on the MSK received from the legacy AAA server.
* Depending on the trust relationship between the SNPN and the external entity, the AUSFp may either interface directly to the external entity or through another network function for security isolation purposes, which is left to the SNPN decision.

[Eri(CJ)] seems to be disagreement

[QC] what is the disagreement? Our proposal was to leave it up to deployment. Does Ericsson disagree?

[Nokia] Also want to enhance AUSF. Do not believe that other functionality in between improves security. Will just add complexity and new protocols that need to be hardened. Inline on enhancements of AUSF.

[QC] understand point about SBI, protocol translation. My point is that it is up to deployment. Just like for NSSAAF. We are neutral on whether AUSF speaks AAA or SBI protocol. Depends on deployment. If isolation is required, could have the additional function in between. Would that be acceptable?

[Eri(CJ)] Is your understanding that NSSAAF is a similar case?

[QC] isolation function and protocol translation are different question.

[Eri(HV)] Ericsson wants AUSF pure SBI function and keep protocol translation external.

[Nokia] Nokia has the opposite opinion. Keep the functionality in the AUSF, utilize protocols directly from the AUSF.

[Eri(HV)] What is the consequence of having it optional?

[Nokia] One would still have the problems mentioned before.

[QC] Agree with Nokia about translation. If AUSF does not provide translation, need to have translation function. But isolation could be optional. If AUSF provides translation, proxy would just be for isolation. Standardization only necessary if there is translation. What is Huawei's position?

[Hua] Not strong opinion, depends on deployment whether isolation and translation is required.

[Eri(CJ)] NSSAAF as specified, does it provide the optionality as proposed here?

[QC] No, because NSSAAF does not connect to AAA servers, just talks SBI. From our point of view, question is whether AUSF speaks AAA or not.

Editor’s Note: Further conclusion(s) are FFS.

**S3-210346 (Eri)**

The primary authentication procedure in TS 33.501 [2] is re-used, with the following changes: the AUSF does not perform the authentication itself but relays the authentication procedure between the external entity and the UE. A new interface is introduced between the AUSF and the external entity, via an intermediate function that provides AAA interworking, as proposed in solutions #1, #2, #5 and #7. The new interface via the intermediate function is used for sending both EAP-messages and other data, e.g. keys.

A solution for the support of a legacy AAA server that supports any key-generating EAP-method will be specified during normative work. The MSK will be used as the root key for 5G key hierarchy as described in solutions #1, #5 and #7. A deployment recommendation needs to be included in the specifications: it is strongly recommended that the same credentials that are used for authentication towards a 5G SNPN are not used for authentication towards a non-5G network.

**S3-210343 (Eri)**

1. "- The SNPN will host a function (e.g. enhanced AUSF or new NF) supporting primary authentication and authorization of SNPN UEs that use credentials from the AAA Server.

NOTE 1: Whether to use a new NF or enhanced AUSF will be determined based on feedback from SA WG3."

[QC] Legacy case, enhancement is KAUSF calculation.

Background information for SA3, to be removed before sending to SA2: All solutions for Key Issue #1 "Credentials owned by an external entity" in TR 33.857 assume that the AUSF is involved in the authentication procedure. All solutions introduce a new interface between AUSF and AAA server, some directly and some via an intermediate function.

SA3 feedback:

a) In the 5G architecture, primary authentication is performed by the AUSF. Therefore, the AUSF should be involved in the primary authentication procedure also for SNPN UEs that use credentials from the AAA Server.

[QC] legacy AAA server (or some other term like 5GS non-aware)

[Eri(CJ)] fundamental disagreement? Seems to be agreeable in this group

b) The AAA Server is an entity external to the SNPN. From a security point of view, it is recommended to not directly expose the AUSF to communication with an external AAA Server. Instead, an intermediate function (AAA interworking function) could be used between the AUSF and the external AAA Server. This function would be very similar to the NSSAAF, because it performs AAA protocol interworking with the AAA Server (i.e. translate the service-based messages from the AUSF to AAA protocols towards the AAA Server).

2. Editor's note: Need for and details of using a UE ID other than the SUPI are FFS.

Background information for SA3, to be removed before sending to SA2: Important input for feedback to this question are the solutions to Key Issue #1 "Credentials owned by an external entity" in TR 33.857. The situation is not completely clear, but at least several of the solutions agree on that SUPI and SUCI are used.

SA3 feedback: It can be assumed that the UE ID is a NAI. Hence, from an SA3 point of view, it can be assumed that the UE ID is a SUPI.

[Nokia] Fine with utilizing same structure. However, SA2 uses sometimes SUPI and sometimes SUCI. Important point is that there is no leakage of identity. Proposal to use SUCI. How (ECIES or other scheme) is to be discussed. Do not send identity in plaintext. SUPI using anonymous scheme could also be fine.

[Eri(CJ)] Do you believe anything new is needed compared to 33.501, with SUCI privacy and option to use privacy provided by EAP-methods like anonymous id

[QC] Do not see that anything new is needed in Rel-17. SUCI is a fundamental part of the architecture. There are related discussions in SA1 (on regulator requirements). Need to wait for further input.

[DCM] Is the discussion about not sending SUCI, sending SUPI earlier? Or about sending SUPI to SNPNs?

[QC] Whether sending SUPI to SNPN is another question. For everything else, it seems that no-one challenges what is in TS 33.501. Depends on whether UE is configured with necessary info.

[Eri(CJ)] For SUPI privacy over the air, is there agreement to use Rel-16 TS 33.501?

[Nokia] Can we add that SUCI will be concealed? Both for devices with UICC and devices without UICC?

[QC] Possible, but for non-UICC it is left to the EAP method. Because key storage is out of scope.

[Nokia] In the EAP-method, will the first message contain plaintext SUPI?

[QC] No, if UE is configured to use privacy it will be an anonymous SUPI. Even with null-SUCI scheme, SUPI will be sent in clear.

**S3-210406 (Eri)**

1)

Editor's note: In order to support UE onboarding using Default UE credentials and O-SNPN as the Onboarding Network (ON) the distribution of security functions when primary authentication is used should be decided by SA WG3, e.g. whether and how to support the primary authentication based on default credential in case DCS is deployed or not.

Background information for SA3, to be removed before sending to SA2: All solutions for Key Issue #4 "Securing initial access for UE onboarding between UE and SNPN" in TR 33.857 assume that default credentials are provisioned in the UE and primary authentication with the DCS using the default credentials is performed. Also, three of four solutions provide further details, they assume that the AUSF is involved in the authentication procedure, and that the DCS is connected to the AUSF either directly or via an intermediate function.

SA3 feedback: SA3 confirms that, for the support of UE onboarding, primary authentication with the DCS based on default credentials pre-provisioned in the UE needs to be performed. The AUSF is involved in the primary authentication procedure. The DCS is connected to the AUSF either directly or via an intermediate function.

[Nokia] Besides the last sentence, ok.

[QC] seems reasonable, except last sentence.

[Intel] Network authentication instead of primary authentication.

[QC] Conclusion could be for the case that primary authentication is used. If there should be a case without primary authentication is ffs.

[Intel] Also if secondary authentication is used.

[QC] Using secondary authentication is not concluded. Do you believe that there should not be an option with primary authentication?

[Eri(CJ)] Is the following agreeable: Primary auth can be used, and if it is used …

[QC] If primary authentication is used …

[Intel], [QC] discuss formulations

Wordsmithing

SA3 confirms that, for the support of UE onboarding, authentication with the DCS based on default credentials pre-provisioned in the UE needs to be performed. When primary authentication is used, The AUSF is involved in the primary authentication procedure.

[Thales] if primary authentication is not used, what is the alternative?

[QC] Intel has proposals using secondary authentication.

[Intel] Our second proposal uses primary authentication.

2)

Editor's note: DCS is potentially introduced to authenticate a UE with default UE credentials or provide means to another entity to do it. There are two potential mechanisms for DCS to authenticate the UE. 1) DCS interacts with O-SNPN and Network Function in SO-SNPN (Subscription Owner SNPN) is not involved in the authentication procedure. As a result, the SO-SNPN is not directly involved with the authentication procedure but gets informed of its result and then performs remote provisioning. 2) DCS interacts with SO-SNPN and Network Function in SO-SNPN (Subscription Owner SNPN) is involved in the authentication procedure. As a result, the SO-SNPN is directly involved and aware of the result of authentication procedure and performs remote provisioning. SA WG3 needs to evaluate the two above mechanisms from security perspective and provide feedback.

Background information for SA3, to be removed before sending to SA2: This is related to Key Issue #2 "Provisioning of Credentials" in TR 33.857. In order to give feedback to SA2, it is essential that the Key Issue is completed so that solutions addressing this Editor's Note can be studied. There is also a relation to Key Issue #4 "Securing initial access for UE onboarding between UE and SNPN" in TR 33.857, as the Editor's Note is about the authentication procedure. However, the aspects how the SO-SNPN is related to the authentication procedure have not yet been studied in the context of Key Issue #4.

SA3 feedback: SA3 will provide feedback when SA3's study has progressed further.

3)

Editor's note: It is up to SA3, whether DCS can interact with PS after the primary authentication for provisioning.

Background information for SA3, to be removed before sending to SA2: This is also related to Key Issue #2 "Provisioning of Credentials" in TR 33.857.

SA3 feedback: SA3 will provide feedback when SA3's study has progressed further.

4)

Editor's note: The decision on whether primary authentication is required during initial access to the O-SNPN is dependent on SA WG3 feedback; until this feedback is received, it is assumed that such authentication is required.

Background information for SA3, to be removed before sending to SA2: This is again related to Key Issue #4 "Securing initial access for UE onboarding between UE and SNPN" in TR 33.857. The answer to Editor's Note 1 also applies here.

SA3 feedback: As pointed out above, primary authentication is required during initial access to the O-SNPN.

 [Eri(CJ)] update according to wordsmithing above

5)

Editor's note: SA WG3 should provide feedback on whether the UEs permanent identifier (SUPI or SUCI) may be used for finding the DCS identity or address/domain that can authenticate the UE, as well their security properties.

Background information for SA3, to be removed before sending to SA2: This is again related to Key Issue #4 "Securing initial access for UE onboarding between UE and SNPN" in TR 33.857. All solutions to Key Issue #4 assume that default credentials providing SUPI and SUCI are provisioned in the UE.

SA3 feedback: It can be assumed that the identifier contained in the default credentials is a NAI, i.e. it has the same format as a SUPI of type NSI. Even when SUPI privacy with a non-null scheme as specified in clause 6.12.2 of TS 33.501 is used, the realm will be in cleartext. Hence the SUPI/SUCI (using Rel-15/16 terminology) can be used to find the DCS.

 [Nokia] Realm is always in cleartext, regardless of whether SUPI/SUCI.

[Eri(CJ)] That was the intention in the above text, needs to be clarified.

6)

Editor's note: SA WG3 feedback will need to be taken into account for including of the CP based provisioning.

Editor's note: SA WG3 to determine whether and how Control Plane based provisioning using UE Parameters Update (UPU) procedure and User Plane provisioning can support devices without UICC i.e. how to secure the provisioned credentials between the PS and an endpoint in ME.

Editor's note: SA WG3 feedback for the suitability of the procedure will need to be taken into account.

Editor's note: whether an extra security layer for protection of credentials between PS and UE is needed should be decided by SA WG3.

Editor's note: The vertical may verify the UE before PNI-NPN credential is provisioned to UE, and how this is done should be decided by SA WG3.

Editor's note: for PNI-NPN credentials remote provisioning, whether the 3GPP operator could decide to update the UE Subscription Data (e.g., S-NSSAI, DNN, CAG information) in the UDM/UDR used to access to the PNI-NPN based on the input from the vertical which may be outside 3GPP operator domain should be decided by SA WG3.

Background information for SA3, to be removed before sending to SA2: These Editor's Notes are also related to Key Issue #2 "Provisioning of Credentials" in TR 33.857.

SA3 feedback: SA3 will provide feedback when SA3's study has progressed further.