**3GPP TSG-SA3 Meeting #99e *S3-201120***

**e-meeting, 11 – 15 May 2020** Revision of S3-20xxxx

**Title:** Draft LS reply to CT4 LS on Multiple Kausf upon registering via multiple SNs

**Response to:** S3-200915/C4-202348

**Release:** Rel-16

**Work Item:**

**Source:** SA3

**To:** CT4

**Cc:**

**Contact Person:**

#### Name: Juan Deng

**Tel. Number:**

E-mail Address: dengjuan5@huawei.com

**Send any reply LS to: 3GPP Liaisons Coordinator,** [**mailto:3GPPLiaison@etsi.org**](mailto:3GPPLiaison@etsi.org)

**Attachments:**

**1. Overall Description:**

SA3 thanks CT4 for the LS on Multiple KAUSF upon registering via multiple Serving Networks.

SA3 would like to confirm that, only one KAUSF (latest one) is maintained in the AUSF and in the UE, as KAUSF is security association between the UE and the HPLMN. The AUSF in home PLMN never maintains two KAUSF, when a user is simultaneously registered in two Serving Networks via different access-types (3gpp and non-3gpp).

The stored KAUSF does not have any dependence on a serving network, even though KAUSF derivation uses Serving Network ID as an input (SN ID is included for backward compatibility with pre Rel-15 UICC). Further keys derived from KAUSF are serving network specific, but KAUSF is not specific to a serving network and it’s the key associated between the UE and the home network.

SA3 would like to correct the CT4 CR assumption on the clause 6.3.2.1 of TS 33.501 that, based on the definition of the 5G security context (clause 3.1 of TS 33.501), 5G security context is between the UE and the Serving network and KAUSF is not part of the 5G security context:

***5G security context:*** *The state that is established locally at the UE and a serving network domain and represented by the "5G security context data" stored at the UE and a serving network.*

*NOTE 1: The "5G security context data" consists of the 5G NAS security context, and the 5G AS security context for 3GPP access and/or the 5G AS security context for non-3GPP access.*

Therefore, UE shall independently maintain and use two different 5G security contexts (5G NAS security context and the 5G AS security context (s)), one per PLMN's serving network, but the UE and the HPLMN maintains only one KAUSF based on the most recent successful authentication. SA3 does not see the need for maintaining multiple KAUSF in the UE and in the HPLMN. Further keeping the old keys laying around in the network is not a good security practice.

It is SA3’s understanding that

* UDM stores the authEvents for both serving networks in multiple registrations. UDM selects the AUSF reporting the most recent successful authentication result.
* To prevent the SoR and UPU failure in the case where the UE having multiple registrations de-registers from the new serving network,
  + AUSF and UE stores the newest KAUSF after UE deregistration;
  + UDM, when deleting the authentication results for the new serving network, keeps the AUSF info in the authEvent.

SA3 would like to provide the following clarifications for the CT4 questions;

1. When two different AUSFs are selected by the two serving PLMNs, how does UDM handle the SoRProtection or UPUProtection services – how does UDM select which AUSF to talk to?

***SA3 response:*** The UDM selects the latest AUSF which served the UE and maintains the latest KAUSF, for SoRProtection or UPUProtection services. The UDM selects the latest AUSF, irrespective of the serving network to which the SoRProtection or UPUProtection services is to be provided.

1. When same AUSF is selected by the two serving PLMNs, does AUSF only save the latest Kausf?

***SA3 response:*** Yes, the AUSF stores only the latest KAUSF upon successful authentication procedure and deletes any stored old KAUSF.

1. Does UE only store the latest Kausf in multiple registrations?

***SA3 response:*** Yes, the UE stores only the latest KAUSF upon successful authentication procedure and deletes any stored old KAUSF.

SA3 would like to add any clarification in relevant specification text in the next meeting, considering CT4 changes if any.

SA3 would like to ask CT4 to evaluate if there are the backward compatibility issues caused by the above the understanding, and inform SA3 if any. In addition SA3 would like to ask CT4 to specify the SA3 recommended behaviour if there are no issues.

**2. Actions:**

**To CT4 group.**

**ACTION:** SA3 kindly asks CT4 group to take the above information into account and inform SA3, and specify the SA3 recommended behaviour if there are no issues. if CT4 identifies any backward capability issue.

**3. Date of Next TSG-SA WG3 Meetings:**

SA3#100e 6 -10 July 2020 e-meeting

SA3#100e-Bis 17 – 21 August 2020 e-meeting