**3GPP TSG-SA3 Meeting #105e draft\_S3-214213-r1**

**e-meeting, 08 – 19 November 2021**

**Source: Ericsson**

**Title: Conclusion for control plane solutions for KI#3, KI#4, KI#9**

**Document for: Approval**

**Agenda Item: 5.7**

# 1 Decision/action requested

***This contribution proposes conclusions for KI #3, KI#4, KI#9***

# 2 References

[1] TR 33.847 v.0.8.0 “Study on security aspects of enhancement for proximity based services in the 5G System (5GS)”

[2] S3-212290 “Handling of KAUSF upon successful primary authentication”

# 3 Rationale

It was agreed in SA3 #104-ad, that for control plane solutions for PC5 link security:

- AUSF derives the PC5 anchor key (e.g., sol#1, sol#15, sol#30, sol#39) used for PC5 keys derivation.

- Performing primary authentication during PC5 link establishment is supported (e.g. Sol#1, Sol#10, Sol#30).

It is however unclear whether Kausf is generated for the UE authentication performed during PC5 link establishment and used as root key for PC5 anchor key.

There were lengthy discussions about the Kausf handling to make sure network side and UE side handling is consistent in past a few SA3 meetings, e.g., as depicted in S3-212290 [2]. Apparently, if the UE authentication performed during PC5 link establishment results to Kausf generation, it would introduce new additional impacts in network side and UE side for Kausf handling and also dependency to those features based on Kausf, e.g., UPU/SOR, AKMA.

It is desirable a target CP solution for Prose should be loosely coupled with the UE's primary authentication and key hierarchy handling for 3GPP access. Therefore, it is proposed that:

- AUSF derives the PC5 anchor key based on the authentication vectors retrieved from the UDM for Remote UE's authentication performed during PC5 link establishment.

- UE authentication performed during PC5 link establishment is independent to the UE's primary authentication of 3GPP access and there is no need to generate Kausf.

Meanwhile, there is left a Note for CP solution on 5G-GUTI handling to normative phase. 5G-GUTI handling for remote UE is tightly linked with UE's context handling, which is owned by its serving AMF, e.g. mobility management, registration management etc. There is no such agreement nor discussion in SA2, that Remote UE's serving AMF should be impacted on the UE context handling or 5G-GUTI handling for L3 U2N relay. Thus, it is proposed that:

- The serving AMF of Remote UE should not be impacted for 5G-GUTI and UE context handling for the Remote UE. There is no need for the relay AMF to assign/maintain/refresh 5G-GUTI of Remote UE in L3 U2N solution.

Further conclusions for CP solutions for UE-to-Network relay are proposed in this contribution for the related KIs (KI#3, KI#4, KI#9).

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the TR 33.847 [1].

**\*\*\*\*\* START OF CHANGES \*\*\*\*\***

## 7.3 Key Issue #3: Security of UE-to-Network Relay

Editor’s Note: Further conclusions is FFS

The solutions for U2N Relay authorization and security can be classified as user-plane (UP) or controlled-plane (CP) based solutions. The UP based solutions use a UP connection to an AF (PKMF) while CP based solutions use the primary authentication for PC5 keys establishment.

It is concluded that both control plane and user plane solutions are supported for L3 U2N relay.

Editor’s Note: Further choices on the co-existence and use cases will be decided further in consultation with SA2.

The following text is taken as conclusions for UE-to-Network Relay solution:

- For the control plane solution, the following conclusion is made:

- For PC5 link security, PC5 keys are derived using keys derived from the primary authentication (e.g., sol#1, #10, #15, #30). The security of the communication between UE-to-Network relay and remote UE is established based on a shared key which is derived and distributed with the assistance of the network. A root credential is configured in the remote UE and the network. The shared key is individually derived from the root credential by the remote UE and the network. The shared key is distributed by the AMF to the UE-to-Network relay.

- AUSF derives the PC5 anchor key (e.g., sol#1, sol#15, sol#30, sol#39) used for PC5 keys derivation.

NOTE1: The detailed procedure to enable the PC5 link security and the details of the PC5 key hierarchy will be determined accordingly during the normative phase.

- For the user-plane solution, the following is concluded for security in U2N relay:

- the approach of using the user plane for key management of security keys used for PC5 communication, between the Remote UE and the UE-to-network relay, is adopted as the basis for normative work.

- a new 5G PKMF function, for commercial services, internal to PLMN, is supporting the key management of security keys used for PC5 communication (between the Remote UE and the UE-to-network relay), which is accessed in the user plane, is adopted as the basis for normative work.

- the user-plane solutions including Solution #18 and Solution #29 are selected as the basis of normative work.

The following text is taken as the conclusion for the L3 UE-to-Network Relay solution:

- In addition to PC5 link security above, support of end-to-end security requirements when required by Remote UE services using N3IWF as described in solution #19 is taken as a baseline for normative work.

The following text is taken as the conclusion for the L2 UE-to-Network Relay solution:

- It is concluded that the high-level procedure defined in the Solution #14 is taken as the baseline for the normative work. The details of AS security establishment between the Remote UE and the NG-RAN is to be discussed and defined in the normative phase.

- For end-to-end security, the existing NAS/AS security and UP security mechanisms defined in 33.501 [14] are to be reused.

For user-plane solutions, the followings are concluded for both commercial and public safety use cases:

- All security materials for ProSe U2N relay are provided to the UE by PKMF.

- The discovery keys are managed by PKMF.

- PC5 keys are managed by PKMF.

- PCF and/or 5G DDNMF provides the PKMF address to the UE.

NOTE2: if PKMF address is configured by both PCF and DDNMF, which one takes precedence will be determined in normative phase in coordination with SA2.

- For commercial use cases, PKMF can be collocated with 5G DDNMF.

- For commercial use cases, the PC3 connection between UE and DDNMF (or Ua) can be reused to deliver both the discovery security materials and the PC5 keys (i.e., PRUK and PRUK ID).

- Both remote UE and relay UE are only required to communicate with the PKMF of their own HPLMN for commercial use cases.

- For the public safety use case, PKMF may be managed by a public safety operator and located outside of the 3GPP network.

- Authorization information is stored at UDM (and is made available to 5G DDNMF and PKMF) for commercial use cases and at the PKMF for the Public Safety use case.

- When the remote UE has been provided with the PC5 security materials by the PKMF, the PRUK ID (or PC5 key ID) is included in the DCR as a UE ID and other UE IDs and/or UE Info are not sent in clear over the air.

**\*\*\*\*\* NEXT CHANGES \*\*\*\*\***

## 7.4 Key issue #4: Authorization in the UE-to-Network relay scenario

The solutions for U2N Relay authorization and security can be classified as user-plane (UP) or controlled-plane (CP) based solutions. The UP based solutions use a UP connection to a PKMF while CP based solutions use the primary authentication for PC5 keys establishment.

The following text is taken as conclusions for the UE-to-Network Relay solution:

- For the control plane solution:

- Baseline solution for Authorization for Remote UE/Relay is based on primary authentication (CP based approach, e.g., sol#1, #10, #15, #30) and using PCF based service authorization and provisioning as defined in [16] TS 23.304 clause 5.1.4.

- Performing primary authentication during PC5 link is supported (e.g. Sol#1, Sol#10, Sol#30).

NOTE: The detailed procedure to enable authorization for Remote UE/Relay will be determined accordingly during normative phase. Additional support for Remote UE using its 5G-GUTI in DCR will be determined during normative phase. There is no need for the relay AMF to assign/maintain/refresh 5G-GUTI of Remote UE.

- For the user-plane solution, based on the conclusions in KI #3, it is concluded that the user-plane solutions including Solution #18, Solution #21 and Solution #29 are selected as the basis of normative work.

Editor's note: Final conclusion for secondary A&A/NSSAA is FFS.

**\*\*\*\*\* NEXT CHANGES \*\*\*\*\***

## 7.9 Key Issue #9: Key management in 5G Proximity Services for UE-to-Network relay communication

The following text is taken as a conclusion for the UE-to-Network Relay solution (L2, L3 with/without N3IWF):

* For the control-plane solution:
	+ Existing network entities (AMF, AUSF, UDM) are used for key derivation and distribution of keys used for UE-to-network relay communication. The security of the communication between UE-to-Network relay and remote UE is established based on a shared key which is derived and distributed with the assistance of the network. A root credential is configured in the remote UE and the network. The shared key is individually derived from the root credential by the remote UE and the network. The shared key is distributed by the AMF to the UE-to-Network relay. The details to realise the above procedures and the details of the PC5 key hierarchy will be determined during the normative phase.
	+ AUSF derives the PC5 anchor key (e.g., sol#1, sol#15, sol#30, sol#39) used for PC5 keys derivation.
* For the user-plane solution, based on the conclusions in KI #3, it is concluded that the user-plane solutions including Solution #18, Solution #21 and Solution #29 are selected as the basis of normative work.

**\*\*\*\*\* END OF CHANGES \*\*\*\*\***