**3GPP TSG-SA3 Meeting #104e-Ad-hoc draft\_S3-213523-r1**

**e-meeting, 27 - 30 September 2021** *revision of S3-21xxxx*

**Source: Qualcomm Incorporated, Ericsson**

**Title: Conclusion for KI #3**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

***This contribution proposes a conclusion for KI #3***

# 2 References

[1] TR 33.847 v.0.7.0 “Study on security aspects of enhancement for proximity based services in the 5G System (5GS)”

# 3 Rationale

Further conclusions for user-plane solutions for UE-to-Network relay are proposed in this contribution.

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the TR 33.809 [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 L3 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 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 the L3 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 from the network to the UE-to-Network relay. The details to realise the above procedures will be determined during the normative phase.

NOTE: Which Network Function (e.g. AMF or AUSF) is responsible for PC5 key derivation and distribution will be decided during normative phase. The detailed procedure to enable the PC5 link security will be determined accordingly during normative phase.

* For the user-plane solution, the following is concluded for security in L3 U2N relay:
	+ the approach of using 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.
* 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 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.
* For PC5 link and end-to-end security, solution#14 is taken as a baseline for normative work.

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.

NOTE: 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.

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