**3GPP TSG-SA3 Meeting #103-e *S3-21xxxx***

**e-meeting, 17 - 28 May 2021** Revision of S3-211803+S3-211998

**Source: Qualcomm Incorporated, Huawei, Hisilicon, Ericsson, Xiaomi**

**Title: New Key Issue on security policy handling for 5G Prose services**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve this contribution to add a new Key issue in TR 33.847***

# 2 References

[1] TR 33.847

# 3 Rationale

The contribution proposes a new Key issue on supporting security policy handling for 5G Prose services.

# 4 Detailed proposal

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

\*\*\* BEGINNING OF CHANGES \*\*\*

## 5.X Key Issue #X: Supporting security policy handling for PC5 connection of 5G ProSe services

### 5.X.1 Key issue details

User-plane security policy provisioning and enforcement for PDU sessions is a new feature in 5GS. This security policy handling feature is extended to 5G V2X in one-to-one communication (i.e. unicast).

To align with the security policy handling in 5GS, 5G V2X one-to-one communication specifies the handling of security policy provisioned by the PCF in TS 33.536 [8]. Due to the similarity of service features between ProSe services and V2X services, it is deemed necessary for 5GS to be able to provision and enforce security policies of PC5 in 5G ProSe scenarios.

Different from 5G V2X which only allows PC5 direct communication, 5G ProSe also allows PC5 indirect communication with a UE-to-UE relay sitting between the source UE and target UE, splitting the PC5 connection of direct communication into two concatenating PC5 links (between the source UE and the U2U relay, and between the U2U relay and the target UE). This implies separate security policies on each of the concatenating PC5 connections.

This key issue is to study how to support security policy handling in 5G ProSe, including security policy provisioning and security enforcement based on the provisioned security policies.

### 5.X.2 Security threats

Without secure provisioning of PC5 security policies for 5G ProSe services, PC5 connections can be downgraded or cannot be set up.

Without negotiation on security policies over PC5 connection for consistent security enforcement,

* PC5 communication may fail
	+ e.g. one UE activates security protection based on “Require” or “Preferred” policy, the other UE deactivates security protection based on “Preferred” or “Not Needed” policy
* Or PC5 communication may fail to meet the security requirements of various 5G ProSe services
	+ e.g. When source UE policy is “Required”, target UE policy is “Not needed”, relay UE policy is “Preferred”, the PC5 connection between the source UE and relay can be set up with protection (for “Required”) and the PC5 connection between the relay and the target can also be set up but without protection (for “Not needed”). This results in two established PC5 links running the service with inconsistent security protection, meaning the security requirement of the 5G ProSe service is not met.

### 5.X.3 Potential security requirements

5G ProSe system shall support a means to configure PC5 security policies for 5G Prose services at the network.

5G ProSe system shall support a means to securely provision the configured PC5 security policies to the UE for 5G Prose services.

5G ProSe system shall support negotiation on the provisioned PC5 security policies for consistent security enforcement by the UEs to meet security requirements of 5G Prose Services.

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