**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220369-r3***

**e-meeting, 14 - 25 February 2022**

**Source: Ericsson**

**Title: Definitation of functional entity PKMF**

**Document for: Approval**

**Agenda Item: 4.13**

# 1 Decision/action requested

***Definition of functional entity PKMF***

# 2 References

[1] TS 33.503

# 3 Rationale

Adding definition of functional entity PKMF to TS 33.503.

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the TS 33.503 [1].

**\*\*\*\*** 1st CHANGE **\*\*\*\***

# 4 Overview

Editor’s Notes: This clause contains the overview of 5G ProSe security and links to other specifications, reference points and functional entities, etc.

## 4.1 General

The overall architecture for 5G ProSe is given in TS 23.304 [2]. 5G ProSe includes several features that may be deployed independently of each other. For this reason, no overall security architecture is provided and each feature describes its own architecture.

Security for the 5G ProSe common procedures is described in clause 5, while the overall security of the 5G ProSe features is described in clause 6.

## 4.2 Reference points and functional entities

### 4.2.1 Functional entities

#### 4.2.1.1 General

Architectural reference model is specified in clause 4.2.1, 4.2.2, 4.2.3, and 4.2.7 of TS 23.304 [2].

#### 4.2.1.2 5G ProSe Key Management Function (5G PKMF)

In addition to the architectural reference model specified in TS 23.304 [2], the architectural reference model shall support the functional entity 5G PKMF which is the logical function handling network related actions required for the key management and the security material for discovery of a UE-to-network relay by a Remote UE; and for establishing a secure PC5 communication link between a Remote UE and UE-to-network relay.

The Remote UE and the UE-to-network relay knows from which 5G ProSe Key Management Function(s) to get the needed PRUK(s) for establishing a secure PC5 link between the Remote UE and the UE-to-network relay as the address of the 5G PKMF(s) are either pre-provisioned or provided by the 5G DDNMF (or the PCF) in the HPLMN of the Remote UE to the Remote UE, and by the 5G DDNMF (or the PCF) in the HPLMN of the UE-to-network relay to the UE-to-network relay.

The 5G PKMF interacts with the 5G ProSe-enabled UE using procedures over PC8 reference point defined in clause 5.2.5. The protection for the key request/response messages are described in subclause 5.2.5.

The 5G PKMF of the Remote UE shall request the discovery security materials to the 5G PKMFs of the potential UE-to-network relays from which the Remote UE gets the relay services.

The 5G PKMF of the Relay UE shall request the security materials (e.g. PRUK key) for PC5 communication with the remote UE, from the 5G PKMF of the remote UE.

### 4.2.2 Reference points

In addition to the reference points are specified in clause 4.2.5 of TS 23.304 [2], the 5G Prose architectural reference model shall support the following reference points:

**PC8**: The reference point between the UE and the 5G ProSe Key Management Function (5G PKMF). PC8 relies on 5GC user plane for transport (i.e. an "over IP" reference point). It is used to transport security material to UEs for 5G ProSe UE-to-Network Relay Communication.

**\*\*\*\***  END OF CHANGE **\*\*\*\***