**3GPP TSG-SA3 Meeting #107-e *draft\_S3-221036-r1***

**e-meeting, 16 - 20 May 2022** Revision of S3-22xxxx

**Source: Xiaomi, China Telecom**

**Title: Discussion on PC5 Key Hierarchy for ProSe U2N Relay Communication**

**Document for: Endorsement**

**Agenda Item: 4.7**

# 1 Decision/action requested

***This contribution discusses the PC5 Key Hierarchy for protecting ProSe U2N relay communication.***

# 2 References

[1] TS 33.503: “Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)”

[2] TS 33.536: “Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services”

# 3 Rationale

According to TS 33.503 v0.3.0 [1], the solutions for establishing 5G ProSe U2N communication security can be categorized into the procedure over user plane and the procedure over control plane.

As per clause TS 33.503 [1] clause 6.3.3.2.3, the key hierarchy for user plane procedure has 4 layers of keys. The keys from top to bottom are **PRUK 🡪 KNRP 🡪 KNRP-SESS 🡪 (NRPEK and NRPIK)**. By running the GBA procedure, the 5G PKMF shall use Ks(\_ext)\_NAF as the top-level key PRUK. Therefore, the keys for user plane procedure from top to bottom can be seen as **PRUK (Ks(\_ext)\_NAF) 🡪 KNRP 🡪 KNRP-SESS 🡪 (NRPEK and NRPIK)**.

As per clause TS 33.503 [1] clause 6.3.3.3.3, the key hierarchy for control plane procedure has 5 layers of keys. The keys from top to bottom are **KAUSF\_P 🡪 5GPRUK 🡪 KNR\_ProSe 🡪 Krelay-sess 🡪 (Krelay-enc and Krelay-inc)**. Actually, based on the current procedure description in TS 33.503 [1] clause 6.3.3.3.2, the top-level key KAUSF\_\_P is derived from KAUSF, which is generated by running the 5G ProSe Remote UE specific authentication procedure. It means that the current key hierarchy over control plane has 6 layers of keys in total. The keys from top to bottom are **KAUSF 🡪 KAUSF-P 🡪 5GPRUK 🡪 KNR\_ProSe 🡪 Krelay-sess 🡪 (Krelay-enc and Krelay-inc)**.



Based on the above analysis, it is identified that the control plane procedure has two extra layers of keys than the user plane procedure. The extra layers and difference between the key layers for user plane and control plane procedures woud increase the complexity of implementation on both the UE side and core network side. Therefore, the key hierarchy for user plane procedure and that for control plane procedure should be as consistent as possible.

**Observation 1: The key hierarchy for control plane procedure in current TS 33.503 [1] is not aligned with the key hierarchy for user plane procedure. Different key hierarchies for the same purpose will increase the implementation complexity in the UE.**

Moreover, the existing key hierarchy for control plane procedure has serveral unclarities. Firstly, in the current version of TS 33.503 [1], there is no clear definition for how KAUSF\_ P is derived from KAUSF.

*Clause 6.3.3.3.2*

*7f. …… After the exchanges, the AUSF of the 5G ProSe Remote UE derives KAUSF without calculating the KSEAF.*

*The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE shall derive a new KAUSF\_P (different from KAUSF). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.*

**Observation 2: There is no clear description for how KAUSF\_ P is derived from KAUSF in current TS 33.503 [1]. The relationship between KAUSF and KAUSF\_P needs to be sorted out.**

Secondly, the existing solution may not correctly establish the correlation between the RSC and the ccorresponding layer of keys.

According to TS 33.536 [2] and TS 33.503 [1], 5GPRUK (control plane) or PRUK (user plane) is the root credential of security of the PC5 unicast link, which is generated or derived by running the authentication procedure. And the KNR\_ProSe (control plane) or KNRP (user plane) is the root key established between the two entities communicating over NR PC5 unicast link.

***Clause 6.3.3.3.2 (user plane key description)***

*- PRUK: The root credential of security of the PC5 unicast link.*

*- KNRP: This is a 256-bit root key that is shared between the two entities that communicating using NR PC5 unicast link. It may be refreshed by re-running the authentication signalling using the long-term credentials. Nonces are exchanged between the UEs and used with the KNRP to generate a KNRP-sess (the next layer of keys). KNRP may be kept even when the UEs have no active unicast communication session between them. The 32-bit KNRP ID is used to identify KNRP.*

***Clause 6.3.3.3.3 (control plane key description)***

*- 5GPRUK: The root credential derived from KAUSF\_P that is the root of security of the PC5 unicast link.*

*- KNR\_ProSe: This is a 256-bit root key that is established between the two entities that communicating using NR PC5 unicast link. It may be refreshed by re-running the authentication to derive a fresh 5GPRUK. SUPI shall behave the same value as parameter P0 in Annex A.7.0 of TS 33.501 [3].*

Although the definitions of the keys on comparable layers in control plane and user plane are consistent in TS 33.503 [1], the derivation functions of the same level keys are somehow inconsistent. The main difference is the usage of RSC.

As defined in TS 33.503 [1], in the user plane solution, Ks(\_ext)\_NAF is directly used as **PRUK** which is not bound with **RSC**, while the input parameters for deriving **KNRP** include **RSC**, KNRP freshness parameter 1 and KNRP freshness parameter 2, i.e. **KNRP** is bound with **RSC**.

***Clause 6.3.3.2.2 (user plane)***

*4c. …… On receiving the GPI, the 5G PKMF shall use Ks(\_ext)\_NAF as the PRUK.*

*4d. The 5G PKMF of the 5G ProSe Remote UE shall generate KNRP freshness parameter 2 and derive KNRP using the PRUK identified by PRUK ID, RSC, KNRP freshness parameter 1 and KNRP freshness parameter 2. Then, the 5G PKMF of the 5G ProSe Remote UE sends a Key Response message that contains KNRP and KNRP freshness parameter 2 and the PC5 security policies of the relay service to the 5G PKMF of the 5G ProSe UE-to-Network Relay. This message shall include GPI if generated.*

However in the control plane, the deriviation of the **5GPRUK** is bound with **RSC**; while for deriving the KNR\_ProSe, the input parameters are nonce 1 and nonce 2, i.e. **KNR\_ProSe** is not bound with **RSC**. Since 5G PRUK is the root of security of the PC5 unicast link base on the defintion, RSC information should not be bound with 5G PRUK, but should be bound with KNR\_ProSe.

***Annex A.2 5GPRUK derivation function (control plane)***

*When deriving a 5GPRUK from KAUSF, the following parameters shall be used to form the input S to the KDF:*

*- FC = 0xXX;*

*- P0 = SUPI;*

*- L0 = length of SUPI.*

*- P1 = relay service code;*

*- L1 = length of relay service code.*

*The input key KEY is KAUSF.*

*SUPI shall behave the same value as parameter P0 in Annex A.7.0 of TS 33.501 [3].*

***Annex A.4 KNR\_ProSe derivation function (control plane)***

*When deriving the KNR\_ProSe from 5GPRUK key, the following parameters shall be used to form the input S to the KDF:*

*- FC = 0xZZ;*

*- P0 = Nonce\_2;*

*- L0 = length of Nonce\_2;*

*- P1 = Nonce\_1;*

*- L1 = length of Nonce\_1*

*The input key KEY shall be 5GPRUK key.*

*SUPI shall be have the same value as parameter P0 in Annex A.7.0 of TS 33.501 [3].*

**Observation 3: The correlation between the RSC and the root key 5GPRUK in current TS 33.503 [1] is incorrect.**

To address the issues in the above observations for aligning and correcting the key hierarchy over user plane and control plane, two proposals are introduced as follows.

# 4 Detailed proposal

**Proposal:** For control plane solution, the KAUSF derived during ProSe authentication should be named and used as KAUSF\_P, so as to be differentiated from the KAUSF derived during primary authentication. Meanwhile, the RSC should be used for deriving KNR\_ProSe but not be used for deriving 5GPRUK, which should be bound with the specific service type, e.g. ProSe U2N relay service.

Based on the above proposal, it is proposed to approve the corresponding pCRs (S3-220706, S3-220707).