**3GPP TSG-SA3 Meeting #109Adhoc-e *draft\_S3-230185-r1***

**Online, 16 - 20 January 2023**

**Source: Huawei, HiSilicon**

**Title: Address EN for Sol#26**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***Approve the proposal to TR 33.740***

# 2 References

N/A

# 3 Rationale

The contribution proposes to address the following editor’s notes in solution #26 in TR 33.740:

Editor’s Note: How Long-term credential is provisioned is FFS.

The EN is deleted by adding the following description: The Long-term credentials are provisioned as specified in clause 5.3.3.1.2.1 of TS 33.536.

Editor’s Note: It is FFS how to setup a connection if the long-term credentials have expired.

NOTE 2 is added to address the EN.

Editor’s Note: It is FFS how the two UE’s authorise each other for direct communication.

The UEs are authorised by each other based on TS 33.536.

Editor’s Note: It is FFS how to distinguish authorisation for establishing link with Relay UE or Peer UE.

The EN does not applies to the L3 scenario as the End UE always establishes link with the UE-to-UE relay. The initiating End UE in L2 scenario awares of the purpose of the link establishment (i.e. hop link to the Relay or end-to-end link to End UE). For this reason, the End UE can distinguish authorisation with Relay or End UE.

This contribution also includes editorial changes to align the term of ‘5G ProSe End UE’ as specified in TS 23.304.

# 4 Detailed proposal

\*\*\*BEGINNING OF THE 1st CHANGE\*\*\*

## 6.26 Solution #26: UE-to-UE relay PC5 connection security establishment

### 6.26.1 Introduction

This solution addresses Key issue #2 (Security of UE-to-UE Relay) and Key issue #3 (Authorization in the UE-to-UE Relay Scenario). This solution reuses the mechanism of unicast mode 5G ProSe Direct Communication security defined in TS 33.503 [6] to setup the security of UE-to-UE Relay Communication. This solution covers both In-Coverage and Out-of-Coverage under both L2 and L3 UE-to-UE relay scenarios.

### 6.26.2 Solution details

This solution reuses the mechanism of unicast mode 5G ProSe Direct Communication security defined in TS 33.503 [6] to setup the security of UE-to-UE Relay Communication. The security between UEs based on the provisioned/pre-configured Long-term credentials in the UEs (i.e. source End UE, target End UE and UE-to-UE Relay) involved in the UE-to-UE relay communication. The Long-term credentials are used to form the root of the security of the PC5 unicast link by exchanging the key\_est\_info during Direct Authentication and Key Establishment procedures as specified in TS 33.503 [6].

The PC5 connection security establishment procedures between the End UE (source End UE or target End UE) and UE-to-UE Relay, or between the End UEs (only for L2 case) follow the procedures below:

0. ProSe UE-to-UE relay communication security-related parameter pre-configuration and provisioning, the security-related parameter includes the Long-term credential and signalling/user plane security policies. The Long-term credentials are provisioned as specified in clause 5.3.3.1.2.1 of TS 33.536 [9]. The details about the Long-term credentials may be a method described outside of 3GPP.

NOTE 1: Step 0 may happen under network coverage (e.g. provisioned by PCF).

NOTE 2: This solution assumes the UE always has valid Long-term credentials.

1. UE-to-UE discovery procedures to find a peer UE. The peer UE can be source End UEtarget End UE and UE-to-UE Relay.

2. In the case, initiating UE determines it needs to establish a PC5 connection with another UE (i.e. the peer UE), the initiating UE sends the Direct Communication Request (DCR) message and this message is received by the peer UE. Under the condition of initiating UE's signalling integrity security policy is not ‘NOT NEEDED’, the DCR shall include the Key\_Est\_Info. The message may also include a KNRP ID if the initiating UE has an existing KNRP for the peer UE.

3. The initiating UE and the peer UE exchanges Direct Auth and Key Establish messages including Key\_Est\_Info. This is mandatory if the peer UE does not have the KNRP and KNRP ID pair indicated in step 1, and signalling integrity protection is needed.

Editor’s Note: It is FFS how the two UE’s authorise each other for direct communication.

Editor’s Note: It is FFS how to distinguish authorisation for establishing link with Relay UE or Peer UE.

4. In case the signalling integrity protection is needed, peer UE shall calculate KNRP and send a Direct Security Mode Command message to initiating UE, including MSB of KNRP ID.

5. On receiving the Direct Security Mode Command, the initiating shall calculate KNRP and choose the LSB of KNRP ID if signalling integrity protection is needed. Initiating UE shall send a Direct Security Mode Complete message to UE\_2 which shall contain the LSB of KNRP ID.

### 6.26.3 Evaluation

The security of the PC5 link relies on the provisioned/pre-configured security materials. Security keys for each PC5 connection can be generated without the assistance from the network. Therefore, the Source UE and the Target UE can establish the UE-to-UE connection via UE-to-UE Relay regardless of whether they are within or out of network coverage.

Editor’s Note: Further evaluation is FFS.

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