**3GPP TSG-SA3 Meeting #108-e *S3-222189-r1***

**e-meeting, 22 - 26 August 2022**

**Source: OPPO**

**Title: New solution: End-to-end security establishment for UE-to-UE relay**

**Document for: Approval**

**Agenda Item: 5.3**

1 Decision/action requested

***This pCR proposes to solve the Key Issue #2 in TR 33.740[1]***

2 References

[1] 3GPP TR 33.740

[2] 3GPP TS 33.501

3 Rationale

This contribution addresses the security requirements for key issue #2 in TR 33.740[1].

4 Detailed proposal

SA3 is kindly requested to agree to the below pCR to TR 33.740 [1].

**\*\*\*\*** START OF CHANGE **\*\*\*\***

6.X End-to-end security establishment for UE-to-UE relay

6.X.1 Introduction

This solution addresses security requirement for providing confidentiality, integrity protection of end-to-end information exchanged between the peer UEs over the UE-to-UE Relay in key issue #2.

6.X.2 Solution details

6.X.2.1 End-to-end security establishment for UE-to-UE relay



Figure 6.X.2.1: End to end security establishment for UE-to-UE relay

Before Step 0, the source UE and target UE have discovered and attached to the UE-to-UE relay. Source UE and Target UE have also discovered each other.

0. During the UE-to-UE relay authentication, several authentication signallings are exchanged between the peer UEs to derive the shared key KD based on the shared credential between source UE and target UE.

Note: How the source UE and the target UE generate the shared key is not addressed in this solution.

1. The source UE sends a Direct Security Mode Command message to the target UE through the UE-to-UE relay, which contains User Info ID of Source UE, Source UE’s security capabilities, Nonce\_1, MSB of KD ID chosen by source UE to uniquely identify KD at source UE.

2a. Upon reception of the Direct Security Mode Command message from the UE-to-UE Relay, target UE generates the session key KD-sess as specified in clause 6.X.2.3.1, and selects integrity and encryption algorithms from Source UE’s capability, generates integrity and encryption keys as specified in clause 6.X.2.3.2 The target UE chooses the LSB of KD ID to uniquely identify KD at target UE, forms KD ID from the received MSB of KD ID and chosen LSB of KD ID, and stores the complete KD ID with KD.

2b. The target UE activates the integrity protection before sending the Direct Security Mode Response message.

3. The target UE sends the Direct Security Mode Response message to source UE through UE-to-UE relay, including User Info ID of Target UE, Nonce\_2, LSB of KD ID, chosen MSB of KD-sess ID, chosen\_algs, and MAC for integrity protection.

4a. Upon reception of the Direct Security Mode Response message from the UE-to-UE Relay, the source UE generates the session key KD-sess as specified in clause 6.X.2.3.1. According to the chosen\_algs from target UE, source UE generates integrity and encryption keys as specified in clause 6.X.2.3.2. The source UE forms KD ID from the received LSB of KD ID and chosen MSB of KD ID, and stores the complete KD ID with KD. The source UE chooses the LSB of KD-sess ID, forms KD-sess ID from the received MSB of KD-sess ID and chosen LSB of KD-sess ID, and stores KD-sess ID with KD-sess.

4b. The source UE verifies the integrity protection using the indicated integrity algorithm in chosen\_algs and the generated integrity key. After the successful verification, source UE starts integrity and encryption protection before sending the Direct Security Mode Complete message.

5. The source UE sends the Direct Security Mode Complete message to target UE through the UE-to-UE Relay, which contains the LSB of KD-sess ID.

6. Upon reception of the Direct Security Mode Complete message from the UE-to-UE Relay, the target UE deciphers and checks the integrity protection on the Direct Security Mode Complete message using the key and algorithm indicated in the chosen\_algs. The target UE forms the KD-sess ID and stores it with KD-sess.

Editor's Notes: Whether to activate the integrity or confidentiality protection is based on the security policy of source UE and target UE, which is FFS.

Editor's Notes: These Security Mode Command messages’ name shall be consistent with TR 23.700-33, which is FFS.

Editor's Notes: How to protect the privacy information in DSMC request message is FFS.

6.X.2.2 Key Hierarchy for UE-to-UE relay

There are 4 different layers of keying material as shown in figure 6.X.2.2-1.



Figure 6.X.2.2-1: Key Hierarchy for UE-to-UE relay

* Security Credentials: Upon successful configuration procedure, each UE will be configured with the credentials which include a public/private key pair. Authentication signallings are exchanged between source UE and target UE via UE-to-UE relay to derive the KD.
* KD: This is a root key that is shared between source UE and target UE that communicating using UE-to-UE relay link. It may be refreshed by re-running the authentication signallings using the security credentials. Nonces are exchanged between the UEs and used with the KD to generate a KD-sess (the next layer of keys). The KD ID is used to identify KD.
* KD-sess: This key is derived by source UE and target UE from KD and is used derive keys that to protect the transfer of data between the peer UEs. The actual keys (see next bullet) that are used in the confidentiality and integrity algorithms are derived directly from KD-sess. The KD-sess ID identifies the KD-sess ID.
* KD-enc, KD-int: The U2U relay Encryption Key (KD-enc) and Integrity Key (KD-int) are used in the chosen confidentiality and integrity algorithms respectively for protecting control plane data and user plane data between source UE and target UE.

6.X.2.3 Key derivation functions

6.X.2.3.1 KD-sess derivation function

When deriving the session key KD-sess from KD in source UE and target UE the following parameters shall be used to form the input S to the KDF.

- FC = 0xXX

- P0 = Nonce\_1

- L0 = length of Nonce\_1

- P1 = Nonce\_2

- L1 = length of Nonce\_2

The input key KEY shall be the KD.

6.X.2.3.2 Integrity and encryption keys derivation function

When deriving the keys KD-int, KD-enc from KD-sess in source UE and target UE, the following parameters shall be used to form the input S to the KDF.

- FC = 0xXX

- P0 = 0x00 if KD-enc is being derived or 0x01 if KD-int is being derived

- L0 = length of P0 (i.e. 0x00 0x01)

- P1 = algorithm identity

- L1 = length of algorithm identity (i.e. 0x00 0x01)

The algorithm identity shall be set as described in TS 33.501 [2].

The input key KEY shall be the KD-sess.

X.X.3 Evaluation

TBD.

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