**3GPP TSG-SA3 Meeting #108-e*-*ad hoc *draft-S3-222585-r3***

**e-meeting, 10 - 14 October 2022**

**Source: OPPO**

**Title: Address the ENs in Sol #6**

**Document for: Approval**

**Agenda Item: 5.3**

1 Decision/action requested

***This pCR proposes to address the ENs*** ***in Sol #6 of TR 33.740[1]***

2 References

[1] 3GPP TR 33.740

[2] 3GPP TS 33.536

3 Rationale

This contribution addresses the EN “These Security Mode Command messages’ name shall be consistent with TR 23.700-33, which is FFS.” in Sol #6 of TR 33.740[1]. According to the conclusion of KI #2 “Support of UE-to-UE Relay”, it is not mentioned E2E the message between source UE and target UE should be named as “Indirect”. Therefore, it is proposed to maintain the name of security mode command message between source UE and target UE, unless there is a reason to change.

This contribution addresses the EN “Which peer UE starts the SMC procedure is FFS.” in Sol #6. It is proposed that after the PC5 links establishment between source UE and UE-to-UE relay, UE-to-UE relay and target UE, the E2E security information of source UE is carried in the DCR message of E2E PC5 link establishment between source UE and target UE, then the target UE can initial the SMC procedure to perform the E2E security establishment.

This contribution addresses the EN “The need of Nounce-1 and Nounce-2 needs more justification.” in Sol #6. The Nonce\_1 is delivered in the DCR message, and Nonce\_2 is delivered in the DSMC message, there will be no duplication.

This contribution addresses the EN “How to protect the privacy information in DSMC request message is FFS.” As proposed above, the E2E security message of source UE is carried in the DCR message which is in the relay traffic, the privacy information of source UE such as source UE’s security capability and security policy, Nonce\_1 can be protected by these security per-hop links between source UE and UE-to-UE relay, UE-to-UE relay and target UE.

4 Detailed proposal

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

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

6.6 Solution #6: End-to-end security establishment for Layer-2 UE-to-UE relay

6.6.1 Introduction

This solution addresses security requirement for providing confidentiality, integrity protection of end-to-end information exchanged between the peer UEs over the L2 UE-to-UE Relay in key issue #2.

6.6.2 Solution details

6.6.2.1 End-to-end security establishment for Layer-2 UE-to-UE relay



Figure 6.6.2.1: End to end security establishment for Layer-2 UE-to-UE relay

1. Service authorisation and policy provisioning is performed for the Source UE, Target UE and UE-to-UE Relay.

2. Source UE has selected a suitable UE-to-UE Relay and received the Layer-2 ID of the target UE after Model A or Model B discovery. Source UE decides to connect with target UE via the selected UE-to-UE Relay.

3. The Source UE and Target UE may need to setup or modify the PC5 link with UE-to-UE Relay.

4. After PC5 link between source UE and UE-to-UE relay, UE-to-UE relay and target UE sets up, the E2E PC5 link establishment performs. The source UE sends a Direct Communication Request message to initiate the E2E PC5 link establishment procedure with the target UE.

Editor's Notes: In addition to the security end-to-end information, what information is included in the DCR message is determined by SA2.

To establish the End-to-End security between source UE and target UE, the message includes RSC, source UE’s security capability and source UE’s security policy. This message may include shared security credential ID between source UE and target UE to generate KD, or if there exists a shared key KD between source UE and target UE, the message may include KD ID, Nonce\_1 (for session key KD-sess generation), and the most significant 8-bits of the KD-sess ID (for uniquely identifying KD-sess at source UE).

NOTE：The provisioning of security credentials and security credential ID in the Source UE and Target UE is out of 3GPP scope.

The privacy information of source UE such as source UE’s security capability and security policy, Nonce\_1 can be protected by these security per-hop links between source UE and UE-to-UE relay, UE-to-UE relay and target UE.

5. During the Direct Auth and Key Establishment, 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 KD is not addressed in this solution.

6a. In case the target UE decides to active the End-to-End security protection, based on source UE’s security policy, target UE choose Nonce\_2 and generates the session key KD-sess as specified in clause 6.6.2.3.1, selects integrity and encryption algorithms from Source UE’s capability, generates integrity and encryption keys as specified in clause 6.6.2.3.2. The target UE may choose LSB of KD-sess ID, forms KD-sess ID, and stores KD-sess ID with KD-sess. The target UE may choose the MSB of KD ID to uniquely identify KD at target UE if a new KD is generated.

6b. The target UE activates the integrity protection before sending the Direct Security Mode message if the U2U relay integrity key KD-int has been derived.

7. The target UE sends the Direct Security Mode message to source UE through UE-to-UE relay, including Source UE’s security capabilities, Source UE’s security policy to protect from bidding down attack. The message also includes Nonce\_2, LSB of KD-sess ID, chosen\_algs, and MAC for integrity protection, or the message may include MSB of KD ID.

8a. Upon reception of the Direct Security Mode message from the UE-to-UE Relay, the source UE generates the session key KD-sess as specified in clause 6.6.2.3.1. According to the chosen\_algs from target UE, source UE generates integrity and encryption keys as specified in clause 6.6.2.3.2. The source UE forms KD-sess ID from the received LSB of KD-sess ID and chosen MSB of KD-sess ID, and stores KD-sess ID with KD-sess. Or, if a new KD is generated, the source 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.

8b. 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.

9. The source UE sends the Direct Security Mode Complete message to target UE through the UE-to-UE Relay, which may contain the LSB of KD ID if a new KD is generated.

10. 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. The target UE may form the KD ID and store it with KD.

11. The Target UE sends a Direct Communication Accept message to the Source UE. The Direct Communication Accept message includes User Info ID of Source UE, User Info ID of Target UE, QoS Info (PFI and PC5 QoS parameters) and RSC.

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.

Note: How the PC5-S messages in steps 4, 5, 7, 9, 11 are forwarded by the UE-to-UE Relay is to be determined by RAN2, such as based on an Adaptation layer.

6.6.2.2 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.

6.6.2.3 Key derivation functions

6.6.2.3.1 KD-sess derivation function

The KD-sess derivation function is specified in clause A.3 of TS 33.536[2], and the input key is KD.

6.6.2.3.2 Integrity and encryption keys derivation function

The integrity key KD-int and encryption key KD-enc derivation function are specified in clause A.2 of TS 33.536[2], and the input key is KD-sess.

6.6.3 Evaluation

TBD.

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