**3GPP TSG-SA3 Meeting #101e-Bis *draft\_S3-202828-r2***

**e-meeting, 09 - 20 November 2020**

**Title: [DRAFT]** Reply to LS C1-206576 on the re-keying procedure for NR SL

**Response to:** LS C1-206576 on the re-keying procedure for NR SL

**Release:** Release 16

**Work Item:** eV2XARC

**Source:** SA3

**To:** CT1

**Cc:** RAN2

**Contact Person:**

#### Name: Dongjoo Kim

**Tel. Number:**

E-mail Address: dongjoo7.kim@lge.com

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachments:** to be S3-202952 (if agreed)

**1. Overall Description:**

SA3 would like to thank CT1 for sending the LS C1-206576 on the re-keying procedure for NR SL. SA3 has reviewed the conclusions on the security activation/deactivation procedure mentioned in the LS and found that there are some misalignment with SA3. So we would like to share the agreed procedures as follow:

[For connection setup]

1. The receiving UE provides the AS layer before sending Direct Security Mode Command with the new security context and indication(s) to indicate that this new security context shall be used to integrity protect the Direct Security Mode Command message and can be used to receive protected (both confidentiality and integrity as appropriate) signalling traffic.
2. The initiating UE provides the AS layer after receiving Direct Security Mode Command with the new security context and an indication that this new security context shall be used to send signalling traffic starting with the Direct Security Mode Complete message and can be used to receive protected signalling traffic .
3. The receiving UE provides the AS layer with an indication that the signalling message starting with the Direct Communication Accept is protected with the new security context before sending the Direct Communication Accept and an indication that the user plane message is integrity and confidentiality protected (if applicable) with the new security context after sending Direct Communication Accept.
4. The initiating UE provides the AS layer with an indication of activation of the PC5 unicast user plane integrity and confidentiality protection for the PC5 unicast link (if applicable) after receiving Direct Communication Accept message.

[For rekeying]

1. The receiving UE provides the AS layer before sending Direct Security Mode Command with the new security context and indication(s) to indicate that this new security context shall be used to integrity protect the Direct Security Mode Command message and can be used to receive protected (both confidentiality and integrity as appropriate) signalling and user plane traffic.
2. The receiving UE provides the AS layer before sending Direct Link Rekeying Response with an indication that the signalling message starting with the Direct Link Rekeying Response is protected with the new security context.

For the detailed information, please refer to S3-202952 that is attached with the LS.

**2. Actions:**

**To CT1 group.**

**ACTION:** SA3 requests CT1 to take the above answers into consideration for subsequent specification work.

**3. Date of Next TSG-SA WG3 Meetings:**

SA3#101Bis-e 18 - 22 January 2021 e-meeting

SA3#102-e 22 February - 5 March 2021 e-meeting