**3GPP TSG-RAN WG2 Meeting #114 e R2-2106616**

**E-Meeting, 19th - 27th May 2021**

**Source: vivo (Rapporteur)**

**Title:****Summary on SL-SRB1 integrity check failure handling**

**Agenda Item:** **6.2.2**

**Document for:** **Discussion and Decision**

# Introduction

The following offline discussion is triggered to mainly discuss these proposals as follows:

* [AT114-e][702][V2X/SL] SL-SRB1 integrity check failure handling (Vivo)

 **Scope:** Check CT1 specification and decide AS behaviour

 **Intended outcome:** Agreeable 38.331 CR in R2-2106615 and discussion summary in R2-2106616 if needed.

 **Deadline:** Comeback in Wed. CB session (May 26)

The Rapporteur kindly request companies to provide feedback on the questionnaire by **2021-05-26 0100 UTC.**

# Discussion

During on-line discussion, an agreement has been reached as highlighted in green:

R2-2105346 Discussion on SL-SRB1 integrity check failure handling vivo discussion

* AS indicates it to the upper layer and the upper layer will handle it (if a timer to re-initiate the procedure is defined in CT1 specification).

Thus, the following offline discussion is organized into two parts:

* Firstly, we check the CT1 specification to see if a timer to re-initiate the procedure is defined.
* Secondly, we make decision on AS layer behavior needed.

## Check CT1 specification

According to CT1 specification TS 24.587, the related PC5 unicast link re-keying procedure text is abstracted as follows:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*TS 24.587\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 6.1.2.10 PC5 unicast link re-keying procedure

##### 6.1.2.10.2 PC5 unicast link re-keying procedure initiation by the initiating UE

*[unrelated text omitted…]*

After the DIRECT LINK REKEYING REQUEST message is generated, the initiating UE shall pass this message to the lower layers for transmission along with the initiating UE's layer-2 ID for unicast communication and the target UE’s layer-2 ID for unicast communication, and start timer T5008. The UE shall not send a new DIRECT LINK REKEYING REQUEST message to the same target UE while timer T5008 is running.

NOTE 2: In order to ensure successful PC5 unicast link re-keying, T5008 should be set to a value larger than the sum of T5006 and T5007.



Figure 6.1.2.10.2: PC5 unicast link re-keying procedure

##### 6.1.2.10.4 PC5 unicast link re-keying procedure completion by the initiating UE

Upon receipt of the DIRECT LINK REKEYING RESPONSE message, the initiating UE shall stop timer T5008 and check the integrity of the DIRECT LINK REKEYING RESPONSE message using the new NRPIK.

After receiving the DIRECT LINK REKEYING RESPONSE message, the initiating UE shall delete the old security context it has for the target UE.

##### 6.1.2.10.5 Abnormal cases at the initiating UE

The following abnormal cases can be identified:

a) Timer T5008 expires.

 The initiating UE shall retransmit the DIRECT LINK REKEYING REQUEST message and restart timer T5008. After reaching the maximum number of allowed retransmissions, the initiating UE shall abort the PC5 unicast link re-keying procedure, shall provide an indication of deactivation of the PC5 unicast security protection and deletion of security context for the PC5 unicast link to the lower layer, if applicable, along with the initiating UE's layer-2 ID for unicast communication and the target UE's layer-2 ID for unicast communication and may initiate the PC5 unicast link release procedure.

NOTE: The maximum number of allowed retransmissions is UE implementation specific.

*[unrelated text omitted…]*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*TS 24.587\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Based on the highlighted text in yellow, we have the follows observations:

**Observation 1: T5008 is used for the initiating UE to complete the PC5 unicast link re-keying procedure.**

**Observation 2: Upon reception of the DIRECT LINK REKEYING RESPONSE message, the initiating UE shall take two actions**:

* **Stop T5008;**
* **check the integrity of the DIRECT LINK REKEYING RESPONSE message using the new NRPIK.**

**Observation 3: Upon T5008 expires, the initiating UE shall retransmit the DIRECT LINK REKEYING REQUEST message and restart timer T5008. After reaching the maximum number of allowed retransmissions, the initiating UE shall abort the PC5 unicast link re-keying procedure and may initiate the PC5 unicast link release procedure.**

Further, according to SA3 specification TS 24.587, the security establishment during re-keying procedure is abstracted as follows:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*TS 33.536\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

5.3.3.1.4.4 Security establishment during re-keying

By rekeying, the UEs ensure fresh session keys KNRP-sess are used. Optionally the rekeying can also enforce refresh of KNRP. Either UE may rekey the connection at any time. This shall be done before the counter for a PDCP bearer repeats with the current keys. A rekeying operation shall refresh the KNRP-sess and NRPEK and NRPIK, and may refresh KNRP. There is no benefit in running the rekeying procedure if the NULL integrity algorithm is in use, hence it is recommended not to trigger it when using the NULL integrity algorithm. A rekeying operation follows the flows given in figure 5.3.3.1.4.4-1.

NOTE: The rekeying procedure is not required from security point of view if the connection is unprotected.



Figure 5.3.3.1.4.4-1: Security establishment during rekeying

*[unrelated text omitted…]*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*TS 33.536\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

According to above Figure, it is observed that the security handling of Direct Link Security Mode Command ‎and Direct Link Security Mode Complete Message which are carried via SL-SRB1are performed **(step 3a/4b)** before the DIRECT LINK REKEYING RESPONSE message **(step 5b)**.

**Observation 4: The security handling of Direct Link Security Mode Command ‎and Direct Link Security Mode Complete Message (which are carried via SL-SRB1) are performed before the DIRECT LINK REKEYING RESPONSE message.**

**Q1: Do companies agree with Observation 1,2,3,4 as above?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Not-agree** | **Comment** |
| OPPO | Agree | although O1 is a bit misleading, since T5008 is to trigger the re-transmission of direct link rekeying request message. |
| Samsung | Agree | Same view as OPPO on T5008 |
| ZTE | Agree |  |

**Summary:**

## Decide AS behavior

Based on above observations, Rapporteur understanding is that if the integrity check fails on SL-SRB1 for **Direct Link Security Mode Command ‎or Direct Link Security Mode Complete Message (step 3a/4b)**, there may be no transmission of **the DIRECT LINK REKEYING RESPONSE message (step 5b)**. As a consequence, the timer T5008 may expire in the initiating UE\_1. However, it is not fully discussed during RAN2 online. Thus, it would be helpful to check companies view on the Rapporteur understanding.

**Q2: Do companies agree that if integrity check failure happens on SL-SRB1, there may be no transmission of the DIRECT LINK REKEYING RESPONSE message and the timer T5008 may expire as a consequence?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Not-agree** | **Comment** |
| OPPO | Agree |  |
| Samsung | Agree |  |
| ZTE | Agree |  |

**Summary:**

If the ANS to Q2 is **Agree**, then there will be no further issue from RAN2 perspective since the T5008 expiry case has already been specified by CT1. The only thing RAN2 has to do is that AS indicates it to the upper layer upon detecting the SL-SRB1 integrity check failure. And the rest is left to the upper layer handling. Moreover, for the cross-layer interaction, Rapporteur would like to check with companies which AS layer behavior that needs to be specified to provide such indication.

**Q3-1: If the ANS to Q2 is Agree, which AS layer behavior needs to be specified to indicate SL-SRB1 integrity check failure to the upper layer?**

* **Option 1: PDCP layer**
* **Option 2: RRC layer**

|  |  |  |
| --- | --- | --- |
| **Company** | **Option** | **Comment** |
| OPPO | no strong view on whether further specification is needed | on the one hand, we understand that not all inter-layer interaction is specified, so no big need for this case.on the other hand, if R2 tend to do the specification, considering IP check failure report from PDCP layer to upper layer (RRC layer) has been specified in 323, the only left work is in RRC (331), i.e., to report the IP check failure to upper layer (PC5-S), e.g., using a NOTE. |
| Samsung | Option 2 | Same understanding as OPPO on the expected behavior and RRC part is missing in the specification: PDCP layer reports integrity check failure to RRC layer which is specified in PDCP specification, then RRC layer reports it to upper layer (i.e., PCS-S) |
| ZTE | Option2 or UE implementation | We agree OPPO’s view that the indication of integrity check failure reported from POCP layer has been specified, we only need to capture this in RRC layer. But, we are also fine to left it to UE implementation. |

**Summary:**

If the ANS to Q2 is **Not-agree**, then it is not clear what the correct understanding is for the upper layer handling if integrity check failure happens on SL-SRB1. Rapporteur would suggest that we simply consult with SA3/CT1 instead of interpreting their specifications from RAN2 perspective. RAN2 impact can be investigated later based on their LS response.

**Q3-2: if the ANS to Q2 is Not-agree, do companies agree to send LS to consult what the correct understanding is for the upper layer handling if integrity check failure happens on SL-SRB1?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree/Not-agree** | **Comment** |
|  |  |  |
|  |  |  |

**Summary:**

# Conclusion

The summary concludes with the following proposals:

1. Reference
2. 3GPP TS 24.587 V17.1.0 (2021-03), Vehicle-to-Everything (V2X) services in 5G System (5GS); Stage 3.
3. 3GPP TS 33.536 V16.2.0 (2020-12), Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services.