**3GPP TSG-RAN WG2 Meeting #113-eR2-21xxxxx**

**Online, 25th Jan – 5th Feb 2021**

**Agenda item:** 6.4.2

**Source:** vivo (Rapporteur)

**Title:** [Offline-702] [V2X] T400 expiry in timer table and protection of RRC message

**Document for:** Discussion and Agreement

# 1 Introduction

This is to report the result of the following email discussion at RAN2#113-e meeting.

* [AT113-e][702][V2X/SL] T400 expiry in timer table and protection of RRC messages (vivo)

**Scope:** discuss the corrections in R2-2101761, R2-2100788, R2-2100978, R2-2100790, R2-2100976, R2-2101760 and R2-2100977. Normative text may also need to be updated if adds some additional/different UE behaviour at T400 expiry. Merge the changes and prepare the agreeable CR.

**Intended outcome:** agreeable 38.331 CR in R2-2102175 and discussion summary in R2-2102176 (if needed).

**Deadline:** Feb 04 0430 (UTC)

The document consists of phase-1 and phase-2, the deadline of each phase is outlined as follow:

* Phase 1: determine agreeable parts, deadline: Monday Feb. 1, 2021, 11:00 UTC.
* Phase 2: for agreeable parts Work on CRs, deadline: Thursday Feb. 4, 2021, 02:30 UTC

# 2 Contact Information

To make it easier to find the correct contact delegate in each company for potential follow-up questions, the rapporteur encourages the delegates who provide input to provide their contact information in this table:

|  |  |
| --- | --- |
| Company | Contact: Name (E-mail) |
| vivo | Kimba Dit Adamou, Boubacar (kimba@vivo.com) |
| OPPO | Qianxi Lu (qianxi.lu@oppo.com) |
| Apple | Zhibin Wu (zhibin\_wu@Apple.com) |
| Nokia | Buthler, Jakob (Jakob.buthler@nokia.com) |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# 3 Discussion

## 3.1 T400 expiry in timer table (TS 38.331)

According to current specifcation TS 38.331 V16.3.1, in the informative table of section 7.1.1 for the timer T400, it is stated that when the timer expires, the sidelink reconfiguration failure procedure need to be performed, highlighed in yellow as below.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*From TS 38.331\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

### 7.1.1 Timers (Informative)

| Timer | Start | Stop | At expiry |
| --- | --- | --- | --- |
| T400 | Upon transmission of RRCReconfigurationSidelink | Upon reception of RRCReconfigurationFailureSidelink or RRCReconfigurationCompleteSidelink | Perform the sidelink RRC reconfiguration failure procedure as specified in 5.8.9.1.8 |

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*From TS 38.331\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

However, in the procedural text of section 5.8.9.3, the UE behaviour upon T400 expiry is treated as SL RLF and the Sidelink radio link failure related actions need to be performed, highlighted in yellow as below.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*From TS 38.331\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

#### 5.8.9.3 Sidelink radio link failure related actions

The UE shall:

1> upon indication from sidelink RLC entity that the maximum number of retransmissions for a specific destination has been reached; or

1> upon T400 expiry for a specific destination; or

1> upon indication from sidelink MAC entity that the maximum number of consecutive HARQ DTX for a specific destination has been reached; or

1> upon integrity check failure indication from sidelink PDCP entity concerning SL-SRB2 or SL-SRB3 for a specific destination:

2> consider sidelink radio link failure to be detected for this destination;

2> release the DRBs of this destination, in according to sub-clause 5.8.9.1a.1;

2> release the SRBs of this destination, in according to sub-clause 5.8.9.1a.3;

2> discard the NR sidelink communication related configuration of this destination;

2> reset the sidelink specific MAC of this destination;

2> consider the PC5-RRC connection is released for the destination;

2> indicate the release of the PC5-RRC connection to the upper layers for this destination (i.e. PC5 is unavailable);

2> if UE is in RRC\_CONNECTED:

3> perform the sidelink UE information for NR sidelink communication procedure, as specified in 5.8.3.3;

NOTE: It is up to UE implementation on whether and how to indicate to upper layers to maintain the keep-alive procedure [55].

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*From TS 38.331\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

As a consequence, the informative table for T400 expiry is inconsistent with the procedural text. It is noticeable that whether to consider T400 expiry as SL reconfiguration failure or SL RLF was discussed at RAN2#109-e meeting. At that meeting, RAN2 has made the following agreement to treat T400 expiry the same as SL RLF, highlighted in green as below.

**RAN2#109-e Agreements on RRC**:

Upon T400 expiry, TX UE detects PC5-RRC RLF and performs the same operations as RLF.

However, according to company CRs in [1][2][3], the UE behaviour upon T400 expiry may not be exactly the same operations as SL RLF. There are three Alternatives on the table as follows:

* **Alt- 1:** Continue using the configuration used prior to corresponding *RRCReconfigurationSidelink* message and perform the sidelink UE information for NR sidelink communication procedure as specified in 5.8.3.3 if UE is in RRC\_CONNECTED. (Huawei CR in R2-2101761).
* **Alt- 2:** Perform the Sidelink radio link failure related actions as specified in 5.8.9.3. (vivo CR in R2-2100788).
* **Alt- 3:** Continue using the configuration used prior to corresponding *RRCReconfigurationSidelink* message and perform the radio link failure related actions as specified in clause 5.8.9.3. (Ericsson CR in R2-2100978).

Rapporteur would like to invite interested companies to check which is the correct understanding of the UE behaviour upon T400 expiry and see if there is some additional/different UE behavior needed.

**Q1-1: Do companies confirm that upon T400 expiry, at least the UE will perform the same operations as SL RLF?**

* **YES;**
* **NO.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Comments** |
| OPPO | Yes | Thanks rapporteur reminding the agreement @ #109, then better to align with it and keep the procedural text and thus update the text for T400 expiry in the table only. |
| Apple | Yes |  |
| Nokia | Yes with comment | We agree in principle, but also want to note that as the expiry of timer T400 is considered as a sidelink RLF, it will further lead to the release of that PC5 connection the expiry of T400 timer is associated with. In case the UE is in mode 1 and it can not obtain a NW-granted resource on time for transmitting the RRCReconfigurationSidelink message, it may lead to the expiry of T400 timer. In that case, the PC5 connection can be released, which is not due to PC5 radio link problem. Thus, if the UE cannot obtain a SL resource for transmitting the RRCReconfigurationSidelink message on time, e.g. there is a Uu RLF and no exceptional resource pool is configured, we think the UE may consider to hold T400 until the Uu problem is resolved.  Furthermore as there are multiple T400 timers we suggest to modify the wording in the proposed/revised 5.8.9.3 to “destination ID” |
|  |  |  |
|  |  |  |

**Q1-2: If the ANS to Q1-1 is YES, any additional UE behaviour is needed on top of the SL RLF related operations?**

1. **None;**
2. **Continue using the configuration used prior to corresponding *RRCReconfigurationSidelink* message;**
3. **Others, please specify.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Option** | **Comments** |
| OPPO | 1 | As replied to Q1-1. |
| Apple | 2 | For this issue, we agree with the change in Ericsson CR R2-2100978 |
| Nokia | 2) and 3) | For option3: UE in RRC\_CONNECTED can report the Sidelink Reconfiguration Failure to network |
|  |  |  |
|  |  |  |

**Q1-3: If the ANS to Q1-1 is NO, it means that the UE will perform some behaviour that can be different from the SL RLF related operations. Then what is the correct UE behaviour that needs to be specified?**

1. **Continue using the configuration used prior to corresponding *RRCReconfigurationSidelink* message and perform the sidelink UE information for NR sidelink communication procedure as specified in 5.8.3.3 if UE is in RRC\_CONNECTED;**
2. **Others, please specify.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Option** | **Comments** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 3.2 Protection of NR RRC messages

According to current specifcation TS 38.331 V16.3.1, in the Annex B.1 for protection of RRC messages, the security requirement for sending *SidelinkUEInformationNR* and *ULInformationTransferIRAT* messages are missing. This issue was discussed in [AT112-e][705][V2X], but was postponed as a left-over issue to this meeting.

## *SidelinkUEInformationNR*

Based on company CRs in [1][4][5], there is consensus that *SidelinkUEInformationNR* message shall not be sent unprotected after AS security activation. However, regarding whether *SidelinkUEInformationNR* message can be sent unprotected before AS security activation, company views diverge much.

In [1], the basic idea is that the security requirement defined for sending *SidelinkUEInformation* message in LTE V2X is reused in NR, i.e., ***SidelinkUEInformationNR* message can be sent unprotected prior to AS security activation**.

In [4], it is proposed not to follow the same principle in LTE V2X and apply the enhanced security requirement, i.e., ***SidelinkUEInformationNR* message shall never be sent unprotected prior to AS security activation**. The main motivation is that the only chance for sending *SidelinkUEInformationNR* message unprotected is in the initial phase of RRC connection establishment before security activation which may be a rare case. Furthermore, the security requirement in NR Uu for some other RRC messages over SRB1 has already been enhanced, e.g., *RRCReestablishment* message is sent over SRB1 with integrity protection instead of SRB0 in LTE. Another example is that *RRCResume* message during resuming from RRC\_INACTIVE is sent over SRB1 with both integrity and ciphering protection. Frome these perpectives, it is better to apply the enhanced security requirement to *SidelinkUEInformationNR* message which is also sent over SRB1.

In [5], some rules in between are considered, i.e., **the *SidelinkUEInformationNR* message can be sent unprotected prior to AS security activation but with some conditions**.

- Firstly, consider different RRC states transition procedures. The *SidelinkUEInformationNR* message may be sent unprotectd before AS security activation if the UE transites from RRC\_IDLE to RRC\_CONNECTED, but shall not be sent unprotected before AS security activation if the UE transits from RRC\_INACTIVE to RRC\_CONNECTED or if the UE is in RRC\_CONNECTED.

- Secondly, depend on the information that is carried in the *SidelinkUEInformationNR* message. One of the main differences between LTE and NR V2X is that *SidelinkUEInformationNR* message can be used to report the sidelink UE capability information of the associated peer UE for unicast communication. Since the UE capabilities are sensitve information, in order to protect privacy of the UE, the *SidelinkUEInformationNR* message shall not be sent unprotected before AS security activation if the sidelink UE capability information is included in the *SidelinkUEInformationNR* message.

Based on above observations, rapporteur would like to invite interested companies to check whether or not *SidelinkUEInformationNR* message can be sent unprotected prior to AS security activation and see if there is some condition that needs to be specified.

**Q2-1: Do companies agree that** ***SidelinkUEInformationNR* message can be sent unprotected prior to AS security activation?**

* **YES;**
* **NO (i.e., *SidelinkUEInformationNR* message shall never be sent unprotected prior to AS security activation).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Comments** |
| OPPO | Yes |  |
| Apple | No | There is no need to always inherit LTE D2D decisions. We think the protection of SUI message is needed to protect user privacy in V2X applications. |
| Nokia | No | We also support protection of SUI messags, but we would also support i.e. if compromise is to ask SA3 |
|  |  |  |
|  |  |  |

**Q2-2: If the ANS to Q2-1 is YES, any condition that needs to be specified for the case when *SidelinkUEInformationNR* message shall not be sent unprotected prior to AS security activation?**

1. **None (i.e., follow LTE V2X);**
2. **If the UE transits from RRC\_INACTIVE to RRC\_CONNECTED or if the UE is in RRC\_CONNECTED; and if the sidelink UE capability information is included in *SidelinkUEInformationNR* message;**
3. **Others, please specify.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Option** | **Comments** |
| OPPO | 1 | For “**if the sidelink UE capability information is included in *SidelinkUEInformationNR* message**”: even *UECapabilityInformation* itself can be sent unprotected, so not sure why SUI has to be restricted.  For “**if the UE is in RRC\_CONNECTED**”, not sure what is the restriction, does it mean that after the reception of *RRCResume* or *RRCSetup*? But then it is contradictory to the intention as described by rapporteur that “The *SidelinkUEInformationNR* message may be sent unprotectd before AS security activation if the UE transites from RRC\_IDLE to RRC\_CONNECTED” which also include the reception of RRCSetup.  For “**transits from RRC\_INACTIVE to RRC\_CONNECTED**”, we are fine with the intention, but our understanding that is the phase “after AS security activation”, while “P” is for “Messages that can be sent (unprotected) prior to AS security activation”, i.e., by not marking it as “A-I” or “A-C”, we already prevent the UE to send SUI during “**transits from RRC\_INACTIVE to RRC\_CONNECTED**”. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## *ULInformationTransferIRAT*

Based on company CRs in [1][4][5], there is also consensus that *ULInformationTransferIRAT* message shall not be sent unprotected after AS security activation. However, regarding whether *ULInformationTransferIRAT* message can be sent unprotected before AS security activation, there are mainly two kinds of views.

In [1] [5], although the two CRs are provided with different wording, rapporteur understands that they share a common view to **consider the same security requirement according to the specific E-UTRA RRC messages carried in *ULInformationTransferIRAT* message.** To be more specific, *ULInformationTransferIRAT* message is used for the cross-RAT control scenario (NR Uu control LTE SL) and this message carries V2X sidelink communication related RRC messages (*MeasurementReport*, *UEAssistanceInformation* and *SidelinkUEInformation*). Therefore, *ULInformationTransferIRAT* follows the same security requirement defined in TS 36.331 as E-UTRA RRC *MeasurementReport* message when it is used to transfer the *MeasurementReport*, the same security requirement as E-UTRA RRC *UEAssistanceInformation* messagewhen transfer the *UEAssistanceInformation* andthe same security requirement as E-UTRA RRC *SidelinkUEInformation* message when transfer the *SidelinkUEInformation*.

In [4], considering *ULInformationTransferIRAT* is sent on NR SRB1 it is proposed to simply follow the enhanced security requirement as defined for *SidelinkUEInformationNR*, i.e., make it not being able to be sent unprotected prior to AS security activation in any cases.

Based on above observations, rapporteur would like to invite interested companies to check whether or not *ULInformationTransferIRAT* message can be sent unprotected prior to AS security activation and see if there is some condition that needs to be specified.

**Q3-1: Do companies agree that the NR *ULInformationTransferIRAT* message can be sent unprotected prior to AS security activation?**

* **YES;**
* **NO (i.e., the NR *ULInformationTransferIRAT* message shall never be sent unprotected prior to AS security activation).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Comments** |
| OPPO | Yes |  |
| Apple | No | For the same reason as in Q2-1, we support the enhanced protection for this message. |
| Nokia | No | Same as in Q2-1 |
|  |  |  |
|  |  |  |

**Q3-2: If the ANS to Q2-1 is YES, any condition that needs to be specified for the case when the NR *ULInformationTransferIRAT* message shall not be sent unprotected prior to AS security activation?**

1. **Apply the same security requirement defined in TS 36.331 according to the specific E-UTRA RRC messages (*MeasurementReport*, *UEAssistanceInformation* and *SidelinkUEInformation*) carried in the NR *ULInformationTransferIRAT* message;**
2. **Others, please specify.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Option** | **Comments** |
| OPPO | 1 |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 3.3 Protection of E-UTRA RRC messages

According to current specifcation TS 36.331 V16.3.0, in the Annex A.6 for protection of RRC messages, the security requirement for sending *ULInformationTransferIRAT* message is missing and needs to be defined. The security requiremnt for sending *SidelinkUEInformation* may also need some clarificaiton case by case.This issue was discussed in [AT112-e][705][V2X], but was postponed as a left-over issue to this meeting.

## *SidelinkUEInformation*

In [6], the CR proposes to make some clarification on the case when the ***SidelinkUEInformation* message shall not be sent unprotected prior to AS security activation**. Rapporteur understands that the CR is trying to address different RRC states transition procedures, and further clarify that even though *SidelinkUEInformationNR* message can be sent unprotected before AS security activation, but shall not be sent unprotected before AS security activation if the UE transits from RRC\_INACTIVE to RRC\_CONNECTED or if the UE is in RRC\_CONNECTED. Rapporteur would like to invite interested companies to share your view on the need of such clarification.

**Q4: Any condition that needs to be specified for the case when *SidelinkUEInformationNR* message shall not be sent unprotected prior to AS security activation?**

1. **None (i.e., without change to current specification)**
2. **If the UE transits from RRC\_INACTIVE to RRC\_CONNECTED or if the UE is in RRC\_CONNECTED**
3. **UE shall not send this message unprotected. UE only send this message after AS security activation**
4. **Others, please specify.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Option** | **Comments** |
| OPPO | 1 |  |
| Apple | 3 |  |
| Nokia | 3 |  |
|  |  |  |
|  |  |  |

## *ULInformationTransferIRAT*

Similar to NR *ULInformationTransferIRAT* message, the E-UTRA *ULInformationTransferIRAT* message is used for the cross-RAT control scenario (LTE Uu control NR SL) and this message carries NR sidelink communication related RRC messages (*MeasurementReport*, *UEAssistanceInformation* and *SidelinkUEInformationNR*). Therefore, it is proposed to consider the same security requirement according to the specific NR RRC messages carried in the E-UTRA *ULInformationTransferIRAT* message in [6][7]. This security pripincle is similar as proposed in TS 38.331. Thus, similar quesitons are designed for theE-UTRA *ULInformationTransferIRAT* message.

**Q5-1: Do companies agree that the E-UTRA *ULInformationTransferIRAT* message can be sent unprotected prior to AS security activation?**

* **YES;**
* **NO (i.e., the E-UTRA *ULInformationTransferIRAT* message shall never be sent unprotected prior to AS security activation).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Comments** |
| OPPO | 1 |  |
| Apple | NO |  |
| Nokia | No |  |
|  |  |  |
|  |  |  |

**Q5-2: If the ANS to Q2-1 is YES, any condition that needs to be specified for the case when the E-URTA *ULInformationTransferIRAT* message shall not be sent unprotected prior to AS security activation?**

1. **Apply the same security requirement defined in TS 38.331 according to the specific NR RRC messages (*MeasurementReport*, *UEAssistanceInformation* and *SidelinkUEInformationNR*) carried in the E-UTRA *ULInformationTransferIRAT* message;**
2. **Others, please specify.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Option** | **Comments** |
| OPPO | 1 |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 4 Conclusion

**TBD**

# 5 References

1. R2-2101761 Miscellaneous corrections on TS 38.331 (Rapportuer CR) Huawei, Hisilicon CR Rel-16 38.331 16.3.1 2437 - F 5G\_V2X\_NRSL-Core
2. R2-2100788 Correction on T400 expiry behavior vivo CR Rel-16 38.331 16.3.1 2357 - F 5G\_V2X\_NRSL-Core
3. R2-2100978 Corrections regarding sidelink impacting NR Ericsson CR Rel-16 38.331 16.3.1 2373 - F 5G\_V2X\_NRSL-Core
4. R2-2100790 Message protection for NR Sidelink vivo discussion
5. R2-2100976 Protection of sidelinkUEInformation and ULInformationTrasferIRAT Ericsson CR Rel-16 38.331 16.3.1 2372 - F 5G\_V2X\_NRSL-Core
6. R2-2100977 Protection of sidelinkUEInformation and ULInformationTrasferIRAT Ericsson CR Rel-16 36.331 16.3.0 4558 - F 5G\_V2X\_NRSL-Core
7. R2-2101760 Miscellaneous corrections on TS 36.331 (Rapportuer CR) Huawei, Hisilicon CR Rel-16 36.331 16.3.0 4591 - F 5G\_V2X\_NRSL-Core