**3GPP** **TSG SA WG3 Meeting 104-e S3-212428r2**

**Electronic meeting, 16-27 August 2021**

**Title: Reply LS on Small data transmission**

**Response to: LS S3-211426 (R2-2104401) on** **Small data transmissions**

**Release: Rel-17**

**Work Item: NR\_SmallData\_INACTIVE-Core**

**Source: SA3**

**To:** **RAN2**

**Cc: SA2**

**Contact person: Alec Brusilovsky**

**Alec.Brusilovsky@interdigital.com**

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

**Attachments:** none

# 1 Overall description

SA3 would like to thank RAN2 for their LS on Small data transmission.

SA3 discussed the incoming LS from RAN2 and would like to provide the following answers to RAN2 questions.

**Q1:** Can a CCCH message reusing the I-RNTI and resumeMAC-I be transmitted again in the same cell after SDT initiation, e.g., similar to legacy RRC Reject case (but without having received RRC Reject at the UE)?

**SA3 answer:**

**(TBD)**

**Q2:** Can NCC and I-RNTI from a former cell in which an SDT procedure was initiated be reused to initiate a new SDT procedure in a new cell?

**SA3 answer:**

**(TBD)**

**The following section contains the analysis of the proposed Reply LSs from Apple, CATT, HW, Intel, and ZTE and is to be removed upon agreement on the text for the SA3 answers.**

**Q1:** Can a CCCH message reusing the I-RNTI and resumeMAC-I be transmitted again in the same cell after SDT initiation, e.g., similar to legacy RRC Reject case (but without having received RRC Reject at the UE)?

**APPLE (S3-212794): “***Strictly speaking, there could be a scenario when an attacker may cause termination of legitimate SDT session by capturing a first SDT RRCResumeRequest and replaying it as a second non-SDT RRCResumeRequest. But the situation is same as the legacy RRC Reject case. If RAN2 does not worry about the legacy RRC Reject case, it is OK to reuse the NCC in the same cell after SDT initiation. If not, then the I-RNTI and resumeMAC-I should not be reused and legacy RRC Reject case should be enhanced*.”

**CATT: (S3-212724)** (no separate answers for Q1 and Q2): “*SA3 would like to acknowledge the security issues related to reusing the same I-RNTI and NCC with the same cell scenario or mobility scenarios as cell reselection.*

*However, for both cases (same cell and different cell), SA3 would like to provide the following feedback.*

*SA3 would like to point out that to avoid replay attacks, keystreams should not be reused. The inputs of keystreams include the following input parameters: KEY, COUNT (e.g., PDCP count), MESSAGE, DIRECTION, and BEARER. Any change in an input parameter will result in a different keystream.*

*SA3 asks RAN2 to verify that the above requirements are met.”*

**HW (S3-212698)** (no separate answers for Q1 and Q2): **“***SA3 would like to acknowledge the security issues related to reusing the same I-RNTI and NCC with the same cell scenario or mobility scenarios as cell reselection.*

*However, for both cases (same cell and different cell), SA3 would like to provide the following feedback.*

*SA3 would like to point out that to avoid replay attacks, keystreams should not be reused. The inputs of keystreams include the following input parameters: KEY, COUNT (e.g., PDCP count), MESSAGE, DIRECTION, and BEARER. Any change in an input parameter will result in a different keystream.*

*SA3 asks RAN2 to verify that the above requirements are met.*

*SA3 could not agree on whether these issues represent “corner” or “normal” cases. For that, SA3 need to receive a feedback from RAN2 on how often the scenario(s) under which second RRC Resume Request is triggered can happen.”*

**INTEL (S3-212685): “***No, to avoid potential Replay Attack, UE should not send Resume Request message with the same I-RNTI and resumeMAC-I in the same cell after SDT initiation.*” Also, **INTEL** states the following for both, Q1 and Q2: “*For both cases (same cell and different cell), SA3 thinks there could be a scenario when an attacker may cause the termination of a legitimate SDT session by capturing a first SDT RRCResumeRequest and replaying it a second non-SDT RRCResumeRequest. SA3 requests RAN2 to assess the impact of the risk as mentioned above, answer the following question*.

*Q1: SA3 asks RAN2 whether network accepting second non-SDT RRCResumeRequest is or not a corner case for SA3 to evaluate whether the security risk is acceptable or not; and investigate if any solution could be commensurate with the risk*.”

**ZTE (S3-212525)** (no separate answers for Q1 and Q2): “*SA3 would like to acknowledge the security issues related to reusing the same I-RNTI and NCC with the same cell scenario or mobility scenarios as cell reselection.*

*For both cases (same cell and different cell), SA3 would like to provide the following feedback.*

*SA3 would like to point out that to avoid replay attacks, keystreams should not be reused. The inputs of keystreams include the following input parameters: KEY, COUNT (e.g., PDCP count), MESSAGE, DIRECTION, and BEARER. Any change in an input parameter will result in a different keystream.*

*SA3 asks RAN2 to verify that the above requirements are met.”*

**Q2:** Can NCC and I-RNTI from a former cell in which an SDT procedure was initiated be reused to initiate a new SDT procedure in a new cell?

**SA3 answer:**

**APPLE (S3-212794):** “*If the new cell is in the same gNB (intra-gNB case), the NCC and I-RNTI can be reused, as KgNB can be retained in the intra-gNB-CU according to the SA3 spec.*

*If the new cell is in a different gNB (inter-gNB case), SA3 has the requirements on not reusing the keystreaming in inter-gNB case, therefore it is not recommended to reuse the NCC and I-RNTI. In this case, the horizontal key derivation is recommended. Horizontal key derivation can also be applied in the intra-gNB case.*”

**CATT** **(S3-212724)** (no separate answers for Q1 and Q2): “*SA3 would like to acknowledge the security issues related to reusing the same I-RNTI and NCC with the same cell scenario or mobility scenarios as cell reselection.*

*However, for both cases (same cell and different cell), SA3 would like to provide the following feedback.*

*SA3 would like to point out that to avoid replay attacks, keystreams should not be reused. The inputs of keystreams include the following input parameters: KEY, COUNT (e.g., PDCP count), MESSAGE, DIRECTION, and BEARER. Any change in an input parameter will result in a different keystream.*

*SA3 asks RAN2 to verify that the above requirements are met*.”

**HW (S3-212698)** (no separate answers for Q1 and Q2): **“***SA3 would like to acknowledge the security issues related to reusing the same I-RNTI and NCC with the same cell scenario or mobility scenarios as cell reselection.*

*However, for both cases (same cell and different cell), SA3 would like to provide the following feedback.*

*SA3 would like to point out that to avoid replay attacks, keystreams should not be reused. The inputs of keystreams include the following input parameters: KEY, COUNT (e.g., PDCP count), MESSAGE, DIRECTION, and BEARER. Any change in an input parameter will result in a different keystream.*

*SA3 asks RAN2 to verify that the above requirements are met.*

*SA3 could not agree on whether these issues represent “corner” or “normal” cases. For that, SA3 need to receive a feedback from RAN2 on how often the scenario(s) under which second RRC Resume Request is triggered can happen.”*

**INTEL (S3-212685): “***No, reusing the same NCC and I-RNTI from a former cell to resume SDT procedure in the new cell violates the forward security principle, and such reuse should be avoided.”* Also, **INTEL** states the following for both, Q1 and Q2: “*For both cases (same cell and different cell), SA3 thinks there could be a scenario when an attacker may cause the termination of a legitimate SDT session by capturing a first SDT RRCResumeRequest and replaying it a second non-SDT RRCResumeRequest. SA3 requests RAN2 to assess the impact of the risk as mentioned above, answer the following question*.

*Q1: SA3 asks RAN2 whether network accepting second non-SDT RRCResumeRequest is or not a corner case for SA3 to evaluate whether the security risk is acceptable or not; and investigate if any solution could be commensurate with the risk.”*

**ZTE (S3-212525)** (no separate answers for Q1 and Q2)**:** “*SA3 would like to acknowledge the security issues related to reusing the same I-RNTI and NCC with the same cell scenario or mobility scenarios as cell reselection.*

*For both cases (same cell and different cell), SA3 would like to provide the following feedback.*

*SA3 would like to point out that to avoid replay attacks, keystreams should not be reused. The inputs of keystreams include the following input parameters: KEY, COUNT (e.g., PDCP count), MESSAGE, DIRECTION, and BEARER. Any change in an input parameter will result in a different keystream.*

*SA3 asks RAN2 to verify that the above requirements are met.”*

**Editor (AB) observations:**

* CATT and ZTE are completely aligned.
* HW is mostly aligned with CATT and ZTE and would like to ask RAN2 an additional “corner case” question. This question was already discussed at Monday’s SA3 call and has limited support.
* INTEL is answering NO to both RAN2 questions and would like to ask another question in the proposed Reply LS.
* APPLE is most permissive in their answer to Q1, stating that, “…*the situation is same as the legacy RRC Reject case. If RAN2 does not worry about the legacy RRC Reject case, it is OK to reuse the NCC in the same cell after SDT initiation.” For Q2, APPLE states, “If the new cell is in the same gNB (intra-gNB case), the NCC and I-RNTI can be reused, as KgNB can be retained in the intra-gNB-CU according to the SA3 spec.” APPLE, however, state that “If the new cell is in a different gNB (inter-gNB case), SA3 has the requirements on not reusing the keystreaming in inter-gNB case, therefore it is not recommended to reuse the NCC and I-RNTI. In this case, the horizontal key derivation is recommended. Horizontal key derivation can also be applied in the intra-gNB case.*”

**WAY to move forward:** base Reply LS on CATT, ZTE, and HW (without the “corner case” question) proposals as representing rough consensus. Add that RAN2 has to compare added security complexity with added security benefits when making a decision.

# 2 Actions

**To RAN2, SA2**

**ACTION:** 3GPP TSG SA WG3 would like RAN2 and SA2 to take the above feedback into account and answer the above question.

# 3 Dates of next TSG SA3 WG3 meetings

TSG SA WG3 meeting schedule is available at the following 3GPP link:

<https://portal.3gpp.org/Home.aspx?tbid=386&SubTB=386#/>