3GPP TSG-RAN WG2 Meeting #109e [R2-200xxx](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_109_e/Docs/R2-2002087.zip)x

Elbonia, Online, 24 February – 6 March 2020

**Agenda item: 5.4.1.1**

**Source: NTTDOCOMO, INC. (offline email discussion rapporteur)**

**Title: Report of [AT109e]** **[070][NR15] Unsecured UE capability handling (NTT Docomo)**

**Document for: Report**

# 1 Scope of the offline email discussion

This document contains the summary of the offline email discussion “**[AT109e] [070][NR15] Unsecured UE capability handling (NTT Docomo)**”, as indicated below:

* [AT109e][070][NR15] Unsecured UE capability handling (NTT Docomo)

 Scope: Based on [R2-2002049](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109_e/Docs/R2-2002049.zip) determine the interest, and if possible arrive at an agreed CR

 Intended outcome: Short report or agreed CR

 Deadline: Mar 3 1200 CET

# 2 Offline email discussion

## 2.1 Summary of paper [R2-2002049](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109_e/Docs/R2-2002049.zip) [1]

Following gives SA3 reply LS regarding unsecured UE capability handling [2]

Question 1: Is AS security required for UE capability enquiry for NB-IoT CP solution?

Answer: SA3 specified security protection of the RRC UE capability transfer procedure in agreed CR S3-192862. In this CR, the fundamental requirement of the protection of UE capability is that UE supports AS security. However, NB-IoT CP solution devices do not support AS security for UE capability transfer. SA3 is currently studying how to mitigate the effect of unprotected UE capability for such UEs.

***Observation 1: For unsecured UE capability, SA3 is still discussing on handling for NB-IoT CP solution.***

Question 2: Is it allowed to send UE capability retrieved without security to other RAN nodes for unauthenticated emergency calls?

Answer: Yes, SA3 has agreed attached CR S3-192862 which states that

“With the exception of unauthenticated emergency calls, if the network had acquired UE capabilities using RRC UE capability transfer procedure before AS security activation, then the network shall not store them locally for later use and shall not send them to other network entities. In that case, the network shall re-run the RRC UE capability transfer procedure after a successful AS SMC procedure.”

***Observation 2: For unsecured UE capability, SA3 agreed not to either store them locally for later use or send them to other network entities except for unauthenticated emergency calls.***

Following table summarizes what the LS mentioned

Table 1: Handling of UE capability



Based on above, following four points needs to be considered.

***1-1: Storing is allowed***

***1-2: Storing is prohibited***

***2-1: Sending is allowed***

***2-2: Sending is prohibited***

The following proposals were obtained.

***Proposal 1: For 1-2 (Storing is prohibited), RAN2 to agree gNB shall release the UE capability, when UE transits from RRC\_CONNECTED to either RRC\_IDLE or RRC\_INACTIVE.***

***Proposal 2: For 2-1 (Sending is allowed), on handover, RAN2 to discuss whether the UE capability is secured or unsecured can be identified in RRC inter-node message.***

***Proposal 3: For 2-2 (Sending is prohibited), on handover, RAN2 to discuss which solution to adopt i.e. (1) just not to transfer and (2) to transfer with invalid indication (e.g. unsecured).***

## 2.2 Questions

### 1: Storing unsecured UE capability due to unauthenticated emergency call

SA3 replied RAN2 it is allowable to store unsecured UE capability due to unauthenticated emergency call. However, the next call may not be “Unauthenticated emergency call”, so we think it is better to discard it without storing it for later use.

**Q1**: Do companies agree gNB/eNB **should not** store the unsecured UE capability (acquired before AS SMC procedure due to unauthenticated emergency call) locally for later use?

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Detailed comments** |
| Ericsson | **-** | This is not to be discussed in RAN2. So far, SA3 have said that emergency calls are exempt from the requirement on AS security for UE capabilities.  |
| Huawei, HiSilicon | **-** | Not specific to this Q1 but to the whole discussions:Firstly, in the past, RAN2 agreed on a LS R2-1911850, and one sentence is as below:RRC specification do not normally capture normative network behaviour in detail. Hence, RAN2 would prefer to capture all the exceptions and mandatory network requirements in SA3 stage 2 specifications.It seems clear that RAN2 will not define anything on the exceptions.Secondly, Q2 in the LS was triggered and sent by RAN2 and it is about unauthenticated emergency calls. We understand that RAN2 may or may not discuss potential RAN2 impacts based on the answers for Q2.Question 2: Is it allowed to send UE capability retrieved without security to other RAN nodes for unauthenticated emergency calls?Based on above considerations, we are not sure whether there were conflicting discussions in RAN2. In addition, after reviewing DoCoMo’s CRs, we think there may be considerable impacts from RAN2 point of view (FFS on other WGs). So we prefer to postpone the whole discussions so that companies may have more time for double check. |
| China Telecom | **Not sure** | Since the unsercured UE capability can be used for emergency call so the network may store it for a period before it can get sercured UE capability. |
| Intel | **-** | For unauthenticated emergency calls, there is no possibility to get secure capability. It is not clear what exactly “later use” means here.  |
| Nokia, Nokia Shanghai Bell | **-** | SA3 already agreed that “not store” is captured in their specifications. We agree with Ericsson and Huawei views that there’s no need for RAN2 to do anything right now, and we agree with Intel that it’s not at all clear how the emergency call would get authenticated later. |
| ZTE | **-** | We agree with the comments from Intel, Ericsson, Nokia and HW above. As noted by Intel above, there is no way to obtain secure capability for unauthenticated emergency calls. In addition, it is unclear whether any capability acquired after SMC is to be considered secure in this case! Note that nia0 is used for unauthenticated emergency calls even if the capability is obtained after SMC. So, just having a condition on SMC seems insufficient. Anyway, further discussion on this aspect should also happen in SA3.  |
| CATT | **-** | A RAN node should have to store the UE capability temporarily which may be delivered to the target RAN node during a unauthenticated call, while have to delete it sooner or later. |
| NEC | **-** | As commented above already, the Q1 itself is what SA3 agreed and no need for RAN2 to discuss further.However, as Intel commented, it would be good to clarify what “later use” mean?  |
| Apple | **-** | We also agree with Intel that for unauthenticated emergency calls, there is no way to obtain the secure capability later.  |
| docomo | **-** | RAN node would store the UE capability during a unthenticated emergency call. The intention is to clarify RAN node should discard it immediately after emergency call finished.  |

Conclusion 1: 10 companies responded this question. Majority companies think unsecured UE capability due to unauthenticated emergency call is already exempted by SA3, no need for RAN2 to do further clarification.

### 2: Storing unsecured UE capability (No unauthenticated emergency call)

SA3 has explicitly replied RAN2 except authenticated emergency call, the network shall not store unsecured UE capability. However, SA3 did not mention clear when to release the UE capability. So, it would be better to clarify that when UE transits from RRC\_CONNECTED to either RRC\_IDLE or RRC\_INACTIVE, the unsecured UE capability should be released.

**Q2.1**: Do companies agree it is necessary to clarify that when UE transits from RRC\_CONNECTED to either RRC\_IDLE or RRC\_INACTIVE, the unsecured UE capability should be released?

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Detailed comments** |
| Ericsson | **No** | We believe what has been captured in the agreed CR [R2-2002094](file:///D%3A%5CDocuments%5C3GPP%5Ctsg_ran%5CWG2%5CTSGR2_109_e%5CDocs%5CR2-2002094.zip) is sufficient. |
| China Telecom | **Maybe not** | We think the description right now is enough. |
| Intel | **May be not** | The current RAN2 text along with what is captured in SA3 specs already seems sufficient.  |
| Nokia, Nokia Shanghai Bell | **No** | Agree with Ericsson. |
| ZTE | **No** | We also think that the current RAN2 text along with what is captured in SA3 is sufficient. Our preference here is to rely on SA3 text as much as possible (via a reference as we currently do) without further additions or changes in RAN2.  |
| CATT | **Maybe not** | We think current description is enough. |
| NEC | **No** | Same view as Ericsson |
| Apple | **No** | The change in CR R2-2002094 is sufficient. |
| Docomo |  | Since agreed CR R2-2002094 already captured eNB should acquire UE capability after SMC, we are fine not to clarify it. |

Conclusion 2: 9 companies responded this question. Majority companies think the agreed CR R2-2002094 is sufficient, no need to further clarify RAN node should release unsecured capability when UE transits from RRC\_CONNECTED to either RRC\_IDLE or RRC\_INACTIVE.

**Q2.2**: if the answer for **Q2.1** is yes, Do companies agree to clarify it in stage2 spec i.e. 36.300, 38.300 as following (highlighted yellow part), also exemplified in [R2-2001604](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109_e/Docs/R2-2001604.zip), [R2-2001608](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109_e/Docs/R2-2001608.zip)?

With the exception of unauthenticated emergency calls, if the eNB had acquired UE capabilities using RRC UE capability transfer procedure before AS security activation, the eNB shall

- release them when UE transits from RRC\_CONNECTED to either RRC\_IDLE or RRC\_INACTIVE.

- not send them to other RAN nodes or MME on handover or retrieve UE context.

- not initiate UE CAPABILITY INFO INDICATION procedure

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Detailed comments** |
|  |  |  |
|  |  |  |

### 3: Sending unsecured UE capability due to unauthenticated emergency call

SA3 replied RAN2 it is allowable to for network to send unsecured UE capability due to unauthenticated emergency call to other network entities. However, the next call may not be “Unauthenticated emergency call” and the receiver may misunderstand it as secured UE capability. So we think it would be necessary to indicate whether the UE capability (acquired before AS SMC procedure due to unauthenticated emergency call) is secured or unsecured when sending to other network entities (eNB/gNB or MME/AMF)?

**Q3.1**: Do companies agree gNB/eNBshould send the unsecured UE capability (acquired before SMC procedure due to unauthenticated emergency call) to other network entities (eNB/gNB or MME/AMF) by indicating the UE capability is unsecured?

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Detailed comments** |
| Ericsson | **No** | No such optimization is needed in our view. |
| China Telecom | **Yes** | We think it will be helpful for the network entities to decide how to deal with the transferred UE capability if it is clearly marked with secured or unsecured.  |
| Intel | **?** | We don’t understand the scenario on how the next call can be “authenticated” for the same UE context.  |
| Nokia, Nokia Shanghai Bell | **No** | This is not needed. |
| ZTE | **?** | Is this is to support HO of unauthenticated calls? If so, couldn’t the target discard the capabilities after the unauthenticated emergency call?  |
| CATT | **No** | Not needed. In our understanding, once the AS security is activated, the RAN node should discard the “unsecured” UE capability (whether NB-IoT is an exception depends on the discussion in SA3). Thus during a handover procedure, the target RAN node can naturally deduce whether the UE capability included is “secured” or not, by checking whether the AS security is activated or not yet. No need for any duplicated indicator. |
| NEC | **?** | this point actually confusing.. On one hand, it is said that the RAN node should not store the unsecured UE capability. If it is obtained for unauthenticated emergency call, then the RAN node should discared when the call is finished. On the other hand, it is said that the RAN node can send the unsecured UE capability to other RAN node. The scenario in question is handover during unauthenticated emergency call? In this case, the target can discard the unsecured UE capability when the call is finished as commented by ZTE. So, the issue is whether the target RAN can know it is unauthenticated emergency call or not?  |
| Apple | **No** |  |
| Docomo | **Yes** | Regarding sending unsecurd UE capability (emergency call) to other nodes, the following could be considered.1. handover for unauthenticated emergency call
2. UE context retrieve for unauthenticated emergency call

For handover or UE context retieve, the target node/new node could implicitly deduce the UE capability is secured or not via UE security capability(i.e. NIA0 or EIA0 is used), while it is preferable there is explicit indication. |

Conclusion 3: 9 companies responded this question. Majority companies think there is no need for this optimization. Some companies think during handover, target node could deduce it is unsecured UE capability from security algorithm (i,e, NIA0 or EIA0), the target node would discard the UE capability after the emergency call finished. Two Operators think explicit indicators (secure or unsecure) would be helpful for target node to decide how to deal with the transferred UE capability.

Proposal 1: No further optimization for indicating the UE capability secured or unsecured when transferring to other nodes.

**Q3.2**: if the answer for **Q3.1** is yes, Do companies agree to indicate the UE capability unsecured in *HandoverPreparationInformation* message as following, also exemplified in [R2-2001614](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109_e/Docs/R2-2001614.zip), [R2-2001619](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109_e/Docs/R2-2001619.zip)?

*HandoverPreparationInformation* message

-- ASN1START

HandoverPreparationInformation ::= SEQUENCE {

 criticalExtensions CHOICE {

 c1 CHOICE{

 handoverPreparationInformation-r8 HandoverPreparationInformation-r8-IEs,

 spare7 NULL,

 spare6 NULL, spare5 NULL, spare4 NULL,

 spare3 NULL, spare2 NULL, spare1 NULL

 },

 criticalExtensionsFuture SEQUENCE {}

 }

}

HandoverPreparationInformation-r8-IEs ::= SEQUENCE {

 ue-RadioAccessCapabilityInfo UE-CapabilityRAT-ContainerList,

 as-Config AS-Config OPTIONAL, -- Cond HO

 rrm-Config RRM-Config OPTIONAL,

 as-Context AS-Context OPTIONAL, -- Cond HO

 nonCriticalExtension HandoverPreparationInformation-v920-IEs OPTIONAL

}

---omitted-----

HandoverPreparationInformation-v1540-IEs ::= SEQUENCE {

 sourceRB-ConfigIntra5GC-r15 OCTET STRING OPTIONAL, --Cond HO4

 nonCriticalExtension HandoverPreparationInformation-v15xy-IEs OPTIONAL

}

HandoverPreparationInformation-v15xy-IEs ::= SEQUENCE {

 ueCapabilitySecured-r15 BOOLEAN OPTIONAL,

 nonCriticalExtension SEQUENCE {} OPTIONAL

}

-- ASN1STOP

| *HandoverPreparationInformation* field descriptions |
| --- |
| ***ueCapabilitySecured***Indicates whether the UE Radio Capability is acquired after security activation (i.e. secured) or before it (i.e. unsecured). Source node shall not send unsecured UE capability to target node except unauthenticated emgencey call. If the field is absent, it is up to network implementation whether the UE capability is secured or unsecured. |

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Detailed comments** |
| China Telecom | **Yes** |  |
| Docomo | **Yes** |  |

Conclusion 4: 2 companies agree with the above change.

### 4: Sending unsecured UE capability (No unauthenticated emergency call)

SA3 has explicitly replied RAN2 except unauthenticated emergency call, the network shall not send unsecured UE capability to other network entities. This rule is fine for normal UE but not for NB-IoT UE. Since in current *HandoverPreparationInformation-NB* message, different from *HandoverPreparationInformation* message (in which UE-CapabilityRAT-ContainerList can be set size of 0), ue-RadioAccessCapabilityInfo-r13 field is mandatory. Therefore, for future proof (though SA3 is still discussing on security handling for NB-IoT CP solution.), we suggest it would be necessary to indicate the NB-IoT UE capability as valid or invalid when sending to other network entities (eNB/gNB or MME/AMF) as following, also exemplified in [R2-2001614](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109_e/Docs/R2-2001614.zip).

*HandoverPreparationInformation-NB* message

-- ASN1START

HandoverPreparationInformation-NB ::= SEQUENCE {

 criticalExtensions CHOICE {

 c1 CHOICE{

 handoverPreparationInformation-r13 HandoverPreparationInformation-NB-IEs,

 spare3 NULL, spare2 NULL, spare1 NULL

 },

 criticalExtensionsFuture SEQUENCE {}

 }

}

HandoverPreparationInformation-NB-IEs ::= SEQUENCE {

 ue-RadioAccessCapabilityInfo-r13 UE-Capability-NB-r13,

 as-Config-r13 AS-Config-NB,

 rrm-Config-r13 RRM-Config-NB OPTIONAL,

 as-Context-r13 AS-Context-NB OPTIONAL,

 nonCriticalExtension HandoverPreparationInformation-NB-v1380-IEs OPTIONAL

}

HandoverPreparationInformation-NB-v1380-IEs ::= SEQUENCE {

 lateNonCriticalExtension OCTET STRING OPTIONAL,

 nonCriticalExtension HandoverPreparationInformation-NB-Ext-r14-IEs OPTIONAL

}

HandoverPreparationInformation-NB-Ext-r14-IEs ::= SEQUENCE {

 ue-RadioAccessCapabilityInfoExt-r14 OCTET STRING (CONTAINING UE-Capability-NB-Ext-r14-IEs) OPTIONAL,

 nonCriticalExtension HandoverPreparationInformation-NB-Ext-r15-IEs OPTIONAL

}

HandoverPreparationInformation-NB-Ext-r15-IEs ::= SEQUENCE {

 ueCapabilityInvalid-r15 BOOLEAN OPTIONAL,

 nonCriticalExtension SEQUENCE {} OPTIONAL

}

-- ASN1STOP

| *HandoverPreparationInformation-NB* field descriptions |
| --- |
| ***ueCapabilityInvalid***Indicates the UE Radio Capability in this message is invalid. |
| ***ue-RadioAccessCapabilityInfo, ue-RadioAccessCapabilityInfoExt***The NB-IoT UE Radio Access Capability Parameters, see TS 36.306 [5]. |

**Q4**: Do companies agree gNB/eNBshould send NB-IoT UE capability to other network entities (eNB/gNB or MME/AMF) by indicating the UE capability is valid or invalid for future proof?

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Detailed comments** |
| Ericsson | **No** | No such optimization is needed in our view. |
| China Telecom | **Not sure** | We should study on this. But not sure if SA3 will provide a solution.  |
| Nokia, Nokia Shanghai Bell | **No** | This is not needed. |
| ZTE | **-** | Please see our comments above.  |
| CATT | **No** | We prefer not to add anything before SA3 has any agreement. |
| NEC | **?** | Need further discussion..As Rapporteur said, the UE capability is mandatory. Thus, even with this indication the source RAN should include the actual UE capability (ue-RadioAccessCapabilityInfo-r13) to ensure the backward compatibility (i.e. cannnot put a dummy information) for legacy target RAN. The legacy target RAN ignore the new indication. Is this correct understanding? |
| Apple | **No** |  |
| Docomo | **Maybe** | Majority companies would like to wait for SA3 response, we are fine with it. |

Conclusion 5: Majority companies think there is no need for this optimization before SA3 provide any solutions to RAN2. Two companies think we need further discussion after SA3 provide RAN2 solutions.

Proposal 2: No further optimization for indicating the NB-IoT UE capability valid or invalid when transferring to other nodes before SA3 provides any solution.

# 3 Conclusions

**Conclusions:**

Proposal 1: No further optimization for indicating the UE capability secured or unsecured when transferring to other nodes.

Proposal 2: No further optimization for indicating the NB-IoT UE capability valid or invalid when transferring to other nodes before SA3 provides any solution.

# 4 List of referenced documents

1. R2-2002049, “Unsecured UE capability handling,” NTT DOCOMO, INC.
2. S3-194488, “Reply LS on Handling of UE radio network capabilities in 4G and 5G”, SA3.
3. R2-2001604, “Unsecured UE capability handling,” NTT DOCOMO, INC.
4. R2-2001608, “Unsecured UE capability handling,” NTT DOCOMO, INC.
5. R2-2001614, “Unsecured UE capability handling,” NTT DOCOMO, INC.
6. R2-2001619, “Unsecured UE capability handling,” NTT DOCOMO, INC.