**3GPP TSG-RAN WG2 #109-e R2-2002049**

Electronic meeting, 24th February - 6th March, 2020

**Agenda item: 5.4.1.1**

**Source: NTT DOCOMO, INC.**

**Title: Unsecured UE capability handling**

**Document for: Discussion and Decision**

# 1 Introduction

SA3 agreed an LS on Handling of UE radio network capabilities [1]. In the LS, unsecured UE capability handling is mentioned. Based on the LS, this contribution discusses possible impact on RAN2 specifications.

# 2 Discussion

#### 2.1 Summary of the LS [1]

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

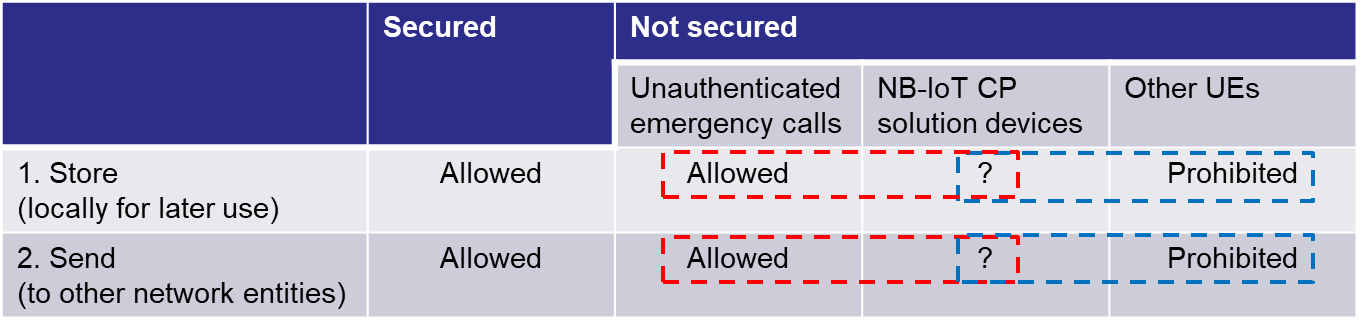
“With the exception of unauthenticated emergency calls, if the network had acquired UE capabilities using RRC UE capability transfer procedure before AS security activation, then the network shall not store them locally for later use and shall not send them to other network entities. In that case, the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

(Note that neither NB-IoT CP solution nor unauthenticated emergency calls can achieve secured UE capability enquiry because they doesn’t support security. That’s why they are under discussion/exception.)

Following table summarizes what the LS mentions.

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***

(Note that, for secured UE capability handling, it seems same with current behaviour; nothing needs to be clarified.)

#### 2.2 Impact on RAN2 specification

In this section, possible impact on RAN2 specification by the LS is analysed.

##### 2.2.1 Storing

###### 1-1: Storing is allowed

How to store and how to use stored UE capability would be up to implementation. (And, even not storing at all seems to be allowed.) So, nothing needs to be clarified.

###### 1-2: Storing is prohibited

In LS from SA3, it was not mentioned clearly 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 UE capability should be released.

***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.***

##### 2.2.2 Sending

There would be three cases for sending UE capability. One is for handover, another one is for retrieval UE context on e.g. reestablishment. The other is UE capability indication for CN.

###### 2-1: Sending is allowed

If the unsecured UE capability is sent, the receiver may misunderstand it as secured and use it as usual (e.g. store it for future use or send it to CN or other neighbour nodes without any restriction) even though the next call may not be “Unauthenticated emergency call” So, it would be necessary to indicate whether the UE capability is secured or unsecured.

1. Handover

On unauthenticated emergency call, EIA0 is necessarily used as follows.

TS33.401 [2]: 5.1.4.1 Integrity requirements

When authentication of the credentials on the UICC during Emergency Calling in Limited Service Mode, as defined in the TS 23.401 [2], can not be successfully performed, the integrity and replay protection of the RRC and NAS signaling shall be omitted (see clause 15). This shall be accomplished by the network by selecting EIA0 for integrity protection of NAS and RRC. EIA0 shall only be used for unauthenticated emergency calls.

So, the receiver can identify it by it.

TS36.413 [3]: 8.4.2.2 Successful Operation (Handover Resource Allocation)

If the *UE Security Capabilities* IE included in the HANDOVER REQUEST message only contains the EIA0 algorithm as defined in TS 33.401 [15] and if this EIA0 algorithm is defined in the configured list of allowed integrity protection algorithms in the eNB (TS 33.401 [15]), the eNB shall take it into use and ignore the keys received in the *Security Context* IE.

Note that similar description in TS33.501 (for NG-RAN), TS32.423, TS38.413, TS38.423.

On the other hand, it may be beneficial to add such indication (i.e. secure or unsecure) in RRC inter-node message for identifying it, otherwise the receiver need to check RAN3 explicit IE (nevertheless the UE capability itself is transferred in the RRC container, RAN2 expertise area).

***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.***

1. Retrieve UE context

On this case, even though same IE with handover is transferred, there is no limitation to send only EIA0. So, it seems necessary to indicate whether the UE capability is secured or not. This can be handled by RAN3 whether to a new IE is needed to indicate whether the UE capability is secured or unsecured.

1. UE capability indication

On this case, UE capability is transferred by several IEs (i.e. UE Radio Capability, UE Radio Capability for Paging, UE Application Layer Measurement Capability) in UE CAPABILITY INFO INDICATION message via S1/NG. This is up to RAN3 whether to work on the secured/unsecured indication.

###### 2-2: Sending is prohibited

When prohibited, there would be two ways. One is just not to transfer. The other is to transfer with invalid indication (e.g. unsecured). The first one would be straight forward but, in some case (e.g. backward compatibility), the latter may be beneficial. In following section, it is analysed further.

***Observation 3: For 2-2 (Sending is prohibited), there would be two ways (1) just not to transfer and (2) to transfer with invalid indication (e.g. unsecured).***

1. Handover

As mentioned in 2-1-(1), the UE capability is transferred via RRC container. And, RAN2 RRC structure seems to allow not to send RRC container as follows for normal UE but not allow for NB-IoT because HandoverPreparationInformation-NB message, different from HandoverPreparationInformation message ue-RadioAccessCapabilityInfo-r13 IE is mandatory; to achieve not to transfer with backward compatible way, the second option needs to be taken (i.e. to transfer with invalid indication).

***HandoverPreparationInformation message***

***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***

***}***

***UE-CapabilityRAT-ContainerList* information element**

-- ASN1START

UE-CapabilityRAT-ContainerList ::=SEQUENCE (SIZE (0..maxRAT-Capabilities)) OF UE-CapabilityRAT-Container

UE-CapabilityRAT-Container ::= SEQUENCE {

rat-Type RAT-Type,

ueCapabilityRAT-Container OCTET STRING,

}

-- ASN1STOP

***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***

***}***

***UECapabilityInformation-NB message***

***-- ASN1START***

***UECapabilityInformation-NB ::= SEQUENCE {***

***rrc-TransactionIdentifier RRC-TransactionIdentifier,***

***criticalExtensions CHOICE{***

***ueCapabilityInformation-r13 UECapabilityInformation-NB-r13-IEs,***

***criticalExtensionsFuture SEQUENCE {}***

***}***

***}***

***UECapabilityInformation-NB-r13-IEs ::= SEQUENCE {***

***ue-Capability-r13 UE-Capability-NB-r13,***

***ue-RadioPagingInfo-r13 UE-RadioPagingInfo-NB-r13,***

***lateNonCriticalExtension OCTET STRING OPTIONAL,***

***nonCriticalExtension UECapabilityInformation-NB-Ext-r14-IEs OPTIONAL***

***}***

But, anyway, RAN2 needs to discuss this topic.

***Observation 4: 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).***

***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).***

1. Retrieve UE context

UE capability is transferred in either the RRC inter-node message Handover Preparation Information message or the HandoverPreparationInformation-NB message. So, same principle with handover should be applied.

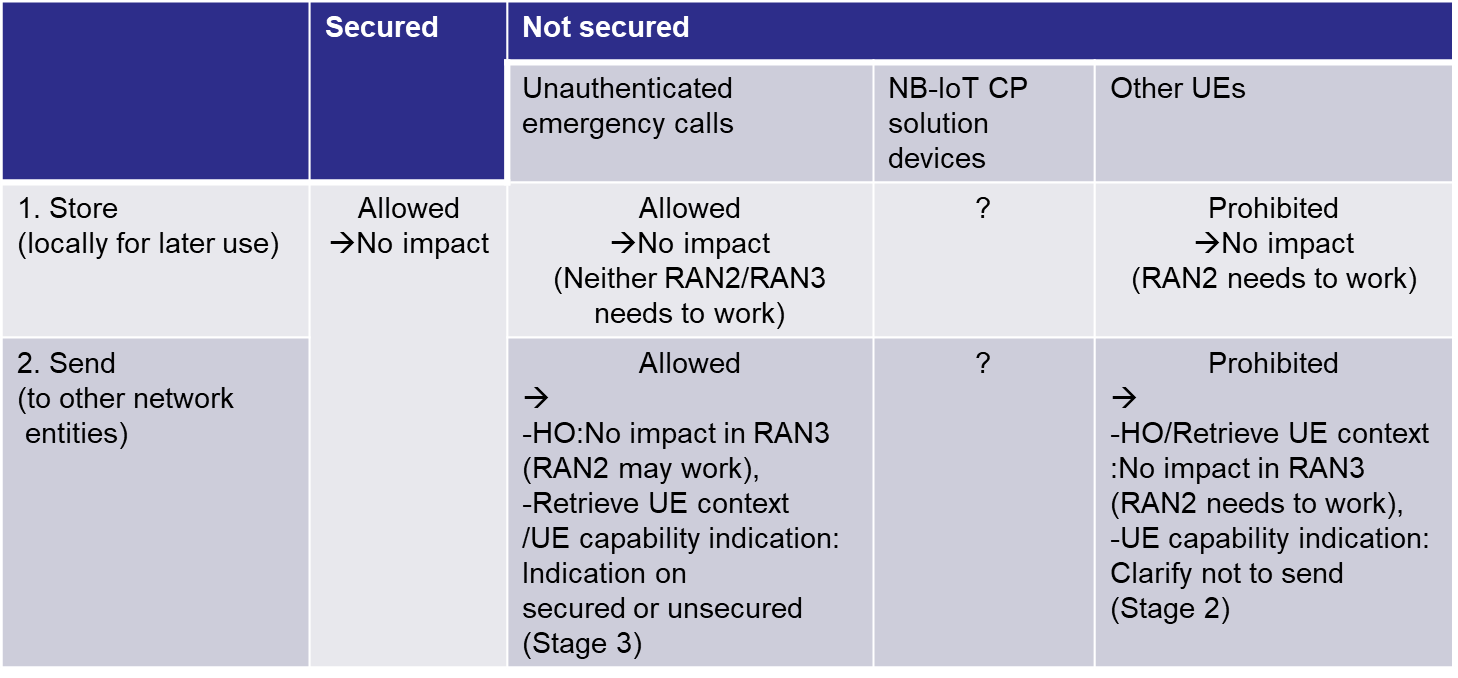
1. UE capability indication

As mentioned in 2-1-(3), UE capability is transferred via S1/NG. So, RAN3 needs to work on the handling. On the solution, it would be more straight forward not to transfer because, considering 2-1-(3), if going with invalid indication, three cases needs to be handled by CN unnecessarily (i.e. in addition to “Secured” and “not secured”, “invalid” is added). It would be necessary to clarify such behaviour in Stage 2.

##### 2.2.3 Summary

Following table summarizes above observations/proposals.

Table 2. Summary of observations/proposals.



# 3 Conclusion

Based on the LS [1] on unsecured UE capability, this contribution discusses possible impact on RAN2 specifications.

Following observations and proposals were obtained.

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

***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.***

***Observation 3: For 2-2 (Sending is prohibited), there would be two ways (1) just not to transfer and (2) to transfer with invalid indication (e.g. unsecured).***

***Observation 4: 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).***

***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).***

Corresponding CRs are available in [4-7]

# References

1. S3-194488, “Reply LS on Handling of UE radio network capabilities in 4G and 5G”, SA3.
2. TS33.401 v16.0.0
3. TS36.413 v15.7.1
4. R2-2001604, “Unsecured UE capability handling,” NTT DOCOMO, INC.
5. R2-2001608, “Unsecured UE capability handling,” NTT DOCOMO, INC.
6. R2-2001614, “Unsecured UE capability handling,” NTT DOCOMO, INC.
7. R2-2001619, “Unsecured UE capability handling,” NTT DOCOMO, INC.