3GPP TSG-RAN WG2 #113-e draftR2-2102039

Electronic meeting, Jan 25th – Feb 5th 2021

Agenda Item: 8.12.1

Source: Rapporteur (Ericsson)

Title: Summary of [AT113-e][108][REDCAP] UE identification and access restriction

Document for: Discussion, Decision

# Introduction

The document summarizes the following offline discussion:

* [AT113-e][108][REDCAP] UE identification and access restriction (Ericsson)

Scope: Continue the discussion on UE identification and access restriction based on the proposals in [R2-2100985](file:///C%3A%5CData%5C3GPP%5CExtracts%5CR2-2100985%20-%20%20TP%20for%20UE%20identification%20and%20access%20restriction.docx)

 The intention of this offline is to describe options in the TR and, whenever applicable/possible, also down-select some alternatives / provide some recommendations.

Initial intended outcome: Summary of the offline discussion with e.g.:

* + - List of proposals for agreement
		- List of proposals that require online discussions
		- Corresponding TP for the TR

Initial deadline (for companies' feedback): Monday 2021-02-01 16:00 UTC

Initial deadline (for rapporteur's summary in R2-2102018): Monday 2021-02-01 22:00 UTC

Updated Scope: Continue the discussion on p13, p18 and detailed TP for p16 and p17 from [R2-2102018](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_113-e/Inbox/R2-2102018.zip).

Updated intended outcome: Summary of the offline discussion with e.g.:

* + - List of proposals for agreement
		- Corresponding TP for the TR

Deadline (for companies' feedback): Wednesday 2021-02-03 18:00 UTC

Deadline (for rapporteur's summary in R2-2102039): Wednesday 2021-02-03 22:00 UTC

This is 2nd round of the previous offline, summarized in [R2-2102108](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_113-e/Inbox/R2-2102018.zip). The relevant proposals in the previous summary are **P13**, **P17** and **P18**:

|  |
| --- |
| **Proposal 13 The legacy UAC principle for Access Categories is assumed for RedCap, that is, different access types are differentiated using Access Categories.** Proposal 17 Capture following text in 11.2.1 on RRC Connection reject: ”To save radio resources and limit negative impact on legacy network performance it is beneficial to bar or reject UEs as early as possible, preferably without additional signalling. Therefore, cell barring and UAC is beneficial compared to RRC connection rejection. However, if the network is aware the UE is a RedCap during initial access, it is possible for the network to reject RRC connection based on UE being a RedCap UE. There is no additional specification impact in case early indication is specified.”Proposal 18 Discuss whether TR should capture RedCap access control by using separate RACH configuration.  |

Additionally, **P16** in R2-2102108 was agreed and a Text proposal is provided in this offline for companies to comment:

|  |
| --- |
| Capture following options with descriptions in TR for RedCap UAC (first two have been agreed to be studied earlier): 1) Define new Access Identity or Identities for RedCap UE 2) Define new Access Category or Categories for RedCap UE 3) Broadcast a separate set of parameters for RedCap UEs 4) Use existing broadcasted UAC parameters for RedCap UEs without any changes |

# Discussion

P13 in R2-2102108 was the result of discussion based on Proposal 3a as an attempt to clarify the original proposal which was misunderstood at least by some participants based on some of the company replies.

Proposal 13 The legacy UAC principle for Access Categories is assumed for RedCap, that is, different access types are differentiated using Access Categories.

To clarify the intention of P13 further:

* For RedCap UAC (which may be some of the options discussed in the agreed P16), different access types are mapped to Access Categories, which is exactly the same principle as in the legacy UAC.
* As a corollary, if a new Access Category is defined for a RedCap UE (type), then likely we would need to define multiple new Access Categories to map the possible access types to Access Categories like in legacy.
* The proposal does not suggest to add any new Access Categories without further discussion – this is not proposed now (also subject checking with SA1/CT1).
* Also subject to further discussion is whether all existing ACs apply to RedCap.

**Question 1: Do you agree to P13?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Agree to Q1 / P13**  | **Comments**  |
| Qualcomm | See comment | We agree with the intention of the proposal, but we can’t agree with how it is worded because it clearly suggests a specific implementation for applying UAC to RedCap and contradicts what is captured in the TP (different options will be studied). We’d therefore like to suggest the following wording instead: The legacy UAC principle is assumed for RedCap. FFS how it is applied for RedCap using access identity(s) and/or access category(s). |
| Intel | No | In the TR, we already captured“*The unified access control (UAC) framework is specified in TS 22.261 and it applies to all UEs in RRC\_IDLE, RRC\_CONNECTED and RRC\_INACTIVE. This mechanism should also apply to RedCap UEs to control RedCap UEs accesses to the network.* “We think the highlighted sentence already reflected the current status well.  |
| OPPO | No | We agree with Intel. |
| vivo | Agree with the intention | We are fine with the wording suggested by Qualcomm. |

The following proposal for TP for “RRC Connection Reject” was discussed online and agreed to be captured in the TR with further offline discussion on the wording:

Proposal 17 Capture following text in 11.2.1 on RRC Connection reject: ”To save radio resources and limit negative impact on legacy network performance it is beneficial to bar or reject UEs as early as possible, preferably without additional signalling. Therefore, cell barring and UAC is beneficial compared to RRC connection rejection. However, if the network is aware the UE is a RedCap during initial access, it is possible for the network to reject RRC connection based on UE being a RedCap UE. There is no additional specification impact in case early indication is specified.”

|  |
| --- |
| RRC Connection RejectTo save radio resources and limit negative impact on legacy network performance it is beneficial to bar or reject UEs as early as possible, preferably without additional signalling. Therefore, cell barring and UAC is beneficial compared to RRC connection rejection. However, if the network is aware the UE is a RedCap during initial access, it is possible for the network to reject RRC connection based on UE being a RedCap UE. There is no additional specification impact in case early indication is specified. |

**Question 2: Please provide suggestions on the wording of the TP, if any.**

|  |  |
| --- | --- |
| **Company** | **Comments / text proposal** |
| Qualcomm | We are fine with this TP. |
| Intel | We are fine with this TP |
| OPPO | We are fine with this TP |
| vivo | We are fine with it in general. Besides, we suggest to modify the below sentence in a more general way as following:However, if the network is aware the UE type during initial access, it is possible for the network to reject RRC connection based on UE type. |

The following proposal related to access control by separate RACH configuration was agreed to be continued to be discussed offline.

During the previous round some companies considered this as not needed. However, this option has been discussed in some of the submitted tdocs since the beginning of RedCap SI. The rapporteur thinks that all reasonable options should be captured in the TR. Note, again, that capturing a solution in the TR does not mean endorsing such solution in any way, but if will show RAN2 has done its part on studying different possible options.

Therefore, the first question is about whether to capture the option at all or not:

**Question 3: Do you agree to capture “Access control using separate RACH configuration” in the TR as one possible method in the study of access restrictions?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Reply to Q3**  | **Comments** |
| **Qualcomm** | See comment | We do not support using separate RACH configuration for access control. We are fine with having RedCap-specific RACH parameters through separate RACH configuration for RedCap. In our view, this separation is more about enabling differentiated RACH, instead of differentiated access control. RACH and access control serve different purposes and should not be mixed.So we do not think it should be captured as one of possible methods for access restriction or access control. Maybe it can be captured in a different section instead? |
| Intel | ok | Ok to capture candidate solutions in the TP.  |
| OPPO | No | Access control should be implemented by cell barring and UAC. We don’t support to use separate RACH configuration to restrict access of RedCap UEs.  |
| vivo | No | We think separate RACH configuration is not intended for access control. For access control, we already has UAC and cell barring by SI, which is enough.  |

During previous round of offline 108 a detailed text proposal was discussed. If companies agree to add the solution in the TR, the following is an update to the previous text proposal (actually, re-written TP):

|  |
| --- |
| Access control using separate RACH configurationOne possibility to control RedCap UEs vs non-RedCap UEs access is to use separate RACH configuration for RedCap, that is, configure the parameters for RedCap UEs random access in a different way.Possible methods include not configuring RACH resources (if s separate resources for RedCap UEs are configured), different number of maximum attempts for preamble transmission, different back-off time after an attempt or a different power ramping step for RedCap UEs. If separate RACH resources are agreed to be used for RedCap UEs (e.g., due to need for early indication in Msg1), there would be limited specification impact. In case separate RACH resources are not defined for early indication, there would be larger impact as separate RACH configuration would need to be defined and used by the RedCap UEs. |

The following question is conditional on the previous Question 3:

**Question 4: Do you agree to include the above TP for “Access control using separate RACH configuration” in the TR (conditional on Q3)?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Reply to Q4** | **Comments / Further TP suggestions** |
| Qualcomm | See comment | We are fine with capturing body of the above text in a more appropriate section in the TR (sorry we don’t have a good suggestion at the moment).  |
| Intel | ok | Ok to capture candidate solutions in the TP.  |
| OPPO |  | See our reply to Q3. |
| vivo |  | See above. |

P16 related to UAC was agreed during the online session. There were comments from companies during the first round of offline 108 which are now taken into account in a revised text proposal.

Agreement:

|  |
| --- |
| Capture following options with descriptions in TR for RedCap UAC (first two have been agreed to be studied earlier): 1) Define new Access Identity or Identities for RedCap UE 2) Define new Access Category or Categories for RedCap UE 3) Broadcast a separate set of parameters for RedCap UEs 4) Use existing broadcasted UAC parameters for RedCap UEs without any changes |

|  |
| --- |
| Unified Access ControlThe unified access control (UAC) framework is specified in TS 22.261 and it applies to all UEs in RRC\_IDLE, RRC\_CONNECTED and RRC\_INACTIVE. This mechanism should also apply to RedCap UEs to control RedCap UEs accesses to the network. In UAC each access attempt is associated with an *Access Category* and one or more *Access Identities* (defined in TS 24.501). The possible solutions for RedCap UAC that have been considered in the study are the following (the options do not need to be mutually exclusive):* Define one or more RedCap specific Access Identities. Access Identities are connected to the UE type and are (currently) used to lift the barring for certain identities, e.g. for special access classes or UEs configured for prioritized services.
* Define RedCap specific Access Categories. Access Categories are related to the type of access attempt and is set per access attempt type depending on what triggered the access (set by NAS if NAS triggered, or by RRC if AS triggered). There can only be one Access Category per access attempt. To be able to treat different RedCap access attempt types differently, e.g. apply different barring two different access types, multiple Access Categories for RedCap could be defined.
* Use some of the operator defined Access Categories for RedCap. The description of the previous solution applies also to this solution, the difference is that this solution has no specification impact but cannot be used for initial attach to the network since it depends to CN configuration of the UE.
* Broadcast a different set of UAC parameters for RedCap UEs. This makes it possible for NW to flexibly and separately provide UAC parameters for RedCap UEs while avoiding impact on UAC configuration of non-RedCap UEs.
* Use existing broadcasted UAC parameters for RedCap UEs with no changes, that is, the same UAC parameters apply for all UEs (non-RedCap UEs and RedCap UEs) and no new Access Categories and Access Identities are defined. This option requires no specification changes.

UAC is defined in TS 22.261 and TS 24.501, and feasibility of the options (e.g. defining new Access Identities or Access Categories) should be consulted with SA1/CT1. |

**Question 5: Do you agree to include the text proposal on UAC in the TR? Please provide a text proposal if you prefer update to the suggested text.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Reply to Q5 / Agree TP**  | **Comments / Text proposals** |
| Qualcomm | Agree |  |
| Intel | Agree |  |
| OPPO | Agree |  |
| vivo | Agree |  |
|  |  |  |

# Summary

TBD

# Delegate contact information

|  |  |
| --- | --- |
| Company | Delegate contact |
| COMPANY\_NAME | NAME (email@address.com) |
| Rapporteur (Ericsson) | tuomas.tirronen@ericsson.com |
| Qualcomm | Linhai He (linhaihe@qti.qualcomm.com) |
| Intel | Yi.guo@intel.com |
| OPPO | Haitao Li (lihaitao@oppo.com) |
| vivo | Chenli (Chenli5g@vivo.com) |