**3GPP TSG-RAN WG2 Meeting #127 *R2-24XXXXX***

**Maastricht, Netherlands, August 19 – 23, 2023**

|  |
| --- |
| *CR-Form-v12.3* |
| **CHANGE REQUEST** |
|  |
|  | **38.843** | **CR** | **-** | **rev** | **-** | **Current version:** | **18.0.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network | **X** | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | RAN2 inputs to TR 38.843 |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | R2 |
|  |  |
| ***Work item code:*** | FS\_NR\_AIML\_Air  |  | ***Date:*** | 2024-06-08 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-19 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19) Rel-20 (Release 20)* |
|  |  |
| ***Reason for change:*** | Introduce in the Technical Report R2’s agreements concerning UE-side data collection. |
|  |  |
| ***Summary of change:*** | Section 7.2.1.3 includes updates as per the RAN2#126 agreements. |
|  |  |
| ***Consequences if not approved:*** | Section 7.2.1.3 includes updates as per the RAN2#126 agreements. |
|  |  |
| ***Clauses affected:*** | 7.2.1.3, 7.2.1.3.2 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** | This CR considers the latest agreements (as of end of RAN2#126) |
|  |  |
| ***This CR's revision history:*** |  |

*START OF CHANGES*

#### 7.2.1.3 Data collection

Data collection plays a crucial role in enabling the different use cases. Therefore, it is important to define the best approaches for collecting data to support UE-side and network-side model inference, monitoring, and training.

Table 7.3.1.2-1 lists existing data collection mechanisms available in current RAN specifications for the UE to report measurements to another entity acting as termination point for this data. As highlighted in clause 4.2, the analysis/selection of the data collection frameworks should focus on the RRC CONNECTED state for both data generation and reporting. As such, the Table can provide useful insights into existing methods with respect to various categories identified as relevant for data collection method selection.

Table 7.2.1.3.1-1. Existing data collection methods identified.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Involved network entity (termination point)** | **RRC state to generate data** | **Max payload size per reporting\*** | **Contents to be collected** | 1) **End-to-End report latency\*\*** | **Report type** | **Security and Privacy** |
| **Method: Logged MDT** |
| TCE/OAM(Data can be utilized by gNB) | IDLE / INACTIVE | <9kbyte | - L3 cell/beam measurements- location information- sensor information- timing information | 1) Procedure latency\*\*\*:- Latency to enter CONNECTED state- Latency to receive gNB request signalling (~20ms)2) Air interface signalling latency\*\*\*\*: - ~20ms (RRC)3) Other latency:- Forwarding latency between gNB and TCE | Upon gNB request after entering RRC\_CONNECTED | AS security via RRC messagePrivacy via user consent  |
| **Method: Immediate MDT** |
| TCE/OAM(Data can be utilized by gNB) | CONNECTED | <9kbyte | - L3 cell/beam measurements- location information- sensor information | 1) Procedure latency:- Report interval:  120ms~30min for periodic report TTT for event triggered report2) Air interface signalling latency:- ~20ms (RRC)3) Other latency:- Forwarding latency between gNB and TCE  | - Event triggered- Periodic reporting  | AS security via RRC messagePrivacy via user consent |
| **Method: L3 measurements** |
| gNB | CONNECTED | <9kbyte | L3 cell/beam measurements | 1) Procedure latency:- Report interval:  l20ms~30min for periodic report TTT for event triggered report2) Air interface signalling latency:- 20ms (RRC) | - Event triggered report- Periodic reporting | AS security via RRC message |
| **Method: L1 measurement (CSI reporting)** |
| gNB | CONNECTED | <1706bit in PUCCH<3840bit in PUSCH | L1 CSI measurement | 1) Procedure latency:- Report interval:  4-320 slot for periodic and semi-persistent report  0-32 slot after reception of DCI for aperiodic report 2) Air interface signalling latency:- 1 TTI (PUCCH)  | - Aperiodic report- Semi-persistent report- Periodic report | No AS security |
| **Method: UE Assistance Information (UAI)** |
| gNB | CONNECTED | <9kbyte | Assistance information to show UE preference | 1) Procedure latency:- Upon generation of UE's preference2) Air interface signalling latency:- ~20ms (RRC) | Up to UE implementation when to report | AS security via RRC message |
| **Method: Early measurements** |
| gNB | IDLE / INACTIVE | <9kbyte | L3 cell/beam measurements | 1) Procedure latency:- Latency to enter CONNECTED state- Latency to receive gNB request signalling (~20ms)2) Air interface signalling latency: - ~20ms (RRC) | Upon gNB request after entering RRC\_CONNECTED | AS security via RRC message |
| **Method: LPP** |
| LMF | CONNECTED | <9kbyte | Location information | 1) Procedure latency:- Latency to get upper layer trigger (for UE triggered)- Or latency to receive network request message (~20ms)2) Air interface signalling latency: - ~20ms (RRC)3) Other latency:- Forwarding latency between gNB and LMF | - UE-triggered- Network-triggered | AS security via RRC message |
| \*: The payload size doesn't consider signalling overhead.\*\*: The End-to-End report latency is the latency from availability of the measurement report at the UE side to the availability of the measurement report at the terminated network entity. The time to generate data or perform measurements depends on RAN1/RAN4 specification.\*\*\*: Procedure latency is the latency caused by procedures, including procedure to ready for reporting (e.g., entering CONNECTED state, report interval).\*\*\*\*: Air interface signalling latency is the latency to transmit one report, e.g., RRC signalling latency or PUCCH signalling latency. |

*NEXT CHANGE*

##### 7.2.1.3.2 Data collection for UE-side model training

The following options were discussed in RAN2:

1a. UE collects and directly transfers training data to the training entity outside the MNO (e.g. Over-The-Top (OTT) server) for the purpose of UE-side model training. No 3GPP specification involvement is expected.

1b. UE collects training data and transfers it to the server for data collection for UE-side model training/OTT server. 3GPP specification involvement is expected.

2. UE collects training data and transfers it to Core Network. Core Network transfers the training data to the server for data collection for UE-side model training/OTT server. 3GPP specification involvement is expected.

3. UE collects training data and transfers it to OAM. OAM transfers the training data to the server for data collection for UE-side model training/OTT server. 3GPP specification involvement is expected.

The options listed above were analysed to understand potential specification impact. The analysis included aspects such as termination entities, data transfer path, whether control plane (CP) or user plane (UP) should be used to transfer the data, protocol layers involved, MNO controllability and visibility over the collected data, etc… The result of this analysis can be found below in Table 7.2.1.3.2-1.

It is worth noting that for the different options, the following levels of data content visibility were discussed:

1. Full visibility for standardized data content.
2. Partial visibility for partially standardized data content.
3. No standardized visibility.

Note: According to RAN2, the data content visibility could be achieved via SLA. However, the details are out of RAN2 scope.

Furthermore, according to RAN2, the Option 1a above has no specification impact.

Table 7.2.1.3.2-1. Analysis of different data collection options for UE-side model training.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  **Option****Aspect** | **1a) Data is directly transferred to the training entity without 3GPP specification involvement** | **1b) Data is directly transferred to the training entity with 3GPP specification involvement** | **2. Data is transferred to the training entity via Core Network** | 1) **3. Data is transferred to the training entity via OAM**  |
| **First termination entity** | Training entity (e.g., Over-The-Top (OTT) server) | Server for data collection for UE-side model training | Inside the CN (e.g., LMF) | Inside OAM domain |
| **AI/ML-specific Data Transfer Path** | UE to OTT server via either 3GPP or non-3GPP network | UE-> CN ->Server for data collection for UE-side model training/OTT server(Note 4) | UE-> CN -> Server for data collection for UE-side model training/OTT server(Note 4) | UE-> OAM -> Server for data collection for UE-side model training/OTT server(Note 4) |
| **UP/CP tunnel** | UP tunnel | UP tunnel  | CP tunnel (provided that the data volume remains within the NAS signalling capacity)FFS: UP tunnel | CP tunnel (provided that the data volume remains within the RRC signalling capacity)FFS: UP tunnel |
| **Protocol layer for data transfer** | Application layer | Application layer | NAS layer for CP tunnelFFS: the protocol layer for UP tunnel | RRC layer for CP tunnelFFS: the protocol layer for UP tunnel |
| **Controllability of MNO on data transfer** | No AI/ML specific controllability | Controllability can be achieved.FFS: level of controllability | Full controllability (Note 1) | Full controllability(Note 1) |
| **Control granularity by NW** | N/A (the OTT server can directly request data from the UE) | Example: per PDU sessions  | NAS procedureFFS: impact to other layers | RRC procedure |
| **Possible Options for Visibility of data content in MNO and Data format (Note 2, Note 3)**  | No standardized visibility | FFS  | Opt A) Full visibility for standardized data content.FFS: Opt B) Partial visibility for partially standardized data content. FFS Opt C) No standardized visibility.FFS: meaning of ‘partial/partially’ and how to achieve different levels of visibility. | Full visibility for standardized data content.Partial visibility for partially standardized data content.No standardized visibility.FFS: meaning of ‘partial/partially’ and how to achieve different levels of visibility. |
| **Involved WGs** | N/A | SA2, SA3, RAN2 | SA2, SA3, RAN3, RAN2, CT1 and CT3 | RAN2, RAN3, SA3, SA5, FFS SA2 |
| * Note 1: Full controllability: The MNO has the capability to manage data transfer to the server for UE-side data collection. This includes initiating, terminating, and fully managing data transfer. FFS if further refinements/modifications to this definition are needed.
* Note 2: Visibility of data content signifies the capability of the MNO to, at least, be aware of, access, and comprehend the data during transfer. FFS if further refinements/modifications to this definition are needed (e.g. on the capability of the MNO to modify the collected data).
* Note 3: For Solution 1b, 2/3, the following options are identified to realize the different levels of data content visibility if different levels of data content visibility to MNO are considered.
	+ Full visibility for standardized data content.
	+ Partial visibility for partially standardized data content.
	+ No visibility for non-standardized data content.
* Note 4: The potential involvement of NF or other higher layers entities/functionalities should be discussed in other WGs.
 |

Related to privacy, it has been stressed in RAN2 the importance that any potential mechanism to collect UE side data for model training purposes (including the options 1a, 1b, 2, 3 listed above) must comply with privacy protection regulations, requirements, laws and/or policies. An informative Annex is included at the end of this document capturing examples of privacy concerns for different stakeholders participating in the discussion.

*NEXT CHANGE*

Annex <Y>:
Informative Annex: Privacy concerns

This Annex compiles some examples of privacy concerns raised during RAN2’s discussion.

MNO:

* Network Information Disclosure: MNOs may inadvertently disclose sensitive network information, such as deployment strategies, network configurations, and performance metrics, to servers outside their network.
* Data Transfer Risks: MNOs are obliged to protect private and/or undisclosed information about the network of users/customers when transferring data to external servers. This could include subscriber identities, locations, website visited, phone calls, etc…
* Regulatory Restrictions: Operators are bound by regulations which mandate the protection of customer data. Thus, any lack of control over data may lead to unwanted exposure of personal information.
* Risk of Penalties: Non-compliance with regulatory guidelines due to improper data handling could result in significant fines or restrictions for the operators.
* Need for Control and Tools: MNOs require robust tools and mechanisms to oversee and control data collection and processing to prevent any leaks or unauthorized sharing of information.
* Data Collection Termination: It is crucial that the initial termination point of data collection be within the operator's network infrastructure (such as CN or OAM) to ensure privacy and compliance.

Network Vendor:

* Sensitive Information Leakage: Network vendors may possess proprietary algorithms, system designs, and other intellectual property that are integral to their competitive edge. Unintentional disclosure of such information to third parties could undermine their market position and lead to potential legal issues.
* Implementation Details Exposure: The specific details of how network equipment is implemented, including software and hardware design, are crucial for maintaining the security and integrity of the network. If such information is disclosed, it could be exploited for malicious purposes or used by competitors to gain insights into the vendor's technology.
* Radio Topology and Settings Disclosure: Disclosing details such as radio topology and specific radio configurations should be prevented, because such information is sensitive and could affect operational security.
* Violation of user privacy regulation: The equipment of the network vendor may be used for collecting user’s data without getting approval/consent from the user in advance, and this behaviour may violate the local regulations and risks the sales of the equipment.

Chipset Vendor:

* Proprietary Technology Exposure: Chipset vendors develop specialized hardware and software that may contain trade secrets or patented technologies. Here is a risk that the sensitive data could be exposed to a second vendor without the original chipset vendor's knowledge, which could compromise their competitive advantage and innovation.
* Respect for Implementation Secrecy: There is a universal understanding within the industry that chipset vendors often add proprietary layers on top of standardized specifications, and these unique implementations are critical for maintaining a diverse and successful ecosystem. The non-disclosure of such proprietary information is seen as essential for the continued success of industry standards.

OEM:

* User Information Disclosure: OEMs handle a vast amount of user data, including personal information, usage habits, and location data. There is a significant privacy concern if this information is disclosed to external entities without user consent, potentially violating privacy laws and damaging the OEM's reputation.
* Proprietary Technology Exposure: OEM vendors develop specialized hardware and software that may contain trade secrets or patented technologies. Here is a risk that shared information could be unintentionally disclosed to unauthorized parties, leading to privacy breaches. Another risk is that some sensitive data of an OEM vendor may be exposed to a second vendor without the knowledge of the OEM vendor.
* Consent for Data Collection: OEMs are adamant that user data should not be shared with third-party entities without explicit and informed user consent. Such disclosure might occur without the knowledge of the UE vendor, who is legally bound by a data protection agreement with the user.
* Universal adherence to privacy principles is a critical aspect of the data collection and transfer process, regardless of the technology or method employed. All entities involved in data handling must give due consideration to the varied privacy concerns expressed by stakeholders across the communication landscape. This includes OEMs, chipset vendors, network vendors, MNOs, and ultimately the end-users whose data may be collected. It is advisable for RAN2 to consider these shared privacy concerns as a starting point and document these concerns, possibly as informative annexes. It would serve as a useful reference for stakeholders, ensuring that privacy considerations are integrated into the discussion and decision-making processes.

*END OF CHANGES*