**3GPP TSG-WG SA2 Meeting #141E *S2-2007387r04***

**Elbonia, October 12 – 23, 2020 (revision of S2-2007387+6860+7015+7278+7292+7642+7724)**

**Source: Qualcomm Incorporated**

**Title: Evaluation for Key Issue #8: UE data as an input for analytics generation**

**Document for: Approval**

**Agenda Item: 8.1**

**Work Item / Release: FS\_eNA\_Ph2 / Rel-17**

*Abstract:* This contribution proposes the evaluation for KI#8*.*

# 1. Introduction

This contribution proposes the evaluation for KI#8: UE data as an input for analytics generation.

# 2. Text Proposal

It is proposed to capture the following new text in TR23.700-91.

\* \* \* \* Start of Changes \* \* \* \*

# 7 Overall Evaluation

Editor's note: This clause will provide evaluation of different solutions.

## 7.8 Key Issue #8: UE data as an input for analytics generation

According to table 6.0-1, solution #27, #28, #29, #62, #63, #64 and #65 are proposed for Key Issue #8.

Table 7.8-1 Evaluation of solutions related to KI#8

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Solution** | **Data collection procedure** | **Parameters collected from UE** | **Trigger of UE data reporting** | **Integrity and Privacy aspects** |
| **27** | UP Solution: UE reports to MNO AF directly | - | MNO AF Event Exposure | HTTPS, Data ciphering, ASP-level user consent |
| **28** | CP Solution | Policy enforcement related information:URSP enforcement  | URSP enforcement update | - |
| **29** | UP Solution: UE reports to (MNO) AF | Application layer information:Part of collective behaviour attributes Application Status information |  UE reports to (MNO) AF | HTTPS, Data anonymisation, ASP-level user consent |
| **62** | - | Policy enforcement related information:Applied WLANSP rule | Events described in the data collection configuration provided by PCF | - |
| **63** | - | Application layer Information: Service experience contribution | Request from AF | - |
| **64** | UP Solution: UE reports to DC AF indirectly | - | DC AF Event Exposure | HTTPS |
| **65** | - | - | Existing or new event triggers via AMF  | - |

For UE data collection procedure, there are two sets of solutions proposed.

User plane solution set:

* Solution #27: UE establishes a user plane connection to MNO AF which is the entity operated by operator. Application layer data request and data report are performed between UE and MNO AF via user plane. The MNO AF provides the data after possible processing like aggregation, normalization, etc. to the NWDAF using Naf\_EventExposure.
* Solution #64: UE establishes a user plane connection to Application Server, Application layer data request and data report are performed between UE and Application Server via user plane. Application Server forwards the data after possible processing to a DC AF owned by operator which in turn exposes it to the NWDAF using Naf\_EventExposure.
* Solution #29 propses a procedure similar to solution #27. If the NWDAF e.g. through prior AF reporting and/ or MDT does not have the requested parameters, it may request the (MNO) AF to configure the application client in the UE in order to provide the data to the (MNO) AF. The (MNO) AF may anonymise, normalise or aggregate the data based on configuration policies agreed before notifying the UE input data.

Control Plane solution set:

* Solution #28: The data request message is encapsulated in a transparent container sent from NWDAF to AMF and then AMF forwards the container to UE via NAS message. UE data reporting is also encapsulated in a transparent container sent to AMF via NAS message and AMF forwards the container to NWDAF.

Other solutions do not explicitly propose the data collection procedure..

For user plane solution, the data collection / report procedure is performed in application layer and treated as data transmission in PDU session. For control plane solution, it requires additional NAS siganlling for data transmission.

For the proposed parameters that collected from UE, there are several different proposals.

* Application layer information:
	+ Solution #27 and solution #64, general solutions for application layer parameters. The solutions may support both 3GPP defined service and non-3GPP defined services but do not define specific parameters to be collected from UE.
	+ Solution # 63: Service experience contribution.
	+ Solution # 29, Part of collective behaviour attributes: (when can not be collected via prior AF reporting and / or MDT) which may include the route, destination, average speed information, time interval spent per location. The usage of this information is to enhance NF load analytics (e.g., for AMF load balancing)
	+ Solution #29, Application status information: which indicates whether flow of the application is in a foreground status or background status. The usage of this information is different than the NF load analytics (i.e. it is to determine new QoS parameters for a new flow, e.g. by PCF). How Network allocation of resources will be impacted based on the foreground status and background status to be clarified as the procedure after UE data collection is not covered.
* Policy enforcement related information:
	+ Solution #28: UE reports the applied RSD information to NWDAF, PCF can use the analytics report to allocate more proper RSD for UE.
	+ Solution # 62: NWDAF collects data from the UE about which of several WLANSP rules and groups of selection criteria is directly involved in the WLAN selection. It also collects data that can measure the quality and performance of the WLAN connection from other 5GC NFs. NWDAF reveals the correlation between WLANSP that UE applied when selecting the WLAN and the resulting WLAN performance. The PCF can use the analytics results to update the WLANSP to improve WLAN performance.

The justification of collecting these policy enforcement related information is not clear, there are multiple inputs and situations that would affect the applicability of the URSP rules, some rules may not be valid due to network access availability, the URSP enforcement may also depends on the URSP engine implementation. In addition, a URSP rule for an application will not be enforced by the UE if the user did not install or used the specific application for a period of time but this does not mean that the user will not start using the specific application in the future, hence it does not make sense to remove the applicable URSP rule if it is not enforced by the UE. The UE should be provided with the superset of rules that is expected to be used in a particular region beforehand. If the UE does not apply a specific URSP rule does not mean the allocated rule is not going to be matched in the future. The proposal of URSP enforcement in solution #28 and the Applied WLANSP rule in solution #62 does not justify the useful for the proposed analytics feature. For solution #62, it is already supported to collect the WLAN SSID by MDT/SON solution, NWDAF can analytics the result based on the already supported parameters from OAM and UPF and there is no need to collect other proposed parameters from UE.

Solution #65 considers the trigger about UE data collection, UE reports the supported type of data to AMF during registration, NWDAF will collect the number of UEs that supporting a specific type of data collection and decide whether start or stop data collection from UEs. The proposal is complementary to the solutions above and combination to other triggers of UE data reporting to be clarified.

\* \* \* \* End of Changes \* \* \* \*