**3GPP TSG- Meeting #**

**, Greece,**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | 0003 | **rev** | **-** | **Current version:** |  |  |
|  |
| *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 |  | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  |  |
|  |  |
| ***Source to WG:*** |  |
| ***Source to TSG:*** | S4 |
|  |  |
| ***Work item code:*** | EVEX |  | ***Date:*** |  |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** |  |
|  | *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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | There are a couple of areas in TS 26.531 where corrections and additions are proposed, to more properly meet the assumptions and objectives of EVEX stage 2 with regards to UE data collection, reporting and exposure functionality. |
|  |  |
| ***Summary of change:*** | * Clauses 4.2 and 4.5.2:
	+ Control of event exposure control in the case of conflict between ASP-defined provisioning rules as conveyed in Data Access Profile and event subscription information should not always defer to the ASP provisioning rules when these are more restrictive than that requested by the subscribing event consumer. This especially applies to event exposure of UE data pertaining to 3GPP-defined reporting domains where the event consumer is the NWDAF.
* Clauses 4.3 and 4.5.2:
	+ Beside indicating what data is to be collected (i.e., set of paramters) being conveyed in the provisioning information issued by the ASP at reference point R1, other information such as how that data should be collected (by format, time, location and possibly other criteria) or whether the collected data should be actually reported by the data collection client to the Data Collection AF (e.g., by sample percentage). Doing so would match the provisioning functionality, for example, as defined in TS 26.501 and TS 26.512 regarding 3GP-DASH QoE metrics collection and reporting rules to be followed by the 5GMSd Client in the logging reporting of QoE metrics to the 5GMSd AF.
 |
|  |  |
| ***Consequences if not approved:*** | Incorrect and incomplete specification. |
|  |  |
| ***Clauses affected:*** | 4.2, 4.3 and 4.5.2 |
|  |  |
|  | **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's revision history:*** |  |

FIRST CHANGE

## 4.2 Functional entities for data collection and reporting

Figure 4.2‑1 below shows the reference architecture for data collection and reporting using reference point notation.



NOTE: The Data Collection AF may be deployed outside the trusted domain, in which case the services it exposes to API invokers are mediated by the NEF. The logical relationships denoted by the reference points are unaffected by such deployment choices.

Figure 4.2‑1: Reference architecture for data collection and reporting in reference point notation

(SNIPPED)

The set of UE data to be collected and exposed by the Data Collection AF is determined by the intersection[[1]](#footnote-1) between its provisioning state provided at R1 and the current set of subscriptions. This is reflected in the data collection and reporting configuration exposed at reference points R2, R3 and R4, and the subscription-driven event notifications sent to consumer entities such as the NWDAF or Event Consumer AF of an Application Service Provider over reference points R5 and R6. The Data Collection AF is responsible for ensuring that access to UE data is controlled according to the rules indicated in its provisioning state.

(SNIPPED)

NEXT CHANGE

## 4.3 Reference points for data collection and reporting

The purposes of the reference points in the functional architecture defined in clause 4.2 above are as follows:

- **R1** supports the following interactions between a Provisioning AF in the Application Service Provider and the Data Collection AF:

- Used by the Application Service Provider to provision data collection and reporting in a Data Collection AF instance by means of the Ndcaf\_DataReportingProvisioning service defined in clause 4.4 of the present document (or else the equivalent service exposed by the NEF if the two functions are deployed in different trust domains). The provisioning information specifies what data is to be collected, and additionally may specify how that data should be reported (e.g., by format, time and location) and whether that data should be reported (e.g., by sample percentage) by data collection clients, how it is to be processed by the Data Collection AF and how it is to be exposed to event notification subscribers. A generic provisioning envelope for data collection and reporting is defined in clause 4.6 of the present document, but this is expected to be extended by individual reporting domains.

- **R2** supports the following interactions between the Direct Data Collection Client in the UE and the Data Collection AF:

- Used by a Direct Data Collection Client instance to obtain its data collection and reporting configuration from the corresponding Data Collection AF instance by means of the Ndcaf\_DataReporting service defined in clause 4.4 of the present document. A generic data collection and reporting configuration envelope is defined in clause 4.6.3 of the present document, but details of the configuration are specific to individual reporting domains and are specified elsewhere.

- Subsequently used by the Direct Data Collection Client to send reports to its Data Collection AF instance by means of the Ndcaf\_DataReporting service defined in clause 4.4 of the present document. A generic data reporting envelope is defined in clause 4.6.4 of the present document, but details of the reporting by format and other rules (e.g., by dimensions of time, location and sample percentage) are specific to individual reporting domains and are specified elsewhere.

NOTE 1: This method of reporting corresponds to the direct data collection procedure defined in clause 6.2.8 of TS 23.288 [4].

(SNIPPED)

NEXT CHANGE

### 4.5.2 Data exposure restriction model

The Provisioning AF restricts the exposure of UE data over reference points R5 and R6 by configuring a set of Data Access Profiles for each Event ID to be exposed. A Data Access Profile specifies a set of data processing operations that need to be performed by the Data Collection AF on the collected UE data in order to synthesize the event data that will be exposed to the NWDAF and/or Event Consumer AF.

NOTE: The UE data exposure restrictions specified in an instance of Data Access Profile to be followed by the Data Collection AF regarding permitted event data exposure to the NWDAF for a given Event ID should apply only to the UE data specific to the ASP application (as identified by External Application Identifier). In other words, it should not be possible for the Data Access Profile to restrict exposure, to the NWDAF, of UE data which pertain to 3GPP-defined reporting domains.

When subscribing to event exposure notifications for a particular Event ID, an NWDAF or Event Consumer AF goes through an authorisation procedure (see clause 5.8) with an Authorisation AS that determines the level of access the event subscriber is allowed to have by selecting one of the provisioned Data Access Profiles for the Event ID in question. If successful, the Authorisation AS supplies an access token to the subscriber which is presented to and validated by the Data Collection AF as part of the event subscription procedure.

NOTE: The procedure for selecting an appropriate Data Access Profile is not specified in the present document.

Figure 4.5.2-1 depicts the static data model for the data collection provisioning with Data Access Profiles to restrict data exposure access.



Figure 4.5.2-1: Data exposure restriction domain model

(SNIPPED)

NEXT CHANGE

### 4.5.2 Data exposure restriction model

The Provisioning AF restricts the exposure of UE data over reference points R5 and R6 by configuring a set of Data Access Profiles for each Event ID to be exposed. A Data Access Profile specifies a set of data processing operations that need to be performed by the Data Collection AF on the collected UE data in order to synthesize the event data that will be exposed to the NWDAF and/or Event Consumer AF.

NOTE: The UE data exposure restrictions specified in an instance of Data Access Profile to be followed by the Data Collection AF regarding permitted event data exposure to the NWDAF for a given Event ID should pertain only to the UE data specific to the ASP application (as identified by External Application Identifier). In other words, it should not be possible for the Data Access Profile to restrict exposure, to the NWDAF, of event information regarding UE data pertaining to 3GPP-defined reporting domains.

When subscribing to event exposure notifications for a particular Event ID, an NWDAF or Event Consumer AF goes through an authorisation procedure (see clause 5.8) with an Authorisation AS that determines the level of access the event subscriber is allowed to have by selecting one of the provisioned Data Access Profiles for the Event ID in question. If successful, the Authorisation AS supplies an access token to the subscriber which is presented to and validated by the Data Collection AF as part of the event subscription procedure.

NOTE: The procedure for selecting an appropriate Data Access Profile is not specified in the present document.

Figure 4.5.2-1 depicts the static data model for the data collection provisioning with Data Access Profiles to restrict data exposure access.



Figure 4.5.2-1: Data exposure restriction domain model

The Data Access Profile defines restrictions along the time, user, and location dimensions:

- Restrictions along the time dimension determine the granularity of access to UE data along the time axis. The finest granularity allows access to events as they take place in time. The coarsest level of access aggregates all event data along the time axis to produce a single aggregated value.

- Restrictions along the user dimension allow the Provisioning AF to restrict access to UE data related events based on groups. The finest granularity allows the event consumer to access events related to single users. Coarse granularity access exposes aggregated collected event data based on user groups. The coarsest granularity access exposes the data being aggregated for all users.

- Restrictions along the location dimension allow the Provisioning AF to restrict access to UE data related events based on the geographical location of the data collection client during the event. The finest granularity allows the event consumer to access events individually, irrespective of the location. Coarse granularity access exposes aggregated collected event data based on a geographical area. The coarsest level of access aggregates all event data along the location axis to produce a single aggregated value for all locations.

The baseline set of aggregation functions is listed in table 4.5.2‑1:

Table 4.5.2‑1: Baseline aggregation functions

|  |  |
| --- | --- |
| Aggregation function | Description |
| None | No aggregation is applied, and all reported data records are exposed as individual events. |
| Count | The number of reported data records is exposed to event consumers. |
| Mean | The mean average of the values in reported data records is exposed to event consumers. |
| Maximum | The maximal observed value in reported data records is exposed to event consumers. |
| Minimum | The minimal observed value in reported data records is exposed to event consumers. |
| Sum | The sum of the values in reported data records is exposed to event consumers. |

The authorization URL, if present in the data exposure restrictions, is used to redirect subscription requests without a valid access token to an authorization server, which will perform the authorization for the requested Data Access Profile.

Upon successful authorization, the consumer entity obtains an access token, which contains an identifier of the Data Access Profile that is allowed for the event consumer. Upon successful subscription, the Data Collection AF shall apply the indicated aggregation functions of the corresponding Data Access Profile along the time and user dimensions on the collected data prior to exposing it to the event consumer.

END OF CHANGES

1. In the event that provisioning data and subscription data contain similar rules, with the exception of event exposure to the NWDAF of UE data associated with 3GPP-defined reporting domains for which ASP-defined provisioning rules are more restrictive than those specified in event subscription from the NWDAF, the permissible information to be exposed by the Data Collection Function shall be governed by the rule with more restrictive semantics. [↑](#footnote-ref-1)