**3GPP TSG-S4 Meeting #117-eS4-220099**

**Online, 14th – 22nd February 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **PSEUDO CHANGE REQUEST** |
|  |
|  | **26.531** | **CR** |  | **rev** | **1** | **Current version:** | 1.0.1 |  |
|  |
| *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 |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | pCR on Procedures for Access Restriction – Stage 2 |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated |
| ***Source to TSG:*** | S4 |
|  |  |
| ***Work item code:*** | EVEX |  | ***Date:*** | 8th February 2021 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-17 |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Introduces the provisioning for access profiles. |
|  |  |
| ***Summary of change:*** |  |
|  |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** | 4.5, 4.6.1, 5.8 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  |  |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  |  |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  |  |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

|  |
| --- |
| **First Change** |

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

…

[9] 3GPP TS 23.501: "Security architecture and procedures for 5G System".

|  |
| --- |
| **Second Change** |

## 4.5 Information security model

### 4.5.1 Transport security

An encrypted data transfer protocol shall be employed at reference point R2 to protect the secrecy and integrity of collected UE data in transit between the Direct Data Collection Client and the Data Collection AF.

### 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.

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.

|  |
| --- |
| **Third Change** |

### 4.6.1 General

Figure 4.6.1‑1 depicts the static data model for the data collection and reporting domain. It is further described below.



Figure 4.6.1‑1: Static domain model

The *Provisioning AF* provisions zero or more sets of *provisioning information* in the Data Collection AF at reference point R1. The baseline set of information provisioned is described in clause 4.6.2. Each set of provisioning information pertains to one application, identified by its *external application identifier*, and one type of exposed *event*, uniquely identified in the 5G System by its *Event ID*, as defined in clause 4.15.1 of TS 23.502 [3]. There may be more than one set of provisioning information for a particular external application identifier, but the combination of the external application identifier and Event ID shall be unique for a given Data Collection AF instance.

The *data processing instructions* and *data exposure restrictions* are expressed as a set of Data Access Profiles (see clause 4.5.2). The data exposure restrictions limit the types of event consumer that are authorised to subscribe to the Event ID provisioned for the application and the data processing instructions specify aggregation functions that are applied to UE data prior to exposure to those event consumers.

Each set of provisioning information is manifested as a *data collection client configuration* that the Data Collection AF makes available to Direct Data Collection Client instances at reference point R2, to Indirect Data Collection Client instances at R3 and to AS instances at R4.

Once configured, these data collection clients then send *data reports* to the Data Collection AF associated with the data collection client configuration. Each data report provides the external application identifier associated with the UE Application and also includes a non-empty list of *data reporting records* containing the parameters collected by the data collection client. These parameters typically include a sampling timestamp.

NOTE: It is the responsibility of the data collection client to discover its external application identifier by means outside the scope of the present document.

Depending on the *data processing instructions* provisioned in the Data Collection AF, a data reporting record contributes to zero or more events exposed to subscribers at reference points R5 and/or R6. Conversely, an exposed event arises from one or more data reporting records. In the case of events synthesised by the Data Collection AF from multiple data reporting records, the timestamp of the event shall indicate when it was synthesised. Otherwise, the timestamp of the event shall be identical to the timestamp of the data reporting record from which it arose.

The Data Collection AF exposes a batch of recent events to consumers (the NWDAF and/or Event Consumer AF) as an *event exposure notification*.

|  |
| --- |
| **Fourth Change** |

## 5.8 Procedures for event consumer authorisation

The procedure for authorising access to the events exposed by the Data Collection AF is depicted by the following call flow:

Figure 5.8‑1: High-level procedures for event consumer authorisation

The steps are:

1. The Provisioning AF provisions the data collection and the report exposure functionality at reference point R1, per the procedures in clause 5.2, including a set of Data Access Profiles.

2. An event consumer sends a subscription request to the Data Collection AF to receive events via reference point R5 or R6, per the procedures in clause 5.3, indicating the Event ID of interest. The subscription request may nominate a specific Data Access Profile by citing its unique identifier.3. In return, the Data Collection AF redirects the event consumer to the Authorisation AS in order to obtain access based on the requested Data Access Profile.

4. The event consumer contacts the Authorisation AS (according to the procedures for authorization of NF service access defined in clause 13.4 of TS 33.501 [9]) with a set of valid credentials and optionally the requested Data Access Profile.5. If access is granted, the Authorisation AS responds with an access token that is valid for the authorised Data Access Profile for a specific period of time. The response may redirect the event consumer to the Data Collection AF using the initial subscription request URL, enhanced with the access token.

6. The event consumer resends the subscription request to the Data Collection AF, this time with the access token.

7. The Data Collection AF may verify the access token with the authorisation server, or it may verify it locally.

8. If verification is successful, the Data Collection AF approves the subscription request for the requested Access Profile

9. The Data Collection AF sends event notifications to the event consumer, per the procedures in clause 5.6.

10. The event consumer cancels its event subscription using the procedures in clause 5.7.