**3GPP TSG SA4 Meeting #116-e *S4-211448***

**E-meeting, November 10-19 2021**

|  |
| --- |
| *CR-Form-v12.0* |
| **PSEUDO CHANGE REQUEST** |
|  |
|  | **TS 26.531** | **CR** | **–** | **rev** |  | **Current version:** | **0.1.2** |  |
|  |
| *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 | **X** |

|  |
| --- |
|  |
| ***Title:***  | Support of direct/indirect reporting |
|  |  |
| ***Source to WG:*** | Huawei Technologies Co.,Ltd. |
| ***Source to TSG:*** | S4 |
|  |  |
| ***Work item code:*** | EVEX |  | ***Date:*** | 2021-10-22 |
|  |  |  |  |  |
| ***Category:*** | D |  | ***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). |  |
|  |  |
| ***Reason for change:*** | Currently, the direct and indirect data collection and reporting methods are supported for the general data collection and reporting architecture. However, whether to choose indirect or direct data reporting methods for UE data collection is still missing.  |
|  |  |
| ***Summary of change:*** | Add the details for choosing direct or indirect methods. |
|  |  |
| ***Consequences if not approved:*** | The data collection and reporting functionality cannot be complete.  |
|  |  |
| ***Clauses affected:*** | 4.2, 4.6.2 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  |  |
| ***affected:*** |  | **X** |  Test specifications |  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications |  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

First CHANGE

## 4.2 Functional entities for data collection and reporting

Editor’s Note: Different realisations of the reference are currently under consideration by SA4, including SEAL-based and CAPIF-based models.

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



NOTE: The Application Service Provider and/or the AS and/or the Data Collection AF may be deployed outside the trusted domain, in which case the services they expose 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

The functional entities illustrated in the figure are described as follows:

1. Data collection and reporting functionality is provisioned at reference point R1 by a *Provisioning AF* inside the *Application Service Provider* that may be deployed either inside or outside the trusted domain.

2. The *Data Collection AF* may be deployed inside or outside the trusted domain. It is responsible for managing the provisioning state for data collection and reporting. When its provisioning state changes, the Data Collection AF updates the set of available NF profile(s) in the NRF by invoking the Nnrf\_NFManagement service defined in clause 5.2.7.2 of TS 23.502 [3] according to the usage defined in clause 6.2.8.2.2 of TS 23.288 [4] and specified in clause 6.1 of TS 29.510 [6].

NOTE 1: If the Data Collection AF is deployed outside the trusted domain, this registration occurs via the NEF, as described in clause 6.2.2.3 of TS 23.288 [4].

Depending on the provisioning information provided by the Application Service Provider (see clause 4.6.2), the Data Collection AF provides a data collection and reporting configuration to the *Direct Data Collection Client* at reference point R2, to the *Indirect Data Collection Client* at reference point R3 or to Application Server (*AS*) instances at reference point R4, and receives data reports from them respectively at those same reference points.

The Data Collection AF processes received data reports according to processing instructions in its provisioning state. The processing activities include, but are not limited to, reporting format conversion, data normalisation, domain-specific anonymisation of data and (dis)aggregation of data into reports to be exposed as events.

Editor’s Note: Currently-defined 3GPP event types are specified in TS 23.502 and TS 23.288. Additional types of UE application level information available at the AF – for example content hosting logs, QoS and charging policy modification, network assistance and consumption reports as defined in TS 26.501 and TS 26.512 for 5G Media Streaming may also be deemed suitable as event exposure services for subscription by the NWDAF in performing related data analytics, based on further discussion with SA2.

Finally, the Data Collection AF is responsible for exposing processed UE data to event notification subscribers both inside the trusted domain (such as the NWDAF) and outside it (such as the *Event Consumer AF* in the Application Service Provider). In this role, the Data Collection AF realises the Event Exposure Service as defined in clause 6.2.2.1 of TS 23.288 [4] and as specified in TS 29.517 [5]. Subscribers fulfil the role of NF consumers of this service in the service-based architecture [2, 3].

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 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.

NOTE 2: When the Data Collection AF is deployed outside the trusted domain, the NWDAF uses the procedure defined in clause 5.2.6.2 of TS 23.502 [3] and further elaborated by clause 6.2.2.3 of TS 23.288 [4] to collect data from the externally deployed Data Collection AF via the NEF.

NOTE 3: The Data Collection AF is intended to be instantiated inside another Application Function in order to satisfy the domain-specific data collection and reporting requirements corresponding to particular features in the 5G System. As such, there may be several domain-specific Data Collection AF instances operating simultaneously in a particular 5G System, each one performing a different role. The definitions of these instantiations are beyond the scope of the present document.

3. The *Direct Data Collection Client* is responsible for collecting relevant data in the UE and for sending data reports to the Data Collection AF via reference point R2 using the Ndcaf\_DataReporting service according to a data collection and reporting configuration that it has previously obtained from the Data Collection AF.

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

NOTE 2: In the case where the Data Collection AF is deployed in a different trust domain than the UE, the Direct Data Collection Client instead invokes the equivalent Nnef\_DataReporting API via the NEF.

NOTE 3: The Direct Data Collection Client function is intended to be instantiated inside other UE functions in order to satisfy the domain-specific data collection and reporting requirements corresponding to particular features of the 5G System. As such, there may be several domain-specific Data Collection Client instances operating simultaneously on a given UE, each one performing a different role. One valid deployment option is to combine these instances in a common middleware component. Another option is to provide the Direct Data Collection Client as an integral part of each relevant UE Application. The definitions of these instantiations are beyond the scope of the present document. The realisation of these logical functions is implementation-dependent.

4. The *UE Application* is responsible for sharing relevant data with the Direct Data Collection Client via reference point R7. This may be achieved as a combination of application design, application configuration via R8 and/or application configuration via R7.

5. An Application Service Provider may also collect data from UE Applications via reference point R8 and employ an *Indirect Data Collection Client* subfunction to then send data reports to the Data Collection AF via reference point R3 by invoking the Ndcaf\_DataReporting service according to a data collection and reporting configuration that it has previously obtained from the Data Collection AF via reference point R3.

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

NOTE 2: In the case where the Application Service Provider server is deployed in a different trust domain than the Data Collection AF, the Indirect Data Collection Client instead invokes the equivalent Nnef\_DataReporting API via the NEF at reference point R3.

Editor’s Note: Need to check with SA2 about stage 2 definition of the Nnef\_DataReporting service (and possibly as follow-up with CT3 on corresponding stage 3 specification) which is currently absent in TS 23.502 [3] and TS 23.288 [4].

6. Application Server instances (labelled *AS*) inside or outside the trusted domain may also collect data and report it to the Data Collection AF via reference point R4 by invoking the Ndcaf\_DataReporting service, according to a data collection and reporting configuration previously obtained from the Data Collection AF via reference point R4.

Editor’s Note: Need to check with SA2 about stage 2 definition of the Nnef\_DataReporting service (and possibly as follow-up with CT3 on corresponding stage 3 specification) which is currently absent in TS 23.502 [3] and TS 23.288 [4].

NOTE 1: In the case where the Application Server is deployed in a different trust domain than the Data Collection AF, the AS instead invokes the equivalent Nnef\_DataReporting service via the NEF.

NOTE 2: The data collection and reporting requirements for such Application Servers are domain-specific and therefore beyond the scope of the present document.

7. The NWDAF is the primary consumer of processed UE data. This is exposed to the NWDAF by the Data Collection AF in the form of data reporting event notifications via reference point R5 using the Naf\_EventExposure service (as specified in TS 29.517 [5]) after any processing by the Data Collection AF has been performed according to its provisioned procesing instructions.

NOTE: If the Data Collection AF is deployed outside the trusted domain, this interaction occurs instead by invoking the Nnef\_EventExposure service via the NEF, as defined in clause 5.2.6.2 of TS 23.502 [3] and as further elaborated by clause 6.2.2.3 of TS 23.288 [4].

8. By means of appropriate data collection and reporting provisioning, certain UE data may also be exposed in the form of data reporting events by the Data Collection AF to an *Event Consumer AF* residing in the Application Service Provider via reference point R6 using the Naf\_EventExposure service defined in clause 5.2.19 of TS 23.502 [4] and specified in TS 29.517 [5].

NOTE: In the case where the Application Service Provider server is deployed outside the trusted domain, the Nnef\_EventExposure service, as defined in clause 5.2.6.2 of TS 23.502 [3], is invoked instead.

Second CHANGE

### 4.6.2 Provisioning information for data collection and reporting

A separate set of provisioning information shall be provided to the Data Collection AF at reference point R1 for each Event ID it is to expose. This provisioning information embodies the Service Level Agreement between the network operator and the Application Service Provider envisaged in clause 6.2.8.1 of TS 23.288 [4]. The provisioning information shall include at least the parameters defined in table 4.6.2‑1 below:

Table 4.6.2‑1: Baseline provisioning information for data collection and reporting

|  |  |  |
| --- | --- | --- |
| Parameter | Cardinality | Description |
| External Application Identifier | 1..1 | The identifier to be used in reports sent to the Data Collection AF by data collection and reporting clients. (This needs to be mapped to the Internal Application Identifier when exposing events to the NWDAF.) |
| Internal Application Identifier | 1..1 | The identifier to be used by event consumers (including the NWDAF and the Event Conumer AF) when subscribing to events in the Data Collection AF. |
| Event ID | 1..1 | The identifier of an AF event that will be exposed to event consumers as a result of the provisioning. |
| Data collection client type | 1..1 | The type of data collection client that will submit data reports to the Data Collection AF. |
| Valid targets | 1..1 | A parameter to control whether event consumers are permitted to filter events by External UE identifier or External Group Identifier when subscribing, instead of receiving events relating to all UEs. |
| Parameters to be collected | 1..\* | The subset of domain-specific parameters associated with the specified Event ID to be collected by the Data Collection AF (subject to user consent). |
| Data transformation recipe | 1..\* | A set of operations to be performed by the Data Collection AF on the parameters reported according to clause 4.6.4 prior to exposure as an event at a particular access level.The set of supported operations shall include at least: COUNT, MEAN, MEDIAN, MINIMUM, MAXIMUM and SUM.. |
| Data exposure restrictions | 1..\* | A set of restrictions on the exposure of the collected data after any data processing, each corresponding to a different access level. |

Third CHANGE

## 5.2 Procedures for data collection and reporting provisioning

Editor’s Note: High-level definition of how data collection and reporting is provisioned, including, but not limited to:

1. Access controls relating to user privacy protection and/or differential exposure of collected data in reports to different parties.

2. Manipulation of collected data for subsequent reporting (e.g. summarisation, anonymisation, etc.).



Figure 5.2‑1: High-level procedures for AF registration and provisioning phases

Initially, the different types of AF register themselves with the NRF using the Nnrf\_NFManagement\_NFRegister service operation defined in clause 5.2.7.2.2 of TS 23.502 [3]:

1. The NWDAF registers itself with the NRF.

2. The Data Collection AF registers itself with the NRF. This registration includes a list of Event IDs that it is capable of exposing to event consumers.

At some later point, Data Collection and Reporting features are provisioned by the Application Service Provider's Provisioning AF:

3. The Provisioning AF discovers the Data Collection AF by following the Nnrf\_NFDiscovery procedure defined in clause 5.2.7.3 of TS 23.502 [3].

4. The Provisioning AF provisions data collection and reporting in the Data Collection AF for a specific Event ID, using the Ndcaf\_DataReportingProvisioning procedures defined in the present document. For certain UE data, the Provisioning AF may need to decide the data reporting method, e.g. direct reporting or indirect reporting.

END OF CHANGES

1. In the event that provisioning data and subscription data contain similar rules, the permissible information to be exposed by the Data Collection Function shall be governed by the rule with more restrictive semantics. [↑](#footnote-ref-1)