**SA WG2 Meeting #137ES2-2001929**

**February 24 - 27, 2020 Electronic meeting (merged with** **S2-2002097)**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **23.503** | **CR** | **0408** | **rev** | **-** | **Current version:** | **16.3.0** |  |
|  |
| *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 |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Policy decisions based on Analytocs |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S2 |
|  |  |
| ***Work item code:*** | eNA |  | ***Date:*** | 2020-02-17 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-16 |
|  | *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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** |  There is no description of which Policy features may be impacted by the subscription to Analytics information from the NWDAF.  There are cross references between 23.288 and 23.503 that complicates undersanding how it works, and the reading of the TSs. |
|  |  |
| ***Summary of change:*** |  Replace references to 23.288 by explicit description when applicable, similar to the description of the BDT feature that may use analytics |
|  |  |
| ***Consequences if not approved:*** | Incomplete description of the feature for Policy decisions based on Analytics |
|  |  |
| ***Clauses affected:*** |  |
|  |  |
|  | **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*

#### 6.1.1.3 Policy decisions based on network analytics

Policy decisions based on network analytics allows PCF to perform policy decisions taking into account the analytics information provided by the NWDAF. The PCF subscribes/unsubscribes to Analytics information as defined in TS 23.288 [24].

The following Analyticd IDs are relevant for Policy decisions, “Load level information”, “Service Experience”, “Network Performance” and “Abnormal behaviour”. The PCF may subscribe to notifications of network analytics related to “Load Level Information” using the Nnwdaf\_AnalyticsSubscription\_Subscribe service operation including the Analytics ID " Load level information ", the Analytics Filter "S-NSSAI and NSI ID”." and the Analytics Reporting Information set to a load level threshold value, The PCF is notified when the load level of the Network Slice Instance reaches the threshold, and then verify if the RFSP index value needs to be modified for a SUPI for which a AM Policy Association is created, this is based on operator policies in the PCF, as defined in clause 6.1.2.1..

The PCF may subscribe to notifications of network analytics related to “Service Experience” using the Nnwdaf\_AnalyticsSubscription\_Subscribe service operation including the Analytics ID "Service Experience", the Target of Analytics Reporting “any UE” and the Analytics Filter one or more “Application ID(s)”, The PCF is notified on the Service Experience statistcs or predictions including for each Application Id including the list of SUPIs for which Service Experience is provided. In addition, both spatial and time validity may be provided as well as the confidence of the prediction. The PCF checks the 5QI values assigned to the Application, the number of UEs affected and use it as input to calculate the authorized QoS for a service data flow template.

The NWDAF service to retrieve the service experience (i.e. the average observed Service MoS) are described in clause 6.4 of TS 23.288 [24].

The PCF may subscribe to notifications of network analytics related to “Network Performance” using the Nnwdaf\_AnalyticsSubscription\_Subscribe service operation including the Analytics ID "Network Performance", the Target of Analytics Reporting “Internal Group Id” and the Analytics Filter including the Area of Interest, The PCF is notified on the Network Performance statistcs or predictions including the Aera of Interest and both the gNB status information and the predicted number of UEs in the Area of Interest. In addition, the confidence of the prediction may be provided. The PCF use this information as inout to calculate the BDT policies that are negotiated with the ASP, as defined in clause 6.1.2.4.

The NWDAF services to retrieve “Network Performance” as described in clause 6.6 of TS 23.288 [24].

The PCF may subscribe to notifications of network analytics related to “Abnormal behaviour” using the Nnwdaf\_AnalyticsSubscription\_Subscribe service operation including the Analytics ID " Abnormal behaviour ", the Target of Analytics Reporting “SUPI” or “Internal Group Id” and the Analytics Filter including the list of Exceptions IDs and per each Expception Id a possible threshold. The list of Exception IDs is listed in TS 23.288 including Unexpected UE location, the PCF may use it as input to determine the Service Area Restrictions defined in clause 6.1.2.1, suspicious DoS attack that the PCF may use to request the SMF to terminate the PDU session as defined in clause 6.1.3.6, wrong destination that is used to perform gating of a service data flow as defined in clause 6.1.3.6 and service data flow with long life time detected, that may be used to perform QoS related policies such as gating or policing as defined in clause 6.2.1.1.

The NWDAF services as] to retrieve the abnormal UE behaviour are described in clause 6.8 of TS 23.288 [24].

The PCF may also use the network analytics as input to its policy decision to apply operator defined actions for example for the UE context(s) or PDU session(s).

*Next Change*

### 6.2.1 Policy Control Function (PCF)

#### 6.2.1.1 General

The PCF provides the following session management related functionality:

- Policy and charging control for a service data flows;

- PDU Session related policy control;

- PDU Session event reporting to the AF.

The PCF provides authorized QoS for a service data flow.

The PCF uses the service information received from the AF (e.g. SDP information or other available application information) and/or the subscription information received from the UDR to calculate the proper QoS authorization (QoS class identifier, bitrates). The PCF may also take into account the requested QoS received from the SMF via N7 interface and the Analytics related to “Service Experience” received by NWDAF.

NOTE 1: The PCF provides always the maximum values for the authorized QoS even if the requested QoS is lower than what can be authorized.

The Authorization of QoS resources shall be based on complete service information unless the PCF is required to perform the authorization of QoS resources based on incomplete service information. The PCF shall after receiving the complete service information, update the affected PCC rules accordingly.

At reception of the service information from the AF, if configured through policy, the PCF determines the Maximum Packet Loss Rate for UL and DL based on the service information e.g. codec and sends it to SMF along with the PCC rule.

NOTE 2: Based on local configuration, the PCF sets the Maximum Packet Loss Rate (UL, DL) corresponding to either the most robust codec mode or the least robust codec mode of the negotiated set in each direction.

NOTE 3: Details for setting the Maximum Packet Loss Rate are specified by SA4.

The PCF supports usage monitoring control for a PDU Session or per Monitoring Key.

The PCF may receive information about total allowed usage per DNN and S-NSSAI combination and UE from the UDR, i.e. the overall amount of allowed resources (based either on traffic volume and/or traffic time) that are to be monitored for the PDN connections of a user. In addition, information about total allowed usage for Monitoring key(s) per DNN and S-NSSAI combination and UE may also be received from the UDR. For the purpose of usage monitoring per access type, the PCF receives an individual Monitoring key per access type from UDR.

For the purpose of usage monitoring control the PCF shall request the Usage report trigger and provide the necessary usage threshold(s), either volume threshold, time threshold, or both volume threshold and time threshold, upon which the requested node (SMF) shall report to the PCF. The PCF shall decide if and when to activate usage monitoring to the SMF.

The PCF may provide a Monitoring time to the SMF for the Monitoring keys(s) and optionally specify a subsequent threshold value for the usage after the Monitoring time.

If the SMF reports usage before the Monitoring time is reached, the Monitoring time is not retained by the SMF. Therefore, the PCF may again provide a Monitoring time and optionally the subsequent threshold value for the usage after the Monitoring time in the response.

It shall be possible for the PCF to request a usage report from the requested node (SMF).

NOTE 4: The PCF ensures that the number of requests/following policy decisions provided over N7 reference point do not cause excessive signalling load by e.g. assigning the same time for the report only for a preconfigured number of PDU sessions.

Once the PCF receives a usage report from the requested node (SMF) the PCF shall deduct the value of the usage report from the totally allowed usage for that DNN and S-NSSAI combination and UE (in case usage per PDU session is reported). If usage is reported from the SMF, the PCF shall deduct the value of the usage report from the totally allowed usage for individual Monitoring key(s) for that DNN and S-NSSAI combination and UE (in case of usage for one or several Monitoring keys is reported).

NOTE 5: The PCF maintains usage thresholds for each Monitoring key and PDU session that is active for a certain DNN and S-NSSAI combination and UE. Updating the total allowanced usage after the SMF reporting, minimizes the risk of exceeding the usage allowance.

If the SMF reports usage for a certain Monitoring key and if monitoring shall continue for that Monitoring key then the PCF shall provide new threshold value(s) in the response to the SMF respectively. If Monitoring time and subsequent threshold value are used then the PCF provides them to the SMF as well.

The PCF may provide a new volume threshold and/or a new time threshold to the SMF, the new threshold values overrides the existing threshold values in the SMF.

If monitoring shall no longer continue for that Monitoring key, then the PCF shall not provide a new threshold in the response to the SMF.

If all PDU session of a user to the same DNN and S-NSSAI combination is terminated, the PCF shall store the remaining allowed usage, i.e. the information about the remaining overall amount of resources, in the UDR.

The PCF may authorise an application service provider to request specific PCC decisions (e.g. authorisation to request sponsored IP flows, authorisation to request QoS resources) based on sponsored data connectivity profile from the UDR. For sponsored data connectivity, the PCF may receive a usage threshold from the AF. If the AF specifies a usage threshold, the PCF shall use the Sponsor Identity to construct a Monitoring key for monitoring the volume, time, or both volume and time of user plane traffic, and invoke usage monitoring on the SMF. The PCF shall notify the AF when the SMF reports that a usage threshold for the Monitoring key is reached provided that the AF requests to be notified for this event, as described in clause 6.1.3.18. If the usage threshold is reached, the AF may terminate the AF session or provide a new usage threshold to the PCF. Alternatively, the AF may allow the session to continue without specifying a usage threshold. If the AF decides to allow the session to continue without specifying a usage threshold, then monitoring in the SMF shall be discontinued for that monitoring key by the PCF, unless there are other reasons for continuing the monitoring.

If the H-PCF detects that the UE is accessing the sponsored data connectivity in the roaming scenario with home routed access, it may allow the sponsored data connectivity in the service authorization request, reject the service authorization request, or initiate the AF session termination based on home operator policy.

NOTE 6: Sponsored data connectivity is not supported in the roaming with visited access scenario in this Release.

If the AF revokes the service information and the AF has notified previously a usage threshold to the PCF, the PCF shall report the usage up to the time of the revocation of service authorization.

If the PDU session terminates and the AF has specified a usage threshold then the PCF shall notify the AF of the accumulated usage (i.e. either volume, or time, or both volume and time) of user plane traffic since the last usage report.

The PCF reports PDU Session events, e.g. Access Type, RAT Type (if applicable), Access Network Information, PLMN identifier where the UE is located, as described in clause 6.1.3.18.

The subscription and reporting of events when the target for reporting is an Internal Group Identifier or any UE accessing a combination of (DNN, S-NSSAI), is described in clause 5.2.5.7 of TS 23.502 [3]. The events that can be reported by the PCF are described in clause 6.1.3.18.

The subscription and reporting of events targeting an individual UE IP address (IPv4 address or IPv6 prefix) and optionally the DN information are described below. The events that can be reported by the PCF are described in clause 6.1.3.18.

The PCF may ensure that the sum of the packet filters used by all PCC rules which trigger the generation of signalled QoS rules does not exceed the number of supported packet filters for signalled QoS rules indicated by the UE for the PDU Session (as defined in clause 5.7.5.1 of TS 23.501 [2]).

For EPC IWK, when PCF receives from the SMF of the report on UE resumed from suspend state, the PCF may provision PCC Rules to the SMF to trigger an IP-CAN Session modification procedure.

The PCF may provide the IP index as the PDU session related policy to the SMF for IP address/Prefix allocation at SM Policy Association Establishment. If PCF receives from the SMF an allocated IP address/Prefix for the PDU session, it shall not include IP Index into the PDU session related policy. The PCF provides the following non-session management related functionality:

- Access and mobility related policy control (as described in clause 6.1.2.1);

- UE access selection and PDU Session selection related policy control (as described in clause 6.1.2.2);

- Negotiation for future background data transfer (as described in clause 6.1.2.4).

On receiving the DN Authorization Profile Index provided by the SMF at the establishment or modification of the SM Policy Association for a PDU session, the PCF takes the DN Authorization Profile Index as input for a policy decision and then obtains the list of PCC Rules (as defined in clause 6.3) and/or PDU Session related policy (as defined in clause 6.4) and provides them to the SMF as part of the Session Management Policy Control Data for enforcement.

On receiving the Session AMBR provided by the SMF at the establishment or modification of the SM Policy Association for a PDU session under the conditions defined in TS 23.501 [2] clause 5.6.6, the PCF provides the Authorized Session AMBR as part of the PDU session policy control information defined in clause 6.4.

*End of changes*