**3GPP TSG-CT3 Meeting #130C3-234225**

**Xiamen, China, 9 - 13 October, 2023 (Revision of C3-23xxxx)**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **29.512** | **CR** | **1143** | **rev** | **-** | **Current version:** | **18.3.0** |  |
|  |
| *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:***  | Remove the EN for PCC rule generation |
|  |  |
| ***Source to WG:*** | Huawei |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | eUEPO |  | ***Date:*** | 2023-09-20 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** |  Rel-18 |
|  | *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:*** | It is agreed in S2-2308254, PCC rule generation based on pre-configured URSP rules may be not enough to restrict the transmission of unexpected traffic to occur, as preconfigured URSP rules can be just subset of provisioned URSP rules for the UE. To avoid the potential inconsistence issue, it would be more proper to let the PCF for the PDU Session to generate PCC rules under consideration of the traffic descriptor correponding to the UE reported Connection Capabilities or the URSP rules which has been sent to the UE. Of course, the PCF for the PDU Session just needs to retrive the URSP related to the RSD of the PDU Session. |
|  |  |
| ***Summary of change:*** | Make an alignment with stage 2. |
|  |  |
| ***Consequences if not approved:*** | Open issue is not resolved. |
|  |  |
| ***Clauses affected:*** | 4.2.2.2, 4.2.4.2 |
|  |  |
|  | **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:*** | The CR doesn’t impact the OpenAPI file. |
|  |  |
| ***This CR's revision history:*** |  |

**Additional discussion(if needed):**

**Proposed changes:**

\*\*\* First Change \*\*\*

#### 4.2.2.2 SM Policy Association establishment



Figure 4.2.2.2-1: SM Policy Association establishment

When the NF service consumer receives the Nsmf\_PDUSession\_CreateSMContext Request as defined in clause 5.2.2.2 of 3GPP TS 29.502 [22], if the NF service consumer was requested not to interact with the PCF, the NF service consumer shall not interact with the PCF. Otherwise, the NF service consumer shall send an HTTP POST request to the PCF to create an "Individual SM Policy" resource as described in step 1 of figure 4.2.2.2-1.

NOTE 1: The decision to not interact with the PCF applies for the entire lifetime of the PDU session.

NOTE 2: The indicator to not interact with the PCF is configured in the UDM. It is delivered by the UDM to the NF service consumer within the Charging Characteristics using the Session Management Subscription Data Retrieval service operation as described in 3GPP TS 29.503 [34]. The indicator is operator specific, therefore it can only be used in non-roaming and home routed roaming cases.

The NF service consumer shall include the "SmPolicyContextData" data structure in the payload body of the HTTP POST request in order to request the creation of a representation of the "Individual SM Policy" resource as described below.

The NF service consumer shall include (if available) in the "SmPolicyContextData" data structure:

- SUPI of the user within the "supi" attribute;

- PDU Session Id within the "pduSessionId" attribute;

- DNN within the "dnn" attribute;

- DNN selection mode within the "dnnSelMode" attribute, if the "DNNSelectionMode" feature is supported;

- URL identifying the recipient of SM policies update notifications within the "notificationUri" attribute;

- PDU Session Type within the "pduSessionType" attribute;

- PEI within the "pei" attribute;

- Internal Group Id(s) within the "interGrpIds" attribute;

- type of access within the "accessType" attribute;

- type of the radio access technology within the "ratType" attribute;

- the combination of additional access type and RAT type within the "addAccessInfo" attribute, if the ATSSS feature is supported;

- the UE Ipv4 address within the "ipv4Address" attribute and/or the UE Ipv6 prefix within the "ipv6AddressPrefix" attribute;

- the UE time zone information within the "ueTimeZone" attribute;

- the UDM subscribed Session-AMBR or, if the "DN-Authorization" feature is supported, the DN-AAA authorized Session-AMBR within the "subsSessAmbr" attribute;

NOTE 3: When both, the UDM subscribed Session-AMBR and the DN-AAA authorized Session-AMBR are available in the NF service consumer, the NF service consumer includes the DN-AAA authorized Session-AMBR.

- if the "VPLMN-QoS-Control" feature is supported, the highest Session-AMBR and the default QoS supported in the VPLMN within the "vplmnQos" attribute, if available;

NOTE 4: In home routed roaming, the H-SMF may provide the QoS constraints received from the VPLMN (defined in 3GPP TS 23.502 [3] clause 4.3.2.2.2) to the PCF.

- the DN-AAA authorization profile index within the "authProfIndex" attribute, if the "DN-Authorization" feature is supported;

- subscribed Default QoS Information within the "subsDefQos" attribute;

- the number of supported packet filters for signalled QoS rules within the "numOfPackFilter" attribute;

- the online charging status within the "online" attribute;

- the offline charging status within the "offline" attribute;

- the charging characteristics within the "chargingCharacteristics" attribute;

- the access network charging identifier within the "accNetChId" attribute;

- the address of the network entity performing charging within the "chargEntityAddr" attribute;

- the 3GPP PS data off status within the "3gppPsDataOffStatus" attribute, if the "3GPP-PS-Data-Off" feature is supported;

- indication of UE support of reflective QoS within the "refQosIndication" attribute;

- user location(s) information within the "userLocationInfo" attribute;

NOTE 5: The SMF encodes both 3GPP and non-3GPP access UE location in the "userLocationInfo" attribute when they are both received from the AMF.

- the S-NSSAI corresponding to the network slice to which the PDU session is allocated within the "sliceInfo" attribute;

- the required QoS flow usage for the default QoS flow within the "qosFlowUsage" attribute;

- the MA PDU session indication within the "maPduInd" attribute, if the "ATSSS" feature is supported;

- the ATSSS capability within the "atsssCapab" attribute, if the "ATSSS" feature is supported;

- the identifier of the serving network (the PLMN Identifier or the SNPN Identifier) within the "servingNetwork" attribute;

NOTE 6: The SNPN Identifier consists of the PLMN Identifier and the NID.

- one or more framed routes within the "ipv4FrameRouteList" attribute for IPv4 and/or one or more framed routes within the "ipv6FrameRouteList" attribute;

NOTE 7: When both, the UDM subscribed framed routes and the DN-AAA authorized framed routes are available in the NF service consumer, the NF service consumer includes the DN-AAA authorized framed routes. If the UDM or DN-AAA updates the framed routes during the lifetime of the PDU Session, the NF service consumer releases the PDU Session as defined in clause 4.2.5.2.

- the serving network function identifier within the "servNfId" attribute;

- when the "PvsSupport" feature is supported, the onboarding indication within the "onboardInd" attribute and the Provisioning Server address(es) within the "pvsInfo" attribute;

- when the "SatBackhaulCategoryChg" or "EnSatBackhaulCatChg" feature is supported, the satellite backhaul category within the "satBackhaulCategory" attribute;

NOTE 8: When the "satBackhaulCategory" attribute is not present, non-satellite backhaul applies.

- when the "AMInfluence" feature is supported, the PCF for the UE callback URI and, if received, SBA binding information within the "pcfUeInfo" attribute;

- when the "URSPEnforcement" feature is supported, the URSP rule enforcement information provided by the UE within the "urspEnfInfo" attribute. In this case, the NF service consumer shall also include the SSC mode within the "sscMode" attribute, the UE requested DNN (if available and different from the selected DNN) within the "ueReqDnn" attribute, and if the PDU session is redundant, the RSN and the PDU session pair ID within the "redundantPduSessionInfo" attribute;

- trace control and configuration parameters information within the "traceReq" attribute;

- when the "EneNA" feature is supported, the list of NWDAF instance IDs used for the PDU Session within the "nwdafInstanceId" and their associated Analytic ID(s) within "nwdafEvents" consumed by the NF service consumer, included within the "nwdafDatas" attribute; and

- for HR-SBO scenario, if the "HR-SBO" feature is supported, the HR-SBO support indication within the "hrsboInd" attribute in the SM policy association.

NOTE 9: VPLMN Specific Offloading Policy can be provisioned in HPLMN per each VPLMN based on the service level agreement between HPLMN and VPLMN.

The NF service consumer may include in the "SmPolicyContextData" data structure the IPv4 address domain identity within the "ipDomain" attribute.

NOTE 10: The "ipDomain" attribute is helpful when within a network slice, there are several separate IP address domains, with SMF/UPF(s) that allocate Ipv4 IP addresses out of the same private address range to UE PDU Sessions. The same IP address can thus be allocated to UE PDU sessions served by SMF/UPFs in different IPv4 address domains. If one PCF controls several SMF/UPFs in different IP address domains, the UE IP address is thus not sufficient for the AF session binding procedure, as described in 3GPP TS 29.514 [17]. The SMF assists the PCF in the session binding supplying an "ipDomain" attribute denoting the IPv4 address domain identity of the allocated UE IPv4 address.

When the PCF receives the HTTP POST request from the NF service consumer, the PCF shall make a policy authorization based on the information received from the NF service consumer and, if available, information received from the AMF, the CHF, the AF, the UDR and/or the NWDAF and operator policies pre-configured at the PCF. If the policy authorization is successful, the PCF shall create a new resource, which represents a new "Individual SM Policy" instance, addressed by a URI as defined in clause 5.3.3.2 and containing a PCF created resource identifier. The PCF shall respond to the NF service consumer with an HTTP 201 Created response, including:

- a Location header field containing the URI of the created resource; and

- a response body providing the session management related policies, e.g. provisioning of PCC rules as defined in clause 4.2.6.2, provisioning of policy control request triggers as defined in clause 4.2.6.4.

The NF service consumer shall use the URI received in the Location header in subsequent requests to the PCF to refer to the created "Individual SM Policy" resource.

If the PCF received the list of NWDAF instance IDs used for the PDU Session in "nwdafInstanceId" attribute and their associated Analytic IDs in "nwdafEvents" attribute included within the "nwdafDatas" attribute the PCF may select those NWDAF instances as described in 3GPP TS 29.513 [7].

If the "URSPEnforcement" feature is supported and the PCF received the URSP rule enforcement information from the SMF, the PCF may generate PCC rules under consideration of the traffic descriptor corresponding to the URSP rules which has been sent to the UE.

It the PCF received a "traceReq" attribute in the HTTP POST request from the SMF, it shall perform trace procedures as defined in 3GPP TS 32.422 [24].

If errors occur when processing the HTTP POST request, the PCF shall apply the error handling procedures specified in clause 5.7.

If the user information received within the "supi" attribute is unknown, the PCF shall reject the request with an HTTP "400 Bad Request" response message including the "cause" attribute of the ProblemDetails data structure set to "USER\_UNKNOWN".

If the PCF is not able, due to incomplete, erroneous or missing information (e.g. QoS, RAT type, subscriber information), to provision a policy decision as response to the request for PCC rules from the NF service consumer, the PCF may reject the request with an HTTP "400 Bad Request" response message including the "cause" attribute of the ProblemDetails data structure set to "ERROR\_INITIAL\_PARAMETERS".

If the NF service consumer receives an HTTP response with the above error codes, the NF service consumer shall reject the PDU session establishment procedure that initiated the HTTP POST Request.

If the PCF, based on local configuration and/or operator policies, denies the creation of the Individual SM Policy resource, the PCF may reject the request with in an HTTP "403 Forbidden" response message including the "cause" attribute of the ProblemDetails data structure set to "POLICY\_CONTEXT\_DENIED". At reception of this error code and based on configured failure actions, the NF service consumer may reject or allow, by applying local policies, the PDU session establishment.

If the "SamePcf" feature as defined in clause 5.8 is supported, when the PCF determines that the same PCF shall be selected for the SM Policy associations to the same UE ID, S-NSSAI and DNN combination in the non-roaming or home-routed scenario and there is no SM Policy association for the UE ID, S-NSSAI and DNN combination, the PCF, after determining whether the BSF supports the "SamePcf" or the "ExtendedSamePcf" feature as described in 3GPP TS 29.521 [39], shall request the BSF to check if there is an existing PCF binding information for the same UE ID, S-NSSAI and DNN combination registered by other PCF(s) as defined in clause 4.2.2.2 of 3GPP TS 29.521 [39]. If the PCF receives the from the BSF "403 Forbidden" status code with the "cause" attribute of the ProblemDetails data structure set to "EXISTING\_BINDING\_INFO\_FOUND" and the FQDN or description of IP endpoints of the Npcf\_SMPolicyControl service of the existing PCF (i.e. that handles SM Policy association(s) to the same UE ID, S-NSSAI and DNN combination) within the "pcfSmFqdn" attribute or the "pcfSmIpEndPoints" attribute of the BindingResp data structure respectively as defined in clause 4.2.2.2 of 3GPP TS 29.521 [39], the PCF shall reply to the SMF with an HTTP "308 Permanent Redirect" error response and the Location header containing a URI as defined in clause 5.3.2.2, with the FQDN or IP endpoint of this PCF's Npcf\_SMPolicyControl service as {apiRoot}. Upon reception of the response, the NF service consumer shall initiate a new HTTP POST request based on the returned URI.

The forwarding of the Origination Time Stamp parameter shall apply as described hereafter, if the NF service consumer supports the detection and handling of late arriving requests as specified in clause 5.2.3.3 of 3GPP TS 29.502 [22] and the procedure is enabled by the operator. If the NF service consumer receives a request to create an SM Context or a PDU session context, which includes the 3gpp-Sbi-Origination-Timestamp header as defined in clause 5.2.3.2, the NF service consumer shall forward this header to the PCF as HTTP custom header. See also clause 4.2.7 for the handling at the PCF, when the PCF receives the 3gpp-Sbi-Origination-Timestamp header.

\*\*\* Next Change \*\*\*

#### 4.2.4.2 Requesting the update of the Session Management related policies



Figure 4.2.4.2-1: Requesting the update of the Session Management related policies

When the NF service consumer detects that one or more policy control request triggers are met, the NF service consumer shall send a POST request to the PCF to update an Individual SM Policy resource. The {smPolicyId} in the URI identifies the Individual SM Policy resource to be updated. The NF service consumer include SmPolicyUpdateContextData data structure in the payload body of the HTTP POST to request a update of representation of the "Individual SM Policy" resource. The NF service consumer shall include the met policy control request trigger(s) within the "repPolicyCtrlReqTriggers" attribute and applicable updated value(s) in the corresponding attribute(s).

The NF service consumer shall include (if the corresponding policy control request trigger is met and the applicable information is available) in SmPolicyUpdateContextData data structure:

- type of access within the "accessType" attribute;

- type of the radio access technology within the "ratType" attribute;

- the new allocated UE Ipv4 address within the "ipv4Address" attribute and/or the UE Ipv6 prefix within the "ipv6AddressPrefix" attribute;

- an additional new allocated UE Ipv6 prefix within the "addIpv6AddrPrefixes" attribute, if the "MultiIpv6AddrPrefix" feature is supported;

- multiple new allocated UE Ipv6 prefixes within the "multiIpv6Prefixes" attribute, if the "UnlimitedMultiIpv6Prefix" feature is supported;

- the released UE Ipv4 address within the "relIpv4Address" attribute and/or the UE Ipv6 prefix within the "relIpv6AddressPrefix" attribute;

- an additional released UE Ipv6 prefix within the "addRelIpv6AddrPrefixes" attribute, if the "MultiIpv6AddrPrefix feature" is supported;

- multiple released UE Ipv6 prefixes within the "multiRelIpv6Prefixes" attribute, if the "UnlimitedMultiIpv6Prefix feature" is supported;

- the UE MAC address within the "ueMac" attribute;

- the released UE MAC address within the "relUeMac" attribute;

- the indication of UE supporting reflective QoS within the "refQosIndication" attribute;

- access network charging identifier within the "accNetChIds" attribute;

- the 3GPP PS data off status within the "3gppPsDataOffStatus" attribute, if the "3GPP-PS-Data-Off" feature is supported;

- the UE time zone information within the "ueTimeZone" attribute;

- the UDM subscribed Session-AMBR or, if the "DN-Authorization" feature is supported, the DN-AAA authorized Session-AMBR within the "subsSessAmbr" attribute;

NOTE 1: When both, the UDM subscribed Session-AMBR and the DN-AAA authorized Session-AMBR are available in the NF service consumer, the NF service consumer includes the DN-AAA authorized Session-AMBR.

- if the "VPLMN-QoS-Control" feature is supported, the highest Session-AMBR and the default QoS supported in the VPLMN within the "vplmnQos" attribute, if available;

NOTE 2: In home routed roaming, the H-SMF may provide the QoS constraints received from the VPLMN (defined in 3GPP TS 23.502 [3] clause 4.3.2.2.2) to the PCF.

- if the "DN-Authorization" feature is supported, the DN-AAA authorization profile index within the "authProfIndex" attribute;

- subscribed Default QoS Information within the "subsDefQos" attribute;

- detected application information within the "appDetectionInfos" attribute;

- if the "UMC" feature is supported, the accumulated usage reports within the "accuUsageReports" attribute;

- if the "PRA" feature is supported, the reported presence reporting area information within the "repPraInfos" attribute;

- the QoS flow usage required of the default QoS flow within the "qosFlowUsage" attribute;

- indication whether the QoS targets of one or more SDFs are not guaranteed or guaranteed again within the "qncReports" attribute;

- user location(s) information within the "userLocationInfo" attribute;

NOTE 3: The SMF encodes both 3GPP and non-3GPP access UE location in the "userLocationInfo" attribute when they are both received from the AMF.

- if the "GroupIdListChange" feature is supported, the Internal Group Identifier(s) of the served UE within the "interGrpIds " attribute;

- if the "SatBackhaulCategoryChg" or "EnSatBackhaulCatChg" feature is supported, the satellite backhaul category or non-satellite backhaul within the "satBackhaulCategory" attribute;

- if the "AMInfluence" feature is supported, the PCF for the UE callback URI and, if received, SBA binding information within the "pcfUeInfo" attribute;

- serving network function identifier within the "servNfId" attribute;

- identifier of the serving network within the "servingNetwork" attribute;

- when the "URSPEnforcement" feature is supported, the URSP rule enforcement information provided by the UE within the "urspEnfInfo" attribute. In this case, the NF service consumer shall also include, if they were not previously provided, the SSC mode within the "sscMode" attribute, the UE requested DNN (if available and different from the selected DNN) within the "ueReqDnn" attribute, and/or if the PDU session is redundant, the RSN and the PDU session pair ID within the "redundantPduSessionInfo" attribute. The NF service consumer shall also provide the "accessType" attribute, if changed compared to the latest reported value;

- if the "EnTSCAC" feature is supported, the BAT offset and the optionally adjusted periodicity within the "batOffsetInfo" attribute;

- when the "EneNA" feature is supported, the list of NWDAF instance IDs used for the PDU Session within the "nwdafInstanceId" and their associated Analytic ID(s) within "nwdafEvents" updated with the new values included within the "nwdafDatas" attribute;

NOTE 4: The NF service consumer provides the complete updated list of NWDAF instance IDs and associated Analytic ID(s) used for the PDU session. If all NWDAF data is deleted an empty list is included.

- for HR-SBO scenario, if the "HR-SBO" feature is supported, the H-SMF may include the HR-SBO support indication within the "hrsboInd" attribute; and

NOTE 5: The "PLMN\_CH" trigger has to be provisioned in order to report this information.

- if the"NetSliceRepl" feature is supported, the alternate S-NSSAI used to replace the existing S-NSSAI for the PDU Session within the "sliceInfo" attribute.

The NF service consumer may include in "SmPolicyUpdateContextData" data structure the IPv4 address domain identity within the "ipDomain" attribute.

In case of a successful update, "200 OK" response shall be returned. The PCF shall include in the "200 OK" response the representation of the updated policies within the SmPolicyDecision data structure. Detailed procedures related to the provisioning and enforcement of the policy decisions within the SmPolicyDecision data structure are contained in clause 4.2.6.

NOTE 5: An empty SmPolicyDecision data structure is included in the "200 OK" response when the PCF decides not to update policies.

If the PCF received a new list of NWDAF instance IDs used for the PDU Session in "nwdafInstanceId" attribute and their associated Analytic IDs in "nwdafEvents" attribute included within the "nwdafDatas" attribute the PCF may select those NWDAF instances based on this new list as described in 3GPP TS 29.513 [7].

If the "URSPEnforcement" feature is supported and the PCF received the URSP rule enforcement information from the SMF, the PCF may generate PCC rules under consideration of the traffic descriptor corresponding to the URSP rules which has been sent to the UE.

If errors occur when processing the HTTP POST request, the PCF shall send an HTTP error response as specified in clause 5.7.

If the feature "ES3XX" is supported, and the PCF determines the received HTTP POST request needs to be redirected, the PCF shall send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [4].

If the PCF is, due to incomplete, erroneous or missing information (e.g. QoS, RAT type, subscriber information) not able to provision a policy decision as response to the request for PCC rules by the NF service consumer, the PCF may reject the request and include in an HTTP "400 Bad Request " response message the "cause" attribute of the ProblemDetails data structure set to "ERROR\_INITIAL\_PARAMETERS".

If the PCF receives the set of session information which is sent in the message originated due to a trigger being met is incoherent with the previous set of session information for the same session (E.g. trigger met was RAT changed, and the RAT notified is the same as before), the PCF may reject the request and include in an HTTP "400 Bad Request" response message the "cause" attribute of the ProblemDetails data structure set to "ERROR\_TRIGGER\_EVENT".

If the PCF detects that the packet filters in the request for new PCC rules received from the NF service consumer is covered by the packet filters of outstanding PCC rules that the PCF is provisioning to the NF service consumer, the PCF may reject the request and include in an HTTP "403 Forbidden" response message the "cause" attribute of the ProblemDetails data structure set to "ERROR\_CONFLICTING\_REQUEST".

If the PCF does not accept one or more of the traffic mapping filters provided by the NF service consumer in an HTTP POST request (e.g. because the PCF does not allow the UE to request enhanced QoS for services not known to the PCF), the PCF shall reject the request and include in an HTTP "403 Forbidden" response message the "cause" attribute of the ProblemDetails data structure set to "ERROR\_TRAFFIC\_MAPPING\_INFO\_REJECTED".

If the NF service consumer receives HTTP response with these codes, the NF service consumer shall reject the PDU session modification that initiated the HTTP Request.

The PCF shall not combine a rejection with provisioning of PCC rule operations in the same HTTP response message.

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