Specification Compliance - N7 and N28

- Feature Summary and Revision History, on page 1
- Feature Description, on page 2
- Configuration Support for the N7 and N28 Interface, on page 3

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	PCF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
Enhancement introduced. With this release, various service configurations are added and enhanced for compliance with the 3GPP December 2018 specification. The procedures to configure use case initiators and retrievers are also added.	2020.01.0
First introduced.	Pre 2020.01.0

Feature Description

PCF complies to the 3GPP December 2018 specification by supporting the N7 and N28 interfaces.

Relationships

The SMF should comply to 3GPP December 2018 specification so that PCF can apply the dedicated bearer rules to SMF.

Components

The following components are involved when PCF is configured to work with the N7 and N28 interface.

- N15 Interface
- N28 Interface
- N7 Interface
- N5 Interface

N15 Interface

The N15 interface complies with *3GPP TS 29.507 Release 15* specification.

N28 Interface

The N28 interface complies with the 3GPP December 2018 specification. Hence, no compliance changes are required on the N28 interface for this feature.

N7 Interface

The pcf-rest-ep and pcf-engine comply with the 3GPP December 2018 specification.

N5 Interface

The pcf-rest-ep and pcf-engine comply with the 3GPP December 2020 specification.

Rx Interface

With the N7 interface being 3GPP December 2018 specification compliant, PCF supports the notification of rule status of the dedicated bearer rules. You can configure this support with the new "ruleReports" parameter, which is sent in the SmPolicyUpdateRequest message. This parameter consists of the report of rule status as successful or failed.

When IMS initiates multimedia calls, PCF installs the dedicated bearer rules on the SMF nodes. SMF enforces these rules and provides the status of these rules to PCF in the ruleReports parameter.

Following are some of the subparameters of the ruleReports parameter that the feature supports:

- Array of pccRuleIds

- Rule Status
- Failure Code

The N5 (Rx) interface works in the following way:

- If the AAR message on the N5 interface receives the “INDICATION_OF_SUCCESSFUL_RESOURCES_ALLOCATION (8)” action, PCF sends the “SUCC_RES_ALLO” event trigger to SMF in the SmPolicyUpdateNotify message.
- SMF sends the status report in the SmPolicyUpdateRequest message. When PCF sends the “SUCC_RES_ALLO” event trigger, ruleReports parameter consists of the rules with the Rule Status as Active. Rule Status value can either be “Active” or “Inactive”. PCF sends these rule reports through Rx_RAR toward AF.
- The ruleReports parameter also consists of “Inactive” rules along with their Failure Status. If some rules are Inactive, PCF sends the failure report of these in Rx_RAR to AF. If all the rules are Inactive, PCF sends the failure report of these rules in Rx_ASR to AF.

Note PCF sends the failure report to AF if the Rx session has already requested the "INDICATION_OF_FAILED_RESOURCES_ALLOCATION(9)" specific action in AAR.

- PCF handles reporting of both Active and Inactive rule status in the same ruleReports along with the “SUCC_RES_ALLO” event trigger.
- If multiple Inactive rules exist under ruleReports with multiple failureCode, then all the rules are mapped to only single Specific-Action. Then, PCF sends these rules in the Rx_RAR (or abort-cause for Rx_ASR).

Configuration Support for the N7 and N28 Interface

This section describes how to configure the N7 and N28 interface by configuring the following services:

- SessionRule
- SessionRuleAction
- SessionRuleConditionData
- QosData
- TableDrivenQosDecision
- TableDrivenDynamicPccRule
- Use Case Initiators
- Retrievers

SessionRule

This section describes how to configure SessionRule Service.

The SessionRule service configuration consists of policy information elements that are associated with a PDU session. The object configures the QoS attributes for the default bearer.

Before setting the service parameters, ensure that you create a use case template and add a service for this configuration. For details, see Configuring the Use Case Template and Adding a Service.

To configure the SessionRule service, use the following configuration:

1. Log in to Policy Builder.
2. Click the **Services** tab.
3. Configure the following parameters:
   a. From the **Use Case Template** pane, select the N7 service configuration object.
   b. From the **Service Configurations** pane, select **SessionRule**.
   c. Click **Add**.
4. From the N7 service configuration, click **SessionRule**.

   The service configuration parameters appear in the right pane.
5. Configure one or more of the following **SessionRule** parameters:
   - **Sess Rule Id**: Enter a unique value to identify the session rule within a PDU session.
   - **Uplink**: This parameter is the Aggregate Maximum Bit Rate (AMBR) for the uplink frequency. Configure the value of this parameter in BitRate.
   - **Downlink**: This parameter is the AMBR for the downlink frequency. Configure the value of this parameter in BitRate.
   - **5qi**: This 5G QoS Identifier identifies a specific QoS forwarding behavior for a 5G QoS flow. Configure a numeric value for this parameter.
   - **Arp**: Configure the following Allocation Retention Priority levels:
     - **Priority Level**: Configure this parameter to define the relative importance of a resource request.
     - **Preempt Cap**: Configure this parameter to define a service data flow to reassign the resources. These resources are already assigned to another service data flow with a lower priority level.
     - **Preempt Vuln**: Configure this parameter to define a service data flow to lose the assigned resources for admitting a service data flow with a higher priority level.
   - **Priority Level**: Configure this parameter to indicate the 5QI priority level. Enter a value from 1 through 127, where 1 implies the highest level, and 127 implies the lowest level.
   - **Aver Window**: Configure this parameter to indicate the Averaging Window, which is in milliseconds. Enter a value from 1 through 4095, where 1 implies the minimum averaging level and 4095 implies the maximum averaging level.

- **Max Data Burst Vol**: Configure this parameter to indicate the Maximum Data Burst Volume, which is in bytes. Enter a value from 1 through 4095, where 1 implies the minimum data burst volume and 4095 implies the maximum data burst volume.

6. Click **Add**.

SessionRuleAction

This section describes how to configure the SessionRuleAction service.

The SessionRuleAction service configures the values for the various SessionRuleAction attributes that are based on Policy or the configured SessionRule.

Before setting the service parameters, ensure that you create a use case template and add a service for this configuration. For details, see Configuring the Use Case Template and Adding a Service.

To configure the SessionRuleAction service parameters, use the following configuration:

1. Log in to Policy Builder.
2. Click the **Services** tab.
3. Configure the following parameters:
   a. From the **Use Case Template** pane, select the N7 service configuration object.
   b. From the **Service Configurations** pane, select **SessionRuleAction**.
   c. Click **Add**.

   The **Select Service Configuration** window appears.
4. From the N7 service configuration, click **SessionRuleAction**.

   The service configuration parameters appear in the right pane.
5. For all the parameters of **SessionRuleAction** service, configure one of the following options:
   - **Mirror**: The value that is requested on the N7 interface is granted.
   - **Enforce**: The default bearer QoS value is granted. Enforce is the default value.
   - **Bound**: The minimum value between the configured value, and the requested value is granted and is sent back as a response.
6. Click **Add**.

SessionRuleConditionData

This section describes how to configure the SessionRuleConditionData service.

The PCF schema lets you set a threshold for an active SessionRules service by configuring the SessionRuleConditionData service. The value that you define in this service configuration indicates the period for which the SessionRules service remains active. After the set period is complete, the SessionRules service is deactivated. The SessionRuleConditionData service includes the Extend Deactivation parameter. If you have configured the Extend Deactivation parameter and an event occurs within the configured interval, then

PCF extends the waiting period. For example, if the deactivation time is set to 2 hours, and an event occurs after 1 hour, then the activation time is extended by 2 hours from the time the event happened. The service remains active for 3 hours.

Before setting the service parameters, ensure that you create a use case template and add a service for this configuration. For details, see Configuring the Use Case Template and Adding a Service.

To configure the SessionRuleConditionData service parameters, use the following configuration:

1. Log in to Policy Builder.
2. Click the **Services** tab.
3. From the **Use Case Template** pane, select the N7 service configuration object.
4. From the **Service Configurations** pane, select **SessionRuleConditionData**, and click **Add**.

   The **Select Service Configuration** window appears.
5. From the N7 service configuration, click **SessionRuleConditionData**.

   The service configuration parameters appear in the right pane.
6. Configure one or more of the following **SessionRuleConditionData** parameters:
   - **Priority**: Enter an integer value to indicate the priority of the service configuration object. This value is considered in case multiple service initiator conditions match.
   - **Deactivation Time (In Minutes)**: Specify the time in minutes after which the SessionRule service is deactivated.
   - **Deactivation Time (In Hours)**: Enter the time in hours after which the SessionRule service is deactivated.
   - **Deactivation Time (In Seconds)**: Specify the time in seconds after which the SessionRule service is deactivated.

Note PCF aggregates the values that you specify in hours, minutes, and seconds to determine the deactivation time.

   - **Extend Deactivation**: If set to true, then PCF extends the SessionRule service deactivation time for the period that you have specified for deactivation.

QosData

This section describes how to configure the QosData Service.

The QosData Service configuration is updated with the parameters to meet the 3GPP December 2018 specification compliance.

Before setting the service parameters, ensure that you create a use case template and add a service for this configuration. For details, see Configuring the Use Case Template and Adding a Service.

To configure the QosData service from Policy Builder, use the following configuration:

1. Log in to Policy Builder.

2. Click the **Services** tab.
3. Configure the following parameters:
   a. From the **Use Case Template** pane, select the N7 service configuration object.
   b. From the **Service Configurations** pane, select **QosData**.
   c. Click **Add**.
4. From the N7 service configuration, click **QosData**.

   The **Select Service Configuration** window appears.
5. Configure one or more of the following **QosData** parameters:
   - **Qnc**: Enter a boolean value for this parameter. This parameter indicates whether notifications are requested from 3GPP NextGen RAN (NG-RAN) when the Guaranteed Flow Bit Rate (GFBR) is no longer available for a QoS Flow during the lifetime of the QoS Flow. By default, the value of this parameter is **False**.
   - **Priority Level**: Enter an integer value to indicate the scheduling of resources among QoS Flows.
   - **Aver Window**: Enter an integer value to indicate the duration for which the guaranteed, and maximum bitrate is to be calculated.
   - **Max Data Burst Vol**: Enter an integer value to indicate the maximum amount of data to be transferred for 5G-AN PDB.
   - **Reflective QoS**: Enter a boolean value to indicate whether the QoS information is reflective for the corresponding Service Data Flow. The default value of this parameter is **False**.
   - **Sharing Key Dl**: Configure this parameter to indicate the PCC rules that can share a resource in the downlink direction.
   - **Sharing Key Ul**: Configure this parameter to indicate the PCC rules that can share a resource in the uplink direction.
   - **Max Packet Loss Rate Dl**: Configure this parameter to indicate the downlink maximum rate for the lost packets that can be used for a service data flow.
   - **Max Packet Loss Rate Ul**: Configure this parameter to indicate the uplink maximum rate for the lost packets that can be used for a service data flow.
   - **Def Qos Flow Indication**: Enter a boolean value to indicate the binding of QoS Flow, which is associated with the default QoS rule, with the dynamic PCC rule. The default value of this parameter is **False**.
6. Click **Add**.

TableDrivenQosDecision

This section describes how to configure the TableDrivenQosDecision Service.

The TableDrivenQosDecision service configuration captures the data from the custom CRD table for the newly added fields. This table defines and associates the parameters in the table.

Before setting the service parameters, ensure that you create a use case template and add a service for this configuration. For details, see Configuring the Use Case Template and Adding a Service.

To configure the TableDrivenQosDecision service parameters, use the following configuration:

1. Log in to Policy Builder.
2. Click the **Services** tab.
3. Configure the following parameters:
   a. From the **Use Case Template** pane, select the N7 service configuration object.
   b. From the **Service Configurations** pane, select **TableDrivenQosDecision**.
   c. Click **Add**.

   The **Select Service Configuration** window appears.
4. From the N7 service configuration, click **TableDrivenQosDecision**.

   The service configuration parameters appear in the right pane.
5. Configure one or more of the following **TableDrivenQosDecision** parameters:
   - **Qnc Source**: Enter the primary key value for the column configured under **Search Column**.
   - **Authorized QoS Priority Level**: Specify the priority that is used for scheduling the resources among the QoS Flows.
   - **Aver Window Source**: Specify the duration over which the guaranteed, and maximum bitrate is calculated.
   - **Max Data Burst Vol Source**: Enter the maximum amount of data that is required to be transferred within a period of 5G-AN PDB.
   - **Reflective QoS Source**: Specify the value that applies reflective QoS for the SDF.
   - **Sharing Key Dl Source**: Specify the value that indicates resource sharing in downlink direction with the service data flows having the same value in their PCC rule.
   - **Sharing Key Ul Source**: Specify the value that indicates resource sharing in an uplink direction with the service data flows having the same value in their PCC rule.
   - **Max Packet Loss Rate DI Source**: Specify the maximum rate for lost packets that can be tolerated in the downlink direction for the service data flow.
   - **Max Packet Loss Rate UI Source**: Enter the maximum rate for lost packets that can be tolerated in the uplink direction for the service data flow.
   - **Def QoS Flow Indication Source**: Enter the value that indicates the dynamic PCC rule that shall always have its binding with the default QoS Flow.

   Only the mandatory parameters are listed in this section. For the complete list of parameters, see TableDrivenQosDecision.
6. Click **Add**.

TableDrivenDynamicPccRule

This section describes how to configure the TableDrivenDynamicPccRule service.

The TableDrivenDynamicPccRule service configuration shows one or more PCC rules that are available in the custom reference data table.

Before setting the service parameters, ensure that you create a use case template and add a service for this configuration. For details, see Configuring the Use Case Template and Adding a Service.

To configure the TableDrivenDynamicPccRule service parameters, use the following configuration.

1. Log in to Policy Builder.
2. Click the **Services** tab.
3. Configure the following:
   a. From the **Use Case Template** pane, choose the N7 service configuration object.
   b. From the **Service Configurations** pane, choose **TableDrivenDynamicPccRule**.
   c. Click **Add**.

   The **Select Service Configuration** window appears.
4. From the N7 service configuration, click **TableDrivenDynamicPccRule**.

   The service configuration parameters appear in the right pane.
5. Configure one or more of the following **TableDrivenDynamicPccRule** parameters:
   - **Search Table**: Enter the name of the table that is used to perform a lookup.
   - **Search Column**: Enter a value, which is associated with the primary key column of the STG. The data that is contained in the STG column has a text value.
   - **Search Value**: Enter a value of the **Search Column** primary key to perform a lookup in **Search Table**.
   - **Input List (List)**: If the lookup requires extra key or value pairs, then configure this field using **InputColumn** under **Input List**.
     - **Column Name**: Enter a value that is associated with the additional key column of STG.
     - **Column Value**: Enter the value that you have entered for the **Column Name** field.
   - **Pcc Rule Id Source**: Specify a value for the key column that is associated with the PccRuleId column within the STG. The data that is contained in the STG column has a text value.
   - **Precedence Source**: Enter a value for this field that is associated with the Precedence column in STG. The data that is contained in the STG column has a numeric value. For the allowed values, see 3GPP specification 29.512.
   - **App Id Source**: Specify a value that is associated with the App Id column in the STG. The data that is contained in the STG column has a text value.
   - **Qos Id Source**: Enter a value that is associated with the Qos Id column in the STG. The data that is contained in the STG column has a text value.

- **Chg Id Source**: Specify a value that is associated with the Chg Id column in the STG. The data that is contained in the STG column has a text value.
- **Flow Information Source**: Enter a value that is associated with the **Flow Information column** in the STG. The data that is contained in the STG column has a text value.

  Only the mandatory parameters are listed in this section. For the complete list of parameters, TableDrivenDynamicPccRule.

Note

- Use the following format to add the **Flow Information Source** parameter for PCF to perform Flow Information grouped parameter mapping:

  Multiple Flow Information is separated by "," as delimiter, whereas each Flow Information the format is: <Flow Description1>;<packetFilterUsage1>;<Tos TrafficClass1>;<Spi1> ;<Flow Label1>;<Flow Direction1>, <Flow Description2>;<packetFilterUsage2>
- Using an incorrect format results in missing the Flow Information value.

6. Click **Add**.

Use Case Initiators

This section describes how to configure the Use Case Initiators.

Use case initiators are a group of conditions that indicate the time, event, or functionality for a specific service to be added for a subscriber. If no use case initiators are configured, then the service configuration objects are added.

1. Log in to Policy Builder.
2. Click the **Services** tab.
3. From the **Use Case Template** pane, select the N7 service configuration object, and click the **Use Case Initiators** tab.
4. In the **Service Initiators (OR Together)** field, configure multiple use case initiators, which activate the Use Case Template and its service configurations. Service Initiators are a group of conditions. If any one of the service initiators of the use case template is true then the service configuration of that use case template are used.

Note In the **Service Initiators (OR Together)** box, select the add icon to add a service initiator and close icon to remove a service initiator. Use the up or down arrow buttons to specify the order in which service initiators are to be evaluated.

5. In the **Initiator Name** field, enter a name for the group of conditions.
6. In the **Conditions (AND Together)** field, click **Add**.

   The condition box appears.

7. Select one or more conditions from the Select a Condition Phrase window from the PCF, N7, 3GPP, or N28 3GPP messages option. The conditions that you add are associated with the service initiator. Conditions are related to the messages session, subscriber information, balance information, or the message itself.

   The conditions that you select appear in the **Conditions (AND Together)** box.

Note If multiple conditions exist for the **Conditions (AND Together)** box, then all the chosen conditions must be true for them to be configured.

8. In the **Conditions (AND Together)** box, click one or multiple conditions.

   The input variables for the selected condition appear in the right pane.

9. From the available input variables, add all or the required input variables. See the Conditions of Input Variables, on page 11 section for the conditions to configure for the input variables.

   The input variables are added.

10. Configure the values for the added variables.

    The use case initiators are configured.

Conditions of Input Variables

The table lists the conditions for the input variables.

Condition for Input Variable	Description
A Policy Request Message exists	An N7, N15, N28, or UDR Policy Request message exists in the system.
A Policy Request Message does not exist	An N7, N15, N28, or UDR Policy Request does not exist in the system.
A Policy Message exists	An N7, N15, N28, or UDR Policy Request or Response message exists in the system.
A Policy Message does not exist	An N7, N15, N28, or UDR Policy Request or Response message does not exist in the system.
A Policy Response Message exists	An N7, N15, N28, or UDR Policy Response message exists in the system.
A Policy Response Message does not exist	An N7, N15, N28, or UDR Policy Response message does not exist in the system.
A Policy N7 TGPP Session exists	A valid N7 TGPP session exists in the Policy Builder configuration for a subscriber.
A Policy N7 TGPP Session does not exist	A valid N7 TGPP session does not exist in the Policy Builder configuration for a subscriber.

Condition for Input Variable	Description
A N28 TGPP Session exists	A valid N28 TGPP session exists in the Policy Builder configuration for a subscriber.
A N28 TGPP Session does not exist	A valid N28 TGPP session does not exist in the Policy Builder configuration for a subscriber.

Retrievers

Retrievers are the values that are retrieved for the key columns from the custom reference data table. You can retrieve the value of retrievers in the following ways in Policy Builder.

- Using the Service Configuration option
- Using the custom reference data table

Following is the list of the available session-level retrievers in PCF:

- N7 Access Type
- N7 Cell Global Identifier
- N7 DNN
- N7 GPSI
- N7 MCC (SUPI Based)
- N7 MNC (SUPI Based)
- N7 Permanent Equipment Identifier
- N7 RAT Type
- N7 Serving Network
- N7 SliceInformation
- N7 SUPI
- N7 Tracking Area Identifier

Note These retrievers are session-level retrievers and not the message-level retrievers. It implies that as a request is received, a session is created in the database for a subscriber. Then, the value of these retrievers is retrieved from those sessions.

Configuring Retrievers through Custom Reference Data Table

This section describes how to configure the retrievers through the custom reference data table.

1. Log in to Policy Builder.
2. From the **Custom Reference Data Tables** pane, select a rule.

The parameters of the selected custom reference table appear in the right pane.

3. In the **Columns** box, select a key column.
4. Click the **Bind to Session/Policy State** option and click **Select**.

   A dialog box with the list of available retrievers appears.
5. In the text box, enter **N7** or **N15**to view all the newly added retrievers.
6. Select a retriever and click **OK**.

Configuring Retrievers through Service Configuration

This section describes how to configure the retrievers through the service configuration.

1. Log in to Policy Builder.
2. From the Services pane, click the N7/N15 service-compliant configuration.
3. Select a service configuration from **Service Configurations** box.

   The parameters of the selected service parameters appear.
4. Choose a parameter and click the pull value icon to pull a value for the parameter.

   The **Dynamically pull this value from** window appears.
5. Click the **Bind to Session/Policy State** option and click **Select**.

   A window showing the list of available retrievers appears.
6. In the text box, enter **N7** or **N15** to view all the newly added retrievers.
7. Select a retriever and click **OK**.