

N5 Authorization

- Feature Summary and Revision History, on page 1
- Feature Description, on page 1
- How it Works, on page 2
- Feature Configuration, on page 8

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
First introduced.	2022.02.0

Feature Description

PCF provides a method for the service providers to regulate the services available to individual subscribers. You can configure the bearer-level regulation through the customization and configuration of N5 Authorization.

The configuration handles the Video over NR (ViNR) authorization as per the subscriber attributes (SUPI, GPSI, and Throttling) to control the services available to each subscriber.

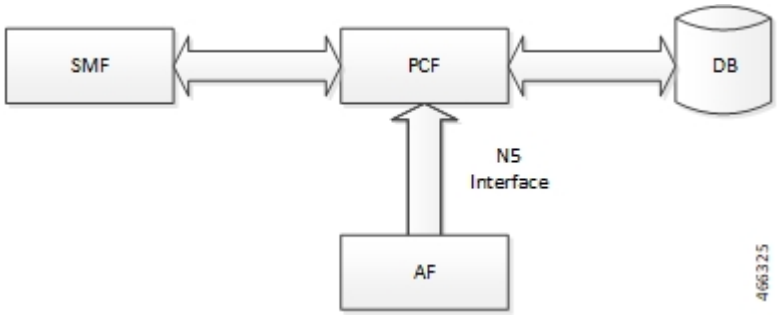
Architecture

This section depicts how the network function components interact during an N5 Authorization.

The SMF and PCF have a bilateral communication over the N7 interface. The AF sends an N5 Create/Update request to PCF. The PCF performs the N5 Authorization of the request by evaluating the message for the missing media type attribute and consults the value that is assigned to the Bearer-Authorization column in the STG table for the configured status as accept or reject. PCF fetches the STG information from the associated database. PCF communicates the evaluation result to the SMF and AF through REST requests.

The following figure illustrates how the NF interactions happen over the N5 interface.

Figure 1: NF Interactions



Components

This section describes the N5AuthorizationSTGConfiguration component in the N5 Authorization process.

The N5AuthorizationSTGConfiguration service configuration is used to evaluate the N5 Authorization table and obtain the configured output values. The N5AuthorizationSTGConfiguration service supports chained evaluation of Search Table Groups (STGs) which means multiple STGs are configured hierarchically in the service and outputs of one table is used as input keys for another table. The N5AuthorizationSTGConfiguration configuration evaluates all the bearers on receiving a Rest message and sends the appropriate Rest requests or responses depending on the bearer's authorization status provided the N5 session exists. The N5 Authorization table from which Bearer Authorization and Error Cause output values are received is configured as the last table in the list of chained STGs configured under N5AuthorizationSTGConfiguration.

How it Works

This section describes how this feature works.

At a high-level, PCF supports the N5-based authorization of bearers. The N5 authorization requires a Search Table Groups (STG), which enables logical grouping of multiple Customer Reference Data (CRD) tables. Within this STG, a CRD table that is dedicated to N5 Authorization is created in the Policy Builder. The input keys in the CRD signify the conditions based on which PCF determines the throttle limit for a bearer. The table has the following output columns:

- Bearer Authorization: Indicates whether to allow or reject a bearer.

- Error Cause: Specifies the Error-Message that is included in the N5 response, if necessary.

If PCF is configured to reject the N5 dedicated bearer when the associated Media-Type is missing, it rejects the bearer with the HTTP status code = 403 Forbidden, problem cause=REQUESTED_SERVICE_NOT_AUTHORIZED and, problem detail="Invalid service information, Media type is not specified" in response.

PCF is configured to reject a non-GBR bearer if the value for both, upload and download of the non-GBR bearer is set to 0. PCF determines if the bearer is non-GBR with 0-bit rate after consulting the NON-GBR QCI and ZERO BIT RATE QoS input columns in the N5 Authorization table. If Bearer-Authorization value is set to REJECT, then PCF rejects the bearer with HTTP status code=403 Forbidden, problem cause=REQUESTED_SERVICE_NOT_AUTHORIZED and, problem detail="BLOCKED" in response.

If PCF receives a N5 Create/Update request with multiple media components, and it rejects one of the media component after assessing for N5 Authorization, PCF sends a successful response for the accepted media components. For the rejected media components, PCF creates a scheduled event for sending a delayed N5 Notify request. You can configure the duration between the rejection and the time when scheduling the delayed message happens. The default value is set to 500 milliseconds.

Note In case, PCF rejects multiple media components with cause=REQUESTED_SERVICE_NOT_AUTHORIZED, the error resulting from the last rejected media component is set as problem detail in the response.

For existing bearers in an N5 session, PCF evaluates them for N5 Authorization when an event occurs such as LDAP refresh, N28 NOTIFY, and N7_NOTIFY. In situations where all the media components that are stored in the N5 sessions are rejected, then PCF sends a N7 Notify Terminate request to Application Function (AF).

Note You may observe a degradation in the performance of the PCF system when the N5AuthorizationSTGConfiguration service is added. The level of degradation corresponds to the number of STGs configured for the chained evaluation in the N5AuthorizationSTGConfiguration service and the number of bearers the service has evaluated.

Call Flows

This section describes the key call flows for this feature.

All Bearers Are Rejected Call Flow

This section describes the All Bearers Are Rejected call flow.

Figure 2: All Bearers Are Rejected Call Flow

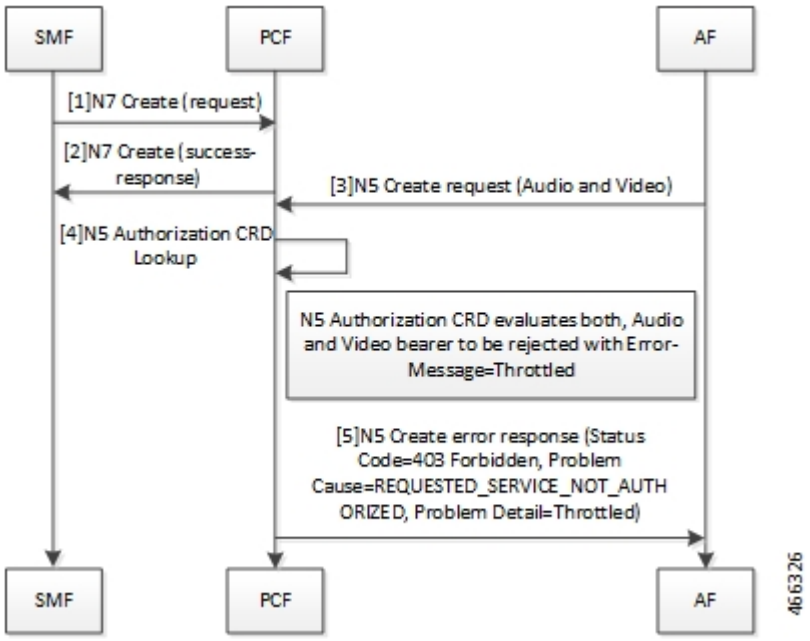


Table 3: All Bearers Are Rejected Call Flow Description

Step	Description
1	The SMF sends a N7 Create request to the PCF.
2	The PCF responds to the SMF with the success response.
3	The AF sends an N5 Create request (Audio and Video) message to the PCF.
4	The PCF performs the N5 Authorization CRD lookup.
5	The N5 Authorization CRD evaluates both, audio and video bearer. If there is a missing MediaType IE, PCF rejects the bearer. PCF validates all the bearers for Bearer-Authorization=REJECT. The bearers are classified as unauthorized and are not installed on the SMF. If all bearers received in the AAR are rejected, PCF sends a N5 Create error response with Status Code=403 Forbidden, Problem Cause=REQUESTED_SERVICE_NOT_AUTHORIZED, Problem Detail=Throttled to the AF

Few Bearers Are Rejected Call Flow

This section describes the Few Bearers are Rejected call flow.

Figure 3: Few Bearers Are Rejected Call Flow

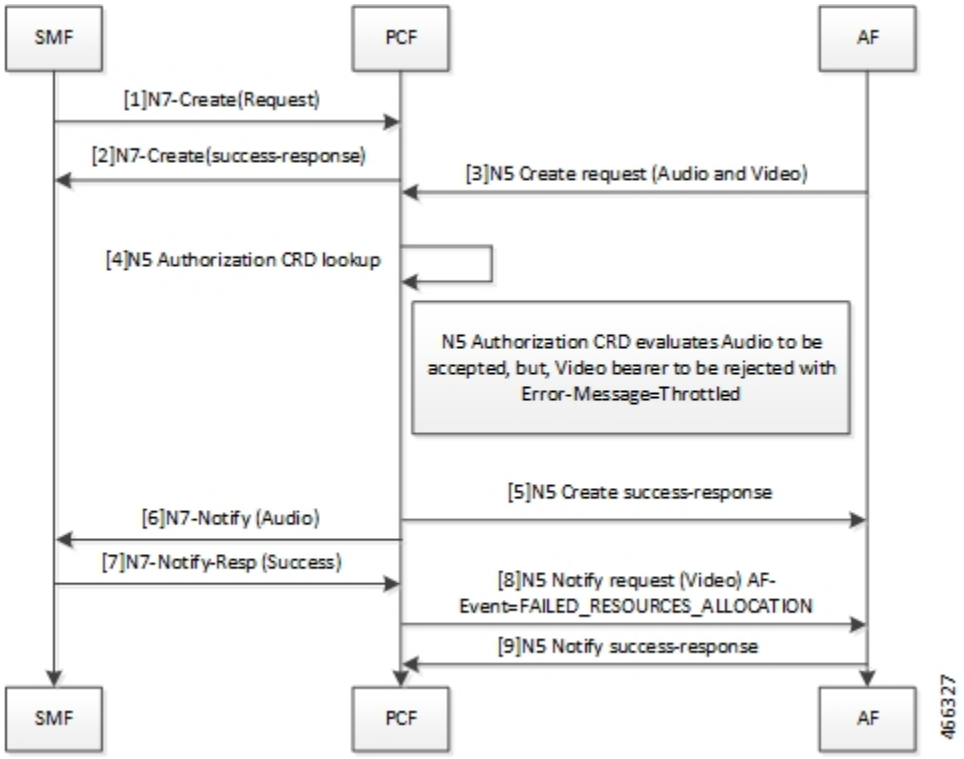


Table 4: Few Bearers Are Rejected Call Flow Description

Step	Description
1	The SMF sends a N7 Create request to the PCF.
2	The PCF responds to SMF with success response.
3	The AF sends an N5 Create request (Audio and Video) message to the PCF.
4	The PCF performs the N5 Authorization CRD lookup.
5	The N5 Authorization CRD evaluates both the audio and video bearers. The audio bearers that contain the required MediaType IE are tagged as accepted. Video bearers with the missing MediaType IE are rejected. Bearers evaluated to Bearer-Authorization=ACCEPT are authorized and installed on the SMF. PCF responds to the accepted audio bearers with N5 Create success response.
6	The PCF sends N7 Notify (Audio) to the SMF.
7	The SMF responds to the PCF with a N7 Notify-Resp (Success).
8	Bearers evaluated to Bearer-Authorization=REJECT are marked as unauthorized and are not installed at the SMF. The PCF sends N5 Notify request (Video) AF-Event=FAILED_RESOURCES_ALLOCATION to AF.

Step	Description
9	The AF responds with N5 Notify success-response to the PCF.

Existing Bearers Are Rejected Call Flow

This section describes the Existing Bearers Are Rejected call flow.

Figure 4: Existing Bearers Are Rejected Call Flow

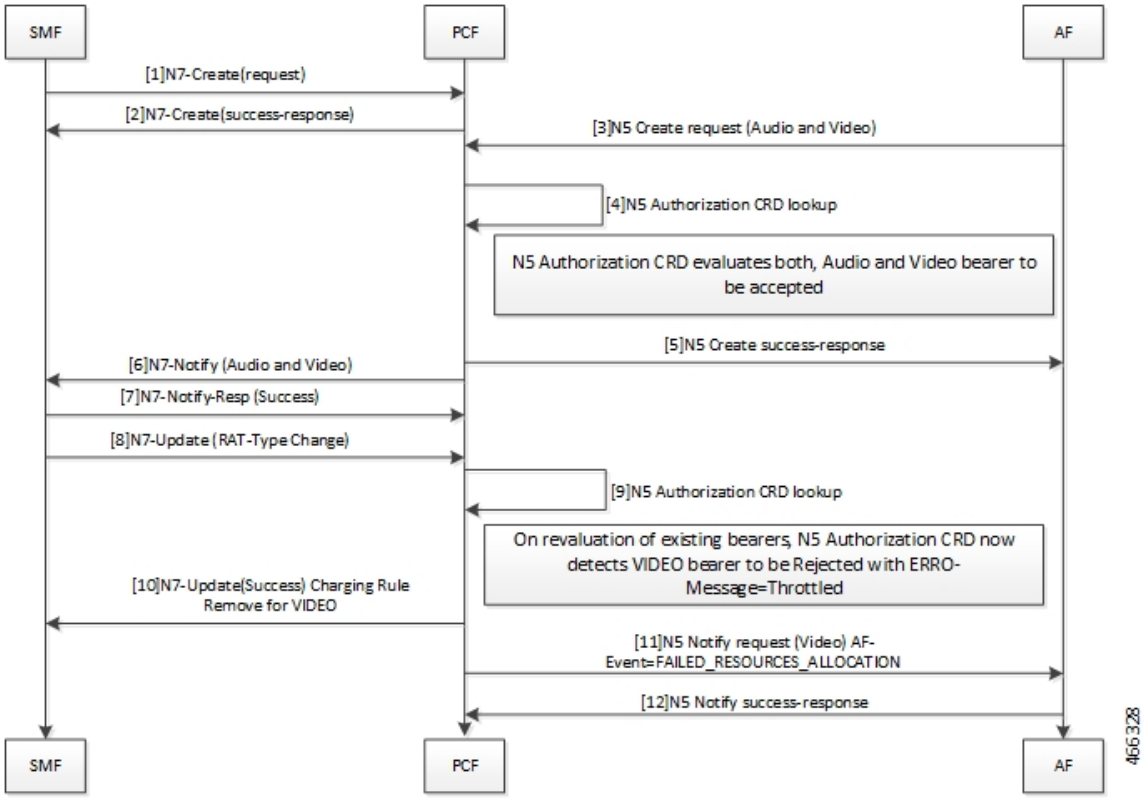


Table 5: All Bearers Are Rejected Call Flow Description

Step	Description
1	The SMF sends a N7 Create request to the PCF.
2	The PCF responds to the SMF with a N7 Create Success response.
3	The AF sends N5 Create request (Audio and Video) message to the PCF.
4	The PCF performs the N5 Authorization CRD lookup.
5	The N5 Authorization CRD evaluates both, the audio and video bearers. If successful authorization, PCF sends N5 Create success response to AF.
6	The PCF sends N7 Notify (Audio and Video) message.

Step	Description
7	The SMF responds with N7-Notify-Resp (Success) to the PCF.
8	The SMF sends N7 Update (RAT-Type Change).
9	The PCF performs the N5 Authorization CRD lookup.
10	When PCF reevaluates the existing bearer and the N5 Authorization CRD detects a VIDEO bearer with the Bearer-Authorization=REJECT, PCF rejects the bearer with Error-Message=Throttled. The PCF sends N7-UPDATE (Success) Charging Rule Remove for VIDEO to the SMF.
11	The PCF sends N5 Notify request (Video) AF-Event=FAILED_RESOURCES_ALLOCATION to the AF
12	The AF responds with N5 Notify success-response to the PCF.

Considerations

The following considerations apply when you configure the N5 Authorization:

- The STG names that are configured in the N5AuthorizationSTGConfiguration should be unique.
- The IE names for the output columns that are configured in the N5AuthorizationSTGConfiguration service should be unique.
- The chained evaluation keys should have the same IE name for the output column in the source table, and the input column in the destination table.
- The result of the N5AuthorizationSTGConfiguration service is available in the last table that is defined in the list. The table includes the output columns with the following mandatory IE names: Bearer-Authorization and Error-Message.
- The Bearer-Authorization column can be configured to accept the fixed values that are Accept and Reject.
- Perform the configurations that are required for defining and mapping the CRD tables as per the requirement.
- The Policy Server evaluates the mapped source output IEs (result column of the STG) through the CRD which it has created. If PCF has not created the CRD, then it cannot query the corresponding chained input key which further limits it from verifying the N5 Authorization.
- 1:1 mapping must exist between a chained pair of output IE and the input key.

Limitations

This feature has the following limitations in this release:

- When N5 Authorization fails, PCF sends an N5 Notify request only if the AF has subscribed to AF-Event=FAILED_RESOURCES_ALLOCATION in N5 Create request.
- The N5 Authorization is performed only against MediaComponent IE in the request. This indicates that the attributes from N5 Create/Update messages that are used as input for the CRD table evaluation should be from MediaComponent IE only. PCF does not evaluate the MediaSubComponent IE.

- If using the PolicyState or Session data retrievers that are bound to the input keys, then PCF retrieves the data for the input keys if it is inserted into the session data.

Feature Configuration

This section describes how to configure N5 Authorization.

The configuration of the N5 Authorization capability in PCF involves the following steps:

1. Creating the STG Tables
2. Adding the N5AuthorizationSTGConfiguration Service
3. Configuring the Service Chaining
4. Rejecting N5 Create with Missing MediaType IE
5. Setting Up the Delayed Message Schedule

Creating the STG Tables

This section describes how to create the STG column in Policy Builder.

To configure the STG column, use the following configuration:

1. Log in to Policy Builder.
2. Click the **Reference Data** tab, and from the left pane click **Custom Reference Data Tables** to view the options.
3. On the left pane, click the **Search Table Groups** folder.
4. In the **Search Table Group Summary** pane, click **Search Table Group**. A default STG gets created under the **Search Table Groups** folder.
5. Click the new STG and in the **Search Table Groups** pane rename the STG with a unique name.
6. Click **Customer Reference Data Table**. A new table gets created on the left pane.
7. Click the new table to open the **Customer Reference Data Table** pane. Rename the table with a unique name.
8. Navigate to the Columns section and click **Add**. A default column gets added to the Columns section.
9. Click the newly created column heading and rename it. Select the options in the corresponding row as applicable to your environment.



Note If the **Key** option is selected for a specific column, then it indicates as the input column.

10. Save the changes.

Adding the N5AuthorizationSTGConfiguration Service

This section describes how to add the N5AuthorizationSTGConfiguration service.

To configure the N5AuthorizationSTGConfiguration service, use the following configuration:

1. Log in to Policy Builder.
2. Choose the **Services** tab, and from the left pane click **Use Case Templates** to create a new service.
3. On the left pane, click **Summary** to open the **Summary** pane.
4. Under **Actions**, click **Use Case Template**.
5. In the **Use Case Template** pane, specify the name for the template.
6. Click the **Actions** tab and select **Add**.
7. In the **Select Service Configuration** dialog box, select the N5AuthorizationSTGConfiguration and click **OK**. The Use Case template with the specified name is created.
8. In the left pane, click **Services > Service Options** to view the options. The newly created service appears in the **Service Options**.
9. Select the service that you have created.
10. Under **Service Configurations**, click **Add** to open the **Select Service Configuration** dialog box.
11. Under **Service Configurations**, select **N5AuthorizationSTGConfiguration**, then click **OK**.

Configuring the Service Chaining

This section describes how to configure the service chaining for N5 Authorization.

Before configuring the service chaining, ensure that you have created the use case templates and added the N5AuthorizationSTGConfiguration service. Use case templates are the building blocks of the PCF architecture. The use case templates allow you to define the Service Configuration objects to be set by a Service Option.

To configure service chaining, use the following configuration:

1. Log in to Policy Builder.
2. Click the **Services** tab, and from the left pane click **Service Options** to view the options.
3. Expand the new service that you have created, and select the child.
4. In the **Service Option** pane, select **N5_AuthorizationSTGConfiguration** service under **Service Configurations** and specify the N5_AuthorizationSTGConfiguration parameters.
5. Expand the **List Of Input Column Avp Pairs (List) > ColumnAndAvpPair**, and enter the appropriate information.
6. Expand the **List Of Output Column Avp Pairs (List) > ColumnAndAvpPair**, and enter the Avp Name as Bearer-Authorization. Similarly, in another **ColumnAndAvpPair > Avp Name** field specify Error-Message.
7. Save the changes.

Rejecting the N5 Create Request with Missing MediaType IE

This section describes how to enable PCF to reject the N5 Create Request with Missing MediaType IE.

To configure PCF to reject the N5 Create Request, use the following configuration:

1. Log in to Policy Builder.
2. Click the **Reference Data** tab.
3. In the left pane, click **SBA Profiles** > **N5 Profiles**.
4. Click **N5 Profile**.
5. In the **N5 Profile** pane, select the **Reject AAR with missing Media Type** check box.
6. Save the changes.

Setting Up the Delayed Message Schedule

This section describes how to set up the duration after which PCF sends the delayed message to the AF.

To configure the delayed message schedule through the Policy Builder, use the following configuration:

1. Log in to Policy Builder.
2. Click the **Reference Data** tab.
3. In the left pane, click **SBA Profiles** > **N5 Profile**.
4. Click **N5 Profile**.
5. In the **N5 Profile** pane, specify the duration in the **Sending Delayed Message Wait Time (In millisec)** field. If you do not specify the period, then PCF considers the default period of 500 milliseconds.

N5 Profile

This section describes the parameters, which you can configure for the N5 Profile.

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.

The following table describes the N5 Profile service parameters:

Table 6: N5 Client Parameters

Parameter	Description
Reject AAR with missing Media Type	Enables PCF to reject the N5 Create/Update requests when MediaComponent have MediaType IE unspecified. PCF rejects the request with HTTP Status Code=403 Forbidden, Problem Cause=REQUESTED_SERVICE_NOT_AUTHORIZED To enable the parameter, select the check box available in the **SBA Profiles** > **N5 Profiles**.

Parameter	Description
Delayed Message Wait Time	Allows you to specify the duration after which PCF sends a delayed message. The default value is 500 milliseconds. To define the duration, specify the period in the text field available in **SBA Profiles > N5 Profiles**.