



Interfaces Support

- [Feature Summary and Revision History, on page 1](#)
- [Feature Description , on page 2](#)
- [Configuring Interfaces, on page 58](#)

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
Added support for: <ul style="list-style-type: none"> • Cause IE on N11 interface. • NAS messages compliance with invalid protocol data handling. • ProblemDetails JSON object on N11 interface. • Error handling with HTTP error codes. • HTTP/2 TLS support for SBA interface. 	2021.02.0
First introduced.	Pre-2020.02.0

Feature Description



Important The PGW-C term used in this chapter denote the EPS interworking functionality supported by SMF and must not be assumed as a standalone P-GW that is used in the LTE network.

In the 5G System Architecture, the SMF performs the session management functions that the 4G Mobility Management Entity (MME), Serving Gateway Control plane function (SGW-C), and PDN Gateway Control plane function (PGW-C) handle. The SMF is one of the elements of the Service-Based Architecture (SBA). SMF is responsible for communicating with the decoupled data plane, creating, updating, and removing Protocol Data Unit (PDU) sessions, and managing session context with the User Plane Function (UPF). For the session management-related functions, SMF communicates with various interfaces, such as N1, N4, and N10.

All the SMF interfaces support IPv4 address but only the SBI (N7, N10, N11, N40), N3, and N4 interfaces support either IPv4 or IPv6 address. For the IP address support, both the endpoint and interfaces configuration must include unique VIP IP and port. For configuration details, see the [Configuring Interfaces, on page 58](#) section.

During UPF association setup, the SMF checks if the transport type in the setup request is the same as the configured address. The SMF proceeds with the association request or rejects the request based on the validation result.

Similarly, during NRF discovery, the transport type must match the statically configured transport type either at the endpoint level or interface level. The SMF performs NF selection based on the IP address matching criteria.

3GPP Specification Compliance for SMF Interfaces

Feature Description

The SMF supports the 3GPP specification compliance either of the December 2018 version or the June 2019 version for the SMF interfaces, such as N1, N2, N4, N7, N10, N11, N40, and Nnrf. The SMF processes the messages from these interfaces in compliance with the profile configured for the corresponding services. For information on the compliance profile configurations, see the [Configuring 3GPP Specification Compliance for Interfaces, on page 4](#) section.

SMF supports only the IE encoding and decoding functionality. The existing features work with the June 2019 specification versions. No additional features in the June 2019 version are supported.



Note The SMF continues to support the older versions of 3GPP specifications and the compliance profile configuration controls the same for the SMF interfaces.

Standards Compliance

The SMF is one of the control plane (CP) NFs of the 5G core network. The SMF uses different interfaces to communicate with the other NFs or nodes. For example, the N4 interface exists between the SMF and User Plane Function (UPF). Each of the SMF interfaces comply to a specific version of the 3GPP specification depending on the supported compliance version.

Use the following table to determine the compliance mapping of each SMF interface and the 3GPP Standards specification versions.

Table 3: SMF Interface and 3GPP Standards Specification Version Map

Interface	Relationship	3GPP Specification	Version
N1/NAS	Between UE and AMF	24.501	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support: 15.4.0
N2/NGAP	Between RAN and AMF	38.413	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support: 15.4.0
N4	Between UPF and SMF	29.244	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support: 15.4.0
N7	Between PCF and SMF	29.512	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support: 15.4.0
N10	Between UDM and SMF	29.503	For December 2018 Compliance Support: 15.2.1 For June 2019 Compliance Support: 15.4.0

Interface	Relationship	3GPP Specification	Version
N11	Between AMF and SMF	29.518 29.502	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support: 15.4.0
N40	Between SMF and CHF	32.291	For December 2018 Compliance Support: 15.1.0 For June 2019 Compliance Support: 15.3.0
Nnrf	Between NRF and SMF	29.510	For December 2018 Compliance Support: 15.0.0 For June 2019 Compliance Support: 15.4.0

Configuring 3GPP Specification Compliance for Interfaces

To configure the SMF interfaces in compliance with the 3GPP specifications, use the following sample configuration:

```

config
  profile compliance profile_name
    service { n1 | n2 | namf-comm | nchf-convergedcharging | nnrf-disc
  | nnrf-nfm | npcf-smpolicycontrol | nsmf-pdusession | nudm-sdm | nudm-uecm
  | threegpp23502 }
    version { full version_format | spec spec_version | uri uri_version }
  end

```



Important Service selection is based only on the specification version. In future releases, the full API version will be used.

NOTES:

- **service** { *n1* | *n2* | **namf-comm** | **nchf-convergedcharging** | **nnrf-disc** | **nnrf-nfm** | **npcf-smpolicycontrol** | **nsmf-pdusession** | **nudm-sdm** | **nudm-uecm** | **threegpp23502** }: Specify the service names as cited in *3GPP TS 29.510 version 15.2.0, section 6.1.6.3.11*.
- **version full** *version_format*: Specify the API full version for each service in the following format:
<Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>]
The format is specified in *3GPP TS 29.501 version 15.2.0, section 4.3.1.1*.
- **version uri** *uri_version*: Specify the API version URI for each service in the following format:
"v" concatenated with a number, where value can be both v1 and v2, or either v1 or v2.
For example, for the compliance version 15.4.0 in the NRF configuration for the service type nudm-sdm or nudm-uecm, mandate the configuration of the uri-version in the version to "v2". For compliance version 15.2.1, this configuration is optional.
For example, version v1: (- url: '{apiRoot}/nsmf-pdusession/v1').

- **version spec** *spec_version*: Specify the 3GPP specification version number, which is one of the following values:
 - 15.0.0
 - 15.1.0
 - 15.2.0
 - 15.2.1
 - 15.4.0
 - 15.3.0
 - 15.3.0.std

For example, to support 3GPP June 2019 specification compliance for the N7 (PCF) interface, configure the specification version as *15.4.0*.

The default version number depends on the SMF interface. For example, the default version is *15.2.0* for the N7 interface. Similarly, for the N10 interface, the default version is *15.2.1*.



Important

Configuring the 3GPP specification version value depends on the SMF interface. Not all the preceding versions are options for the SMF interfaces. Only a combination of the preceding versions exist as options for the 3GPP version compliance configuration. For details on the compliance version, see the [Standards Compliance, on page 3](#) section.

Configuration Verification

To verify if the 3GPP specification profile compliance is configured, use the following **show full-configuration profile smf** command:

```
[smf] smf(config)# show full-configuration profile smf
profile smf smf1
  locality      LOC1
  allowed-nssai [ slicel ]
  instances 1 fqdn cisco.com.apn.epc.mnc456.mcc123 node-id abcdef
  plmn-list mcc 123 mnc 456
  exit
  plmn-list mcc 242 mnc 01
  exit
  plmn-list mcc 310 mnc 210
  exit
  plmn-list mcc 310 mnc 220
  exit
  plmn-list mcc 310 mnc 260
  exit
  plmn-list mcc 310 mnc 310
  exit
  plmn-list mcc 440 mnc 550
  exit
  service name nsmf-pdu
  type          pdu-session
  schema        http
  service-id    1
  version       1.Rn.0.0
  http-endpoint base-url http://smf-service
```

```

icmpv6-profile      icmpprf1
compliance-profile compl
access-profile      access1
subscriber-policy   polSub
exit
exit
    
```

To verify the configuration, use **show full** command in the 3GPP specification profile compliance configuration mode:

```

product smf(config-compliance-compl)# show full
profile compliance compl
  service nsmf-pdusession
  version uri v1
  version full 1.0.0
  version spec 15.2.0
product smf(config-service-nsmf-pdu)# compliance-profile compl
    
```

Supported SMF Interfaces

This section describes the different interfaces that SMF use for facilitating communication with other network functions.

GTP Interface

General Packet Radio Service (GPRS) tunneling protocol (GTP) is the primary protocol used in a GPRS core network through the 3G, 4G, or the 5G network. The GTP is responsible for signaling and transporting mobile data within the core network.

GTP uses the N9 interface as the reference point between two core user plane functions (UPFs).

GTP Cause Code Handling

Feature Description

The SMF supports GTP cause code handling for 4G procedures when it detects any failure with the IEs.

Create Session Request

The SMF supports the following causes in the Create Session Request message.

Table 4: Supported Causes in Create Session Request

Cause	SMF Behavior
Missing or unknown APN	If the configured DNN does not match the DNN received in Create Session Request, then SMF rejects the message with this cause value in Create Session Response and sets the appropriate disconnect reason.
User authentication failed	If SMF receives failure AAA secondary authentication response from RADIUS, then SMF rejects the message with this cause value in Create Session Response. This cause indicates that the request is rejected due to failure in authentication or security procedure, and sets the appropriate disconnect reason.

Cause	SMF Behavior
APN access denied – no subscription	If SMF receives the subscription fetch failure response from UDM, then SMF rejects the message with this cause value in Create Session Response. This cause indicates that the SMF has denied user access to an APN because the subscriber does not have the necessary subscription. SMF also sets the appropriate disconnect reason.
New PDN type due to single address bearer only	If the Dual Address Bearer Flag (DAF) indication is not set and the requested PDN-type is IPV4V6 in Create Session Request message, then SMF rejects the message with this cause value in Create Session Response. SMF also sets the appropriate disconnect reason.
Late Overlapping Request	<p>The Create Session Request message includes the Origination Time Stamp indicating the absolute time at which the request is initiated (as specified in clause 13.2.2, TS29.274).</p> <p>If SMF receives any subsequent CSR from different S-GW and different sequence number with older timestamp in "Origination Time Stamp" than the time stamp stored for the existing session, then SMF rejects the new CSR with this cause value in Create Session Response. This cause indicates the incoming request collides with an existing session that does not have a recent time stamp than the time stamp of the new request.</p> <p>If the timestamp is newer, then SMF aborts the current procedure and handles the new CSR request with the recent time stamp.</p>
Timed Out Request	If the incoming CSR received origination-time-stamp and maximum-wait-time IEs, SMF starts the SLA timer with maximum-wait-time value at the start of the Create procedure and aborts the Create procedure on expiry of the timer. Then SMF rejects with this cause value in CSR Response.
New PDN type due to network preference	If the session type configured under profile dnn is IPv4 or IPv6, and the requested PDN type coming in Create Session Request is IPv4v6, then SMF rejects the message with this cause value in Create Session Response.

Delete Bearer Request

The SMF supports the following causes in the Delete Bearer Request message.

Table 5: Supported Causes in Delete Bearer Request

Cause	Scenario
Reactivation required	SMF sends Delete Bearer Response for default bearer with this cause value in the following cases: <ul style="list-style-type: none"> • CHF reconciliation • PCF reconciliation • Internal DB conflict • Session Report with SRSR/GTER/SRIR/SPTER/ERIR
PDN connection inactivity timer expires	SMF sends Delete Bearer Response for default bearer with this cause value in the following cases: <ul style="list-style-type: none"> • CP-IDLE timer expiry • Session Report with UPIR • Absolute Timer Expiry

RAN/NAS Cause IE

SMF receives the RAN/NAS Cause IE from access network in the GTP messages due to QoS flow termination or PDU session termination. SMF provides the received cause in the ranNasRelCauses attribute of the RuleReport to PCF. For more information about this cause, see the 3GPP TS 29.274 version 15.4.0.

The RAN/NAS Cause IE supports the following GTP messages:

- Create Bearer Response
- Update Bearer Response
- Delete Bearer Command
- Delete Session Request

Spec-Derived Cause Code Mapping

The SMF supports specification derived (TS 29.524) cause code mapping for 5G messages for UDM and PCF interfaces.

Table 6: Mapping from HTTP to 5GSM cause values—Request rejected by UDM due to N10 failures

HTTP Status Code on N10	Protocol or Application Error	5GSM Cause to UE
403 Forbidden	ROAMING_NOT_ALLOWED	Cause #29—User authentication or authorization failed
	DNN_NOT_ALLOWED	Cause #27—Missing or unknown DNN
404 Not Found	USER NOT FOUND	Cause #29—User authentication or authorization failed

Table 7: Mapping from HTTP to 5GSM cause values—Request rejected by PCF

HTTP Status Code on N7	Protocol or Application Error	5GSM Cause to UE
400 Bad Request	USER_UNKNOWN	Cause #29—User authentication or authorization failed
	ERROR_INITIAL_PARAMETERS	Cause #31—Request rejected, unspecified
	ERROR_TRIGGER_EVENT	Cause #31—Request rejected, unspecified
403 Forbidden	ERROR_TRAFFIC_MAPPING_INFO_REJECTED	Cause #29—User authentication or authorization failed
	ERROR_CONFLICTING_REQUEST	Cause #67—insufficient resources for specific slice and DNN
	POLICY_CONTEXT_DENIED	Cause #29—User authentication or authorization failed
	VALIDATION_CONDITION_NOT_MET	Cause #29—User authentication or authorization failed

Standards Compliance

The supported GTP cause codes comply with the following standards:

- 3GPP TS 29.274, Version 15.4.0
- 3GPP TS 29.524

Configuring GTP Cause Codes

This section describes how to configure cause-to-class mapping and class-to-cause mapping.

For source interface failures, the **cause-map-class** profile determines which **class-map-cause** profile must be applied on the corresponding target interface, only if the latter is configured under access profile. The respective CLI configurations send the user-defined cause values to the target interface based on the source interface failures and cause values. If the CLI commands are not configured, the target interface sends the spec-driven cause values as default values.

Configuring the GTP cause codes involves the following steps:

- [Cause to Class Mapping Configuration, on page 10](#)
 - [Configuring Cause-to-Class Map under cause-map-class Profile, on page 10](#)
 - [Configuring Cause-to-Class Map under Network-Element Profile, on page 10](#)
- [Class to Cause Mapping Configuration, on page 11](#)
 - [Configuring Class-to-Cause Map under class-map-cause Profile, on page 11](#)
 - [Configuring Class-to-Cause Map under Access Profile, on page 12](#)

Cause to Class Mapping Configuration

This section describes how to configure cause to class mapping in SMF.

Configuring Cause-to-Class Map under cause-map-class Profile

To configure cause-to-class mapping under the cause-map-class profile, use the following sample configuration:

```
config
  profile cause-map-class nf-type [ udm | pcf ] cmc_profile_name
    source { status-code httpv2_code cause cause_value } fail-class
failclass_string
  exit
```

NOTES:

- **profile cause-map-class nf-type [udm | pcf] cmc_profile_name**: Specify the NF profile name to configure the cause-map-class profile.
- **source { status-code httpv2_code cause cause_value } fail-class failclass_string**
 - **status-code httpv2_code**: Specify the HTTPv2 status code of the source interface.
 - **cause cause_value**: Specify the cause value as a string.
 - **fail-class failclass_string**: Specify the failure class as a string.
- The **profile cause-map-class** is associated to the network-element profile.
- The **status-code** and **cause** keywords are optional. If both are configured, then the corresponding **fail-class** is given higher priority followed by **status-code** and **cause**.

Example

The following is an example of the UDM interface configuration:

```
profile cause-map-class nf-type udm UDM-CMC
  source status-code 403 cause DNN_NOT_ALLOWED fail-class congestion
```

Configuring Cause-to-Class Map under Network-Element Profile

To configure cause-to-class mapping under the network-element profile, use the following sample configuration:

```
config
  profile network-element [ udm | pcf ] nfprofile_name
    cause-map-class-profile cmcp_name
  exit
```

NOTES:

- **profile network-element [udm | pcf] nfprofile_name**: Specify the NF profile name to configure the network-element profile.
- **cause-map-class-profile cmcp_name**: Specify the cause-to-class map profile name.

Example

The following is an example of the UDM interface configuration:

```
profile network-element udm nfprf-udm
  cause-map-class UDM-CMC
```

Sample Configuration

```
[smf] smf# show running-config profile cause-map-class
profile cause-map-class nf-type udm CMC-UDM-1
  source status-code 500 cause CAUSE2 fail-class failClass2
  source status-code 500 cause CAUSE3 fail-class failClass3
  source status-code 501 cause CAUSE1 fail-class failClass1
  source status-code 502 cause CAUSE2 fail-class failClass1
  source status-code 504 cause CAUSE4 fail-class failClass4
  source status-code 505 cause CAUSE4 fail-class failClass5
exit
profile cause-map-class nf-type udm CMC-UDM-2
  source status-code 501 cause CAUSE1 fail-class failClass6
  source status-code 501 cause any fail-class failClass6
  source status-code 502 cause CAUSE1 fail-class failClass6
  source status-code 502 cause CAUSE2 fail-class failClass6
  source status-code 502 cause any fail-class failClass6
  source status-code any cause CAUSE1 fail-class failClass6
  source status-code any cause CAUSE2 fail-class failClass6
exit
profile cause-map-class nf-type udm CMC-UDM-3
  source status-code 504 cause CAUSE4 fail-class failClass4
  source status-code 505 cause CAUSE4 fail-class failClass5
exit
profile cause-map-class nf-type pcf PCF-CMC-1
  source status-code 500 cause CAUSE2 fail-class failClass2
  source status-code 500 cause CAUSE3 fail-class failClass3
  source status-code 501 cause CAUSE1 fail-class failClass1
  source status-code 502 cause CAUSE2 fail-class failClass1
  source status-code 504 cause CAUSE4 fail-class failClass4
  source status-code 505 cause CAUSE4 fail-class failClass5
exit
profile cause-map-class nf-type pcf PCF-CMC-2
  source status-code 500 cause any fail-class failClass2
  source status-code 501 cause any fail-class failClass3
  source status-code any cause CAUSE2 fail-class failClass2
  source status-code any cause CAUSE3 fail-class failClass3
exit
[smf] smf#
```

Class to Cause Mapping Configuration

This section describes how to configure class to cause mapping in SMF.

Configuring Class-to-Cause Map under class-map-cause Profile

To configure class-to-cause mapping under the class-map-cause profile, use the following sample configuration:

```
config
  profile class-map-cause cmc_profile_name
    fail-class failclass_string
      target n1 { status-code httpv2_code cause cause_value } | [ n1 | n2
| gtp ] { cause cause_value }
    exit
```

NOTES:

- **profile class-map-cause** *cmc_profile_name*: Specify the profile name to configure class-map-cause.
- **fail-class** *failclass_string*: Specify the failure class as a string.

- **target n1** { **status-code** *httpv2_code* **cause** *cause_value* } [**n1** | **n2** | **gtp**] { **cause** *cause_value* }:
 - **target**: Specify the target interface.
 - **status-code** *httpv2_code*: Specify the HTTPv2 status code for the target interface.
 - **cause** *cause_value*: Specify the cause value for the target interface.
- The **profile class-map-cause** is associated to the access profile.
- The **status-code** keyword is not applicable to the GTP, N1, and N2 interfaces.

Example

The following is an example of the CLI configuration:

```
profile class-map-cause cmc1
  fail-class congestion
  target gtp cause 72
```

Configuring Class-to-Cause Map under Access Profile

To configure class-to-cause mapping under the access profile, use the following sample configuration:

```
config
  profile access access_profile_name
    [ gtpc | n1 | n2 | n11 ] class-map-cause-profile cmc_profile_name
  exit
```

NOTES:

- **profile access** *access_profile_name*: Specify the profile name to configure the access profile.
- **class-map-cause-profile** *cmc_profile_name*: Specify the profile name to configure the class-to-cause map profile.

Example

The following is an example of the CLI configuration:

```
profile access access1
  n11 class-map-cause cmc1
```

Sample Configuration

```
[smf] smf# show running-config profile class-map-cause
profile class-map-cause CMC
  fail-class failClass1
  target n11 status-code 403 cause CA1
  target n1 cause CA_N1
  target n2 cause CA_n2
  target gtp cause 75
exit
fail-class failClass2
  target n11 status-code 402 cause CAUSE4
  target n1 cause CAUSE3
  target n2 cause CAUSE2
  target gtp cause 95
exit
```

```
exit
[smf] smf#
```

GTP Cause Code Handling OAM Support

This section describes operations, administration, and maintenance information for this feature.

Statistics Support

The source interface failures support the following disconnect reasons:

- `disc_new_pdn_type_due_to_single_addr_bearer_only`—The number of Create Session Request failures with cause value "New PDN type due to single address bearer only" in Create Session Response.
- `disc_new_pdn_type_due_to_network_preference`—The number of Create Session Request failures with cause value "New PDN type due to network preference" in Create Session Response.
- `disc_pdnsetup_dnn_missing_or_unknown`—The number of Create Session Request failures with cause value "Missing or unknown APN" in Create Session Response.
- `disc_request_timeout_at_originating_entry`—The number of Create Session Request failures with cause value "Timed Out Request" in Create Session Response.

GTPv2 IE and Cause Codes

Feature Description

This section describes the GPRS Tunneling Protocol, Version 2 (GTPv2) IEs and cause codes for 4G and 5G procedures.

Cause Source Errors

The Cause Source (CS) bit supports the following cause values in Create Session Response, Modify Bearer Response, Modify Bearer Failure Indication (MBFI), or Delete Bearer Failure Indication (DBFI).

Table 8: CS Bit Causes

Cause Value	Scenario
Context Not Found	When the subscriber is not present in SMF and receives Create Session Response with handover indication, the SMF sends this cause.
Missing Or Unknown APN	When Create Session Response receives missing or unknown APN, the SMF sends this cause.
DBFI with Context Not Found	When the subscriber is not present in SMF and receives Delete Bearer Command, the SMF sends this cause.
Delete Session Response with Context Not Found	When the subscriber is not present in SMF and receives a Delete Session Request in old TEID, the SMF sends this cause.

Bearer Context IE Errors

The Bearer Context IE Error (BCE) bit supports the following cause values in Delete Session Response, Modify Bearer Response, Modify Bearer Failure Indication (MBFI), or Delete Bearer Failure Indication (DBFI).

Table 9: BCE Bit Causes

Cause Value	SMF Behavior or Scenario
MBFI with Context Not Found	When SMF receives Modify Bearer Request with a wrong EBI in bearer context, the SMF sends this cause.
DBFI with Context Not Found	When SMF receives Delete Bearer Command with a wrong EBI in bearer context, the SMF sends this cause.

Remote Node Errors

SMF supports the following remote node errors:

- Context not found
- Missing or unknown APN
- PduSessionType
- Mandatory IE missing
- Malformed message errors

Statistics Support

This feature supports the following statistics related to GTPC messages:

smf_gtpc_msg_stats

Description: Stats for GTPC interface messages

Sample Query: 'smf_gtpc_msg_stats{message_type="modify_bearer_request"}'

Labels:

- Label: `message_type`
Label Description: GTPC Message Type
Example: `modify_bearer_request`, `delete_bearer_request`, `delete_session_request`
- Label: `status`
Label Description: GTPC message status
Example: `attempted`, `success`, `failures`
- Label: `reason`
Label Description: The reason associated with the failure
Example: `ipc_failed`, `sgw_failure`, `EGTP_CAUSE_LOCAL_DETACH`, `EGTP_CAUSE_RAT_CHANGED_FROM_3GPP_TO_NON_3GPP`,

EGTP_CAUSE_COMPLETE_DETACH, EGTP_CAUSE_ISR_DEACTIVATION,
EGTP_CAUSE_ERROR_IND_RCVD_RNC_ENODE, EGTP_CAUSE_IMSI_DETACH_ONLY,
EGTP_CAUSE_REACTIVATION_REQUESTED,
EGTP_CAUSE_PDN_RECONNECTION_TO_THIS_APN_DISALLOWED,
EGTP_CAUSE_ACCESS_CHANGED_FROM_NON_3GPP_TO_3GPP,
EGTP_CAUSE_PDN_CONN_INACTIVITY_TIMER_EXPIRED,
EGTP_CAUSE_PGW_NOT_RESPONDING, EGTP_CAUSE_NETWORK_FAILURE,
EGTP_CAUSE_QOS_PARAMETER_MISMATCH, EGTP_CAUSE_REQ_ACCEPTED,
EGTP_CAUSE_REQ_ACCEPTED_PARTIALLY,
EGTP_CAUSE_NEW_PDN_TYPE_NETWORK_PREFERENCE,
EGTP_CAUSE_NEW_PDN_TYPE_SINGLE_ADDR_BEARER_ONLY,
EGTP_CAUSE_CONTEXT_NOT_FOUND, EGTP_CAUSE_INVALID_MESSAGE_FORMAT,
EGTP_CAUSE_VERSION_NOT_SUPPORTED_BY_NEXT_PEER,
EGTP_CAUSE_INVALID_LENGTH, EGTP_CAUSE_SERVICE_NOT_SUPPORTED,
EGTP_CAUSE_MANDATORY_IE_INCORRECT, EGTP_CAUSE_MANDATORY_IE_MISSING,
EGTP_CAUSE_SYSTEM_FAILURE, EGTP_CAUSE_NO_RESOURCES_AVAILABLE,
EGTP_CAUSE_SEMANTIC_ERROR_IN_TFT_OPERATION,
EGTP_CAUSE_SYNTACTIC_ERROR_IN_TFT_OPERATION,
EGTP_CAUSE_SEMANTIC_ERROR_IN_PKT_FILTERS,
EGTP_CAUSE_SYNTACTIC_ERROR_IN_PKT_FILTERS,
EGTP_CAUSE_MISSING_OR_UNKNOWN_APN, EGTP_CAUSE_UNEXPECTED_REPEATED_IE,
EGTP_CAUSE_GRE_KEY_NOT_FOUND, EGTP_CAUSE_REALLOCATION_FAILURE,
EGTP_CAUSE_DENIED_IN_RAT, EGTP_CAUSE_PREFERRED_PDN_TYPE_UNSUPPORTED,
EGTP_CAUSE_ALL_DYNAMIC_ADDR_OCCUPIED,
EGTP_CAUSE_UE_CTX_WO_TFT_ALREADY_ACTIVATED,
EGTP_CAUSE_PROTOCOL_TYPE_NOT_SUPPORTED, EGTP_CAUSE_UE_NOT_RESPONDING,
EGTP_CAUSE_UE_REFUSES, EGTP_CAUSE_SERVICE_DENIED,
EGTP_CAUSE_UNABLE_TO_PAGE_UE, EGTP_CAUSE_NO_MEMORY_AVAILABLE,
EGTP_CAUSE_USER_AUTHENTICATION_FAILED,
EGTP_CAUSE_APN_DENIED_NO_SUBSCRIPTION, EGTP_CAUSE_REQUEST_REJECTED,
EGTP_CAUSE_PTMSI_SIGNATURE_MISMATCH, EGTP_CAUSE_IMSI_IMEI_NOT_KNOWN,
EGTP_CAUSE_SEMANTIC_ERROR_IN_TAD_OPERATION,
EGTP_CAUSE_SYNTACTIC_ERROR_IN_TAD_OPERATION,
EGTP_CAUSE_RESERVED_MESSAGE_VALUE_RECEIVED,
EGTP_CAUSE_PEER_NOT_RESPONDING,
EGTP_CAUSE_COLLISION_WITH_NETWORK_INIT_REQUEST,
EGTP_CAUSE_UNABLE_TO_PAGE_UE_DUE_TO_SUSPENSION,
EGTP_CAUSE_CONDITIONAL_IE_MISSING, EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE,
EGTP_CAUSE_INVALID_LENGTH_WITH_PIGGYBACK_MSG,
EGTP_CAUSE_DATA_FORWARDING_NOT_SUPPORTED,
EGTP_CAUSE_INVALID_REPLY_FROM_REMOTE_PEER,
EGTP_CAUSE_FALLBACK_TO_GTPV1, EGTP_CAUSE_INVALID_PEER,
EGTP_CAUSE_TEMP_REJECTED_DUE_TO_HANDOVER_IN_PROGRESS,
EGTP_CAUSE_REQ_REJECTED_FOR_PMIPv6_REASON, EGTP_CAUSE_APN_CONGESTION,
EGTP_CAUSE_BEARER_HANDLING_NOT_SUPPORTED,
EGTP_CAUSE_UE_ALREADY_REATTACHED,
EGTP_CAUSE_MULTI_PDN_CONNECTION_FOR_APN_NOT_ALLOWED,
EGTP_CAUSE_MME_SGSN_REFUSES_DUE_TO_VPLMN_POLICY,
EGTP_CAUSE_GTPC_ENTITY_CONGESTION,
EGTP_CAUSE_TARGET_ACCESS_RESTRICTED_FOR_THE_SUBSCRIBER,
EGTP_CAUSE_UE_TEMP_NOT_REACHABLE_DUE_TO_POWER_SAVING,

EGTP_CAUSE_RELOC_FAILURE_DUE_TO_NAS_MSG_REDIRECTION,
 EGTP_CAUSE_MISSING_TIMESTAMP_OPTION,
 EGTP_CAUSE_MULTIPLE_HNP_NOT_ALLOWED, EGTP_CAUSE_SN_MALFORMED_MSG,
 EGTP_CAUSE_INT_TIMEOUT

- Label: qos_5qi

Label Description: 5Qi applicable for the QoS flow

Example: 1, 2, 5

- Label: rat_type

Label Description: Type of the radio access associated with the request

Example: EUTRA, NR, WLAN, rat_type_unknown

- Label: smf_current_procedure

Label Description: Current Procedure Name for Message Level Stats

Example: nr_to_untrusted_wifi_handover, eps_fb_ded_brr, PdnDisconnectProcedure,
 enb_to_untrusted_wifi_handover, pcf_req_ded_brr_create, pcf_req_ded_brr_delete, pcf_req_ded_brr_mod,
 smf_initiated_pdn_detach, untrusted_wifi_to_enb_handover, upf_sess_report_srir_sess_rel,
 utn3gpp_to_5g_handover

N1/NAS Interface

The N1 interface is the reference point between the User Equipment (UE) and the Access and Mobility Management Function (AMF). This interface is used to transfer UE information, which is related to connection, mobility and sessions, to the AMF.

For session management, PDU sessions are established upon UE request, modified upon UE and 5GC request, and released upon UE and 5GC request through the NAS SM signalling. This signalling is exchanged over N1 interface between the UE and the SMF.

NAS Messages Compliance with Invalid Protocol Data Handling

Feature Description

The SMF is NAS messages compliant with invalid protocol data handling as defined in 3GPP TS 24.501 with this release.

How it Works

The NAS messages compliance with invalid protocol data handling feature works as follows:

- SMF ignores a NAS message that is too short to contain a complete message type information element (IE).
- SMF ignores a NAS message that is longer than the maximum limit as defined in the 3GPP specification.
- SMF ignores the IEs that are unknown in a NAS message.
- SMF ignores the IEs with incorrect sequence in a NAS message.
- If an information element with the T, TV, TLV, or TLV-E format repeats in a message with the unspecified repetition of the IE, then the SMF handles only the contents of the information element that appears first. In addition, SMF ignores the subsequent repetitions of the information element.

- SMF considers any optional IE with incorrect syntax in a message as an unavailable message.
- The network ignores any of the following messages and returns a status message with cause #100 “conditional IE error”:
 - When SMF receives a NAS message with a missing conditional IE error
 - When SMF receives an unexpected conditional IE error
 - When SMF receives a message with at least one syntactically incorrect conditional IE

NAS Messages Compliance and Invalid Protocol Data Handling

SMF complies with the following sections of the 3GPP specifications for the NAS messages compliance with invalid protocol data handling feature:

Message Too Short

SMF discards a NAS message whose size doesn't meet the minimum limit.

Following table lists the minimum limit for NAS messages that SMF receives from UE:

Table 10: Minimum Limit for NAS Messages

Number	NAS Message	Minimum Limit
1	PDU Session Establishment Request	6 octets
2	PDU Session Authentication Complete	4 octets
3	PDU Session Modification Request	4 octets
4	PDU Session Modification Complete	4 octets
5	PDU Session Modification Command Reject	5 octets
6	PDU Session Release Request	4 octets
7	PDU Session Release Complete	4 octets

Message Too Long

SMF discards a NAS message whose size doesn't meet the maximum limit.

The maximum size of a NAS message for NR that is connected to 5G Core Network is 9000 bytes.

Unknown IEs

SMF ignores unknown IEs in a NAS message.



Note SMF handles only the IEs relevant to a specific NAS message type. SMF ignores other IEs that are unknown to the message type.

Out of Sequence IEs

SMF ignores IEs that have incorrect sequence of mandatory IEs in a NAS message.

Repeated IEs

Sometimes SMF can receive an IE multiple times in a NAS message with no information on the repetition of IE. In such a case, SMF considers only the first occurrence of the repeated IE and ignores all the subsequent occurrences of the IE.

Syntactically Incorrect IEs

SMF ignores syntactically incorrect optional IEs in a NAS message.

Missing or Unexpected Conditional IEs

SMF ignores the received NAS message with the following conditional IE errors:

- Missing expected conditional IE
- Unexpected conditional IE
- Syntactically incorrect conditional IE

Standards Compliance

The NAS messages compliance with invalid protocol data handling feature complies with the following standards:

- *3GPP TS 24.501 – 5G; Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3*
- *3GPP TS 38.323 – 5G; NR; Packet Data Convergence Protocol (PDCP)*

5GSM Cause Code Handling

Feature Description

The SMF or vSMF supports 5G Session Management (5GSM) cause handling for the UE-initiated and network-initiated procedures.

The supported procedures are:

- PDU Session Establishment
- PDU Session Modification
- PDU Session Release

PDU Session Establishment Reject Cause Values

If the connectivity with the requested data network (DN) is rejected by the network, SMF sets the 5GSM cause IE of the PDU Session Establishment Reject message to indicate the reason for rejecting the PDU Session Establishment procedure.

The following table describes the supported 5GSM causes in the PDU Session Establishment Reject message.

Table 11: 5GSM Causes—PDU Session Establishment Reject

5GSM Reject Cause	SMF Behavior
Cause #26 – Insufficient Resources	The SMF includes this cause when it receives N2SmInfoType with "PDU_RES_SETUP_FAIL" along with any of the following N2 causes: <ul style="list-style-type: none"> • RadioNetwork/Radio_resources_not_available • RadioNetwork/Failure_in_the_radio_interface_procedure • Misc/Not_enough_user_plane_processing_resources
Cause #27 – Missing or unknown DNN	The SMF includes this cause when the DNN is not available in SmContextCreateData because the DNN is required and not configured in SMF.
Cause #28 – Unknown PDU session type	The SMF includes this cause when the PDU Session Establishment Request message includes a PDU session type that is not supported by SMF.
Cause #29 – User authentication or authorization failed	The SMF includes this cause when the DNN authentication of the UE was unsuccessful (RADIUS Authentication Timeout).
Cause #32 – Service option not supported	The SMF includes this cause when the validation of received S-NSSAI fails against the allowed list of S-NSSAI.
Cause #33 – Requested service option not subscribed	The SMF includes this cause when the UE requests a service option for which it has no subscription.
Cause #38 – Network failure	The SMF includes this cause when the requested service was rejected due to an error in the network. This includes any internal failures or no response from any external NF during the PDN-setup procedure.
Cause #54 – PDU session does not exist	The SMF includes this cause when it does not have any information about the PDU session which is requested by the UE to transfer between 3GPP access and non-3GPP access or from the EPS to the 5GS.
Cause #70 – Missing or unknown DNN in a slice	The SMF includes this cause when the slice configuration is present but the requested DNN is not configured under the slice in the SMF.
Protocol errors	

5GSM Reject Cause	SMF Behavior
Cause #95 – Semantically incorrect message	<p>This 5GSM cause reports receipt of a message with semantically incorrect content.</p> <p>Important The SMF also sends this cause for mandatory parameters with non-semantical errors such as PDU Session Identity and Procedure Transaction Identity.</p>

PDU Session Modification Reject

If the SMF does not accept the request to modify the PDU session, it sets the 5GSM cause IE of the PDU Session Modification Reject message to indicate the reason for rejecting the PDU session modification procedure.

The following table describes the supported 5GSM causes in the PDU Session Modification Reject message.

Table 12: 5GSM Causes—PDU Session Modification Reject

5GSM Reject Cause	SMF Behavior
Cause #43 – Invalid PDU session identity	The SMF sends this cause when SMF does not have the session.
Protocol errors	
Cause #95 – Semantically incorrect message	<p>This 5GSM cause reports receipt of a message with semantically incorrect content.</p> <p>Important The SMF also sends this cause for mandatory parameters with non-semantical errors such as PDU Session Identity and Procedure Transaction Identity.</p>

PDU Session Release Reject

If the SMF does not accept the request to release the PDU session, SMF sets the 5GSM Cause IE of the PDU Session Release Reject message to indicate the reason for rejecting the PDU session release.

The SMF supports the following causes in the PDU Session Release Reject message.

Table 13: 5GSM Causes—PDU Session Release Reject

5GSM Reject Cause	SMF Behavior
Cause #43 – Invalid PDU session identity	The SMF supports this cause when SMF does not have the PDU session.
Protocol errors	

5GSM Reject Cause	SMF Behavior
Cause #95 – Semantically incorrect message	This 5GSM cause reports receipt of a message with semantically incorrect content. Important The SMF also sends this cause for mandatory parameters with non-semantical errors such as PDU Session Identity and Procedure Transaction Identity.

PDU Session Release Request

To initiate the UE-requested PDU Session Release procedure, UE sends the PDU Session Release Request message with the 5GSM Cause IE to indicate the reason for releasing the PDU session.

The SMF supports the following causes in the PDU Session Release Request message.

Reject Cause / 5GSM Cause	SMF Behavior
Cause #36 – regular deactivation	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #41 – Semantic error in the TFT operation	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #42 – Syntactical error in the TFT operation	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #44 – Semantic errors in packet filter(s)	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #45 – Syntactical errors in packet filter(s)	The SMF retains the statistics based on the cause and continues with the Release procedure.

PDU Session Modification Command Reject

If the UE rejects the PDU-Session-Modification-Command, it sets the 5GSM cause IE of the PDU Session Modification Reject message to indicate the reason for rejecting the PDU session modification.

The SMF supports the following 5GSM causes.

Table 14: Supported PDU Session Modification Reject messages

5GSM Cause	SMF Behavior
Cause #26 – insufficient resources	The SMF retains the statistics based on the cause.
Cause #43 – Invalid PDU session identity	The SMF retains the statistics based on the cause and releases the existing PDU session.
Cause #44 – Semantic error in packet filter(s)	The SMF retains the statistics based on the cause.
Cause #45 – Syntactical error in packet filter(s)	The SMF retains the statistics based on the cause.
Cause #83 – Semantic error in the QoS operation	The SMF retains the statistics based on the cause.

5GSM Cause	SMF Behavior
Cause #85 – Syntactical error in the QoS operation	The SMF retains the statistics based on the cause.

How it Works

The SMF supports 5GSM cause handling for the PDU Session Establishment, PDU Session Modification, and PDU Session Release procedures. An appropriate SM cause will be sent through the N1 message to the UE.

The vSMF sends an indication toward hSMF to release the PDU session and associated resources for all session cleanups in the preceding scenarios.

Standards Compliance

The 5GSM Cause Handling feature complies with *3GPP TS 24.501 Release 15—Non-Access-Stratum (NAS) protocol for 5G System (5GS), Stage 3*.

5GSM Cause Handling OAM

This section describes operations, administration, and maintenance information for this feature.

Statistics

The 5GSM Cause Handling feature supports the following statistics to track the number of failures based on the 5GSM cause.

SMF N1 Message Stats

PDU-Session-Establishment-Reject:

- NETWORK_FAILURE: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "NETWORK_FAILURE".
- UNKNOWN_PDU_SESSION_TYPE: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "UNKNOWN_PDU_SESSION_TYPE".
- USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED".
- REQUESTED_SERVICE_OPTION_NOT_SUBSCRIBED: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "REQUESTED_SERVICE_OPTION_NOT_SUBSCRIBED".
- MISSING_OR_UNKNOWN_DNN: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "MISSING_OR_UNKNOWN_DNN".
- SERVICE_OPTION_NOT_SUPPORTED: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "SERVICE_OPTION_NOT_SUPPORTED".
- INSUFFICIENT_RESOURCES: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "INSUFFICIENT_RESOURCES".
- MISSING_OR_UNKNOWN_DNN_IN_A_SLICE: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "MISSING_OR_UNKNOWN_DNN_IN_A_SLICE".

- **PDU_SESSION_DOES_NOT_EXIST**: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "PDU_SESSION_DOES_NOT_EXIST".

PDU-Session-Modification-Reject:

- **INVALID_PDU_SESSION_IDENTITY**: The number of PDU-Session-Modification-Reject messages sent from SMF with N1 Cause "INVALID_PDU_SESSION_IDENTITY".

PDU-Session-Release-Reject:

- **INVALID_PDU_SESSION_IDENTITY**: The number of PDU-Session-Release-Reject messages sent from SMF with N1 Cause "INVALID_PDU_SESSION_IDENTITY".

PDU-Session-Release-Request:

- **REGULAR_DEACTIVATION**: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "REGULAR_DEACTIVATION".
- **SEMANTIC_ERRORS_IN_PACKET_FILTER**: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SEMANTIC_ERRORS_IN_PACKET_FILTER".
- **SYNTACTICAL_ERROR_IN_PACKET_FILTER**: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SYNTACTICAL_ERROR_IN_PACKET_FILTER".
- **SEMANTIC_ERROR_IN_THE_TFT_OPERATION**: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SEMANTIC_ERROR_IN_THE_TFT_OPERATION".
- **SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION**: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION".

PDU-Session-Modification-Command-Reject:

- **INSUFFICIENT_RESOURCES**: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "INSUFFICIENT_RESOURCES".
- **INVALID_PDU_SESSION_IDENTITY**: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "INVALID_PDU_SESSION_IDENTITY".
- **SEMANTIC_ERRORS_IN_PACKET_FILTER**: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SEMANTIC_ERRORS_IN_PACKET_FILTER".
- **SYNTACTICAL_ERROR_IN_PACKET_FILTER**: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SYNTACTICAL_ERROR_IN_PACKET_FILTER".
- **SEMANTIC_ERROR_IN_THE_QOS_OPERATION**: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SEMANTIC_ERROR_IN_THE_QOS_OPERATION".
- **SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION**: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION".

N2/NGAP Interface

The N2 interface is the reference point between the RAN and the AMF. This interface connects the gNodeB to the AMF and is required due to Control and User Plane Separation (CUPS).

The N2 interface is needed because before accessing a service, the UE must be connected to the network. SMF handles the session control and the AMF handles the UE context. So, before initiating traffic or session, information, such as UE context, is required.

The N2 interface handles control-plane signalling. So, SMF uses N2 to generate and validate user traffic.

N4 Interface

The SMF sends messages to the User Plane Function (UPF) over the N4 interface by using the Packet Forwarding Control Protocol (PFCP). SMF performs various session management procedures using the N4 interface. An example of a management procedure is when UPF identifies and transports user plane traffic information and flow based on session management data that it receives from the SMF.

N7 Interface

The N7 interface is the reference point between the SMF and the Policy Control Function (PCF) during session establishment or modification.

PCF uses the policy control for session management. This network function implements N7 interface to trigger session management policies towards SMF. SMF controls the User plane Function (UPF) and translates policies that it receives from PCF to the information that the UPF understands and then forwards it to the UPF.

Error Handling with HTTP Error Codes

Feature Description

SMF supports error responses and the related HTTP error codes for the SM Policy Update Notify service towards PCF with this release. For this feature, SMF complies with 3GPP TS 29.512, section 4.2.3.2—SM Policy Association Update request.

How it Works

SMF responds with the error details and HTTP error codes to the SM Policy Update Notify service from PCF.

Call Flows

This section describes the call flow of the SM Policy Update Notify service from PCF.

Figure 1: SM Policy Update Notify Service from PCF

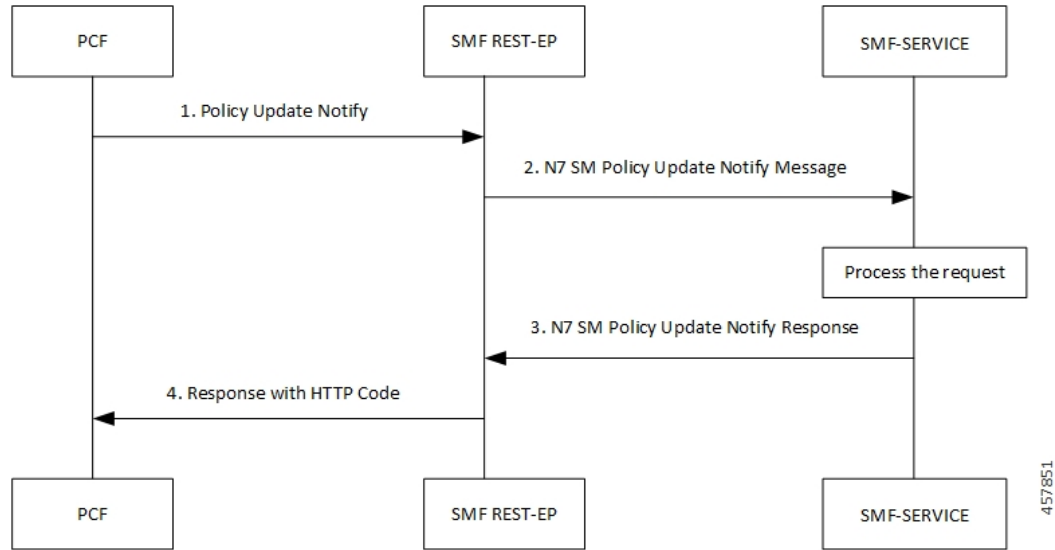


Table 15: SM Policy Update Notify Service from PCF Call Flow

Step	Description
1	PCF sends the Policy Update Notify request to SMF REST-EP.
2	SMF REST-EP sends the N7 SM Policy Update Notify message to SMF-service for processing.
3	SMF-service processes the request and sends a response with either success details or failure details to PCF.
4	SMF-RESTEP processes a response with HTTP codes and the required data structures, and then sends the response to PCF.

SMF Error Handling

SMF handles the HTTP error codes towards PCF through the following validations:

- SMF handles the RuleStatus enumeration in the RuleReport data structure. This data structure works on the following guidelines:
 - Validate the installed or activated Policy and Charging Control (PCC) rule for a PDU session. If the validation fails, the RuleStatus enumeration shows the configuration as "inactive".
 - Validate the updated PCC rule in a PDU session. If the validation fails, the RuleStatus enumeration shows the configuration as "active".
- SMF handles the RuleStatus enumeration in the SessRuleReport data structure. This data structure works on the following guidelines:
 - Validate that an installed or activated Session Rule exists for PDU session. If the validation fails, then the SessionRuleStatus attribute shows the configuration as "inactive".

- Validate that the updated Session Rule exists after activation or installation in a PDU session. If the validation fails, then the SessRuleStatus attribute shows the configuration as "active".
- SMF handles the cause by using the FailureCause enumeration in ProblemDetails when a PCC rule fails due to validation.
 - Use PCC_RULE_EVENT for PCF to retry connection with SMF. You can view the error details in the "InvalidParams" attribute.
- SMF handles the cause by using the FailureCause enumeration in ProblemDetails when a SessionRule fails due to validation.
 - Use RULE_PERMANENT_ERROR for PCF to retry connection with SMF. You can view the error details in the "InvalidParams" attribute.
- SMF handles SessionRuleFailureCode in the SessionRuleReport data structure, which works on the following guideline:
 - Use only UNSUCC_QOS_VAL as the supported value for this release.
- SMF handles SessionRuleFailureCode in the SessionRuleReport data structure, which works on the following guideline:
 - Use UNSUCC_QOS_VAL as the supported value.
- SMF supports the ProblemDetails JSON object to show error details in the HTTP response body. With this object, the SMF service includes a "Content-Type" header field configured to "application/problem+json".

Error Codes

Following table lists the error codes that SMF uses for error handling:

Table 16: Error Codes with Details

Number	Enum	Details	SMF Support
1	UNK_RULE_ID	Indicate that the preprovisioned PCC rule isn't activated. This error occurs when SMF has no information on the PCC rule identifier.	Yes
2	RA_GR_ERR	Indicate that the PCC rule isn't activated or enforced. This error occurs when the PCC rule referring to the specified Rating Group, in the Charging Data policy decision, is unknown or invalid.	Yes

Number	Enum	Details	SMF Support
3	SER_ID_ERR	Indicate that the PCC rule isn't activated or enforced. This error occurs when PCC rule referring to the specified service identifier, in the Charging Data policy decision, is invalid, unknown, or not applicable to the service being charged.	Yes
4	NF_MAL	Indicate that the PCC rule isn't installed, activated, or enforced due to SMF or UPF functionality issues. The PCC rule installation is for the rules provisioned from PCF. The PCC rule activation is for the rules predefined in SMF. The PCC rule enforcement is for the installed rules.	No
5	RES_LIM	Indicate that the PCC rule isn't installed, activated, or enforced due to limitation of resources at the SMF or UPF.	No
6	MAX_NR_QoS_FLOW	Indicate that a PDU session has reached the maximum number of QoS flows.	Yes
7	MISS_FLOW_INFO	Indicate that the PCC rule isn't installed. This error occurs when PCF fails to specify either the "flowInfos" attribute or the "appId" attribute in the PccRule data structure during the first installation request of the PCC rule.	Yes
8	RES_ALLO_FAIL	Indicate that the PCC rule isn't installed or maintained. This error occurs due to the QoS flow establishment, modification failure, or release of the QoS flow.	Yes
9	UNSUCC_QOS_VAL	Indicate QoS validation failure or when the Guaranteed Bandwidth is more than the maximum requested bandwidth.	Yes
10	INCOR_FLOW_INFO	Indicate that the PCC rule isn't installed or modified at SMF. This error occurs when the network doesn't support the flow information, such as IP address or an IPv6 prefix doesn't correspond to the applicable IP version for the PDU session.	Yes

Number	Enum	Details	SMF Support
11	PS_TO_CS_HAN	Indicate that the PCC rule isn't maintained due to packet switched (PS) to circuit switched (CS) handover.	No
12	APP_ID_ERR	Indicate that the PCC rule isn't installed or enforced. This error occurs due to invalid, unknown, or nonapplicable application identifier that an application requires for detection.	No
13	NO_QOS_FLOW_BOUND	Indicates that no QoS flow exists for the SMF to associate the PCC rules to.	Yes
14	FILTER_RES	Indicates that the SMF is unable to handle the flow information in "flowInfos". This error occurs when the restrictions defined in subclause 5.4.2 of 3GPP TS 29.212 [23] aren't met.	Yes
15	MISS_REDI_SER_ADDR	Indicate that the PCC rule isn't installed or enforced at the SMF. This error occurs when PCF doesn't provide a valid redirect server address in the Traffic Control Data policy decision for the PCC rule and no pre-configured redirection address for this PCC rule exists at the SMF.	No
16	CM_END_USER_SER_DENIED	Indicate that the charging system denied the service request due to service restrictions. For example, termination of rating group or end-user related limitations, such as the end-user account doesn't include the requested service.	No
17	CM_CREDIT_CON_NOT_APP	Indicate that the charging system determined that the service can be granted to the end user. However, no credit control is applicable for the service. For example, a service is free of charge or available for offline charging.	No

Number	Enum	Details	SMF Support
18	CM_AUTH_REJ	Indicate that the charging system denied the service request to terminate the service for which an end user requested a credit.	No
19	CM_USER_UNK	Indicate that an end-user information is unavailable in the charging system.	No
20	CM_RAT_FAILED	Indicate that the charging system can't rate the service request. This error occurs due to insufficient rating input, incorrect AVP combination, or because of an unrecognized or unsupported attribute value in the rating.	No
21	UE_STA_SUSP	Indicates that the UE is in the suspended state. Note This error is applicable only to the interworking scenario, as defined in Annex B of the 3GPP specification.	No

N10 Interface

During session establishment or modification, the SMF communicates with the PCF over the N7 interface and the subscriber profile information that is stored in the Unified Data Management (UDM) function on the N10 interface.

N11 Interface

The N11 interface is the reference point between the Access and Mobility Management Function (AMF) and SMF.

To request a new session, both the UE and the gNB use the Next Generation Application Protocol (NGAP) to carry Non Access Stratum (NAS) messages across the N1 or N2 interface. AMF receives these requests and handles the connectivity and mobility management. Then, the AMF forwards the session management related requirements over the N11 interface to the SMF. The AMF identifies the SMF that can handle the connection request by querying the Network Repository Function (NRF).

The messages that SMF receives over the N11 interface are the requests to add, modify, or delete a PDU session across the user plane.

ProblemDetails JSON Object

Feature Description

SMF supports sending and receiving the ProblemDetails JSON object on the N11 interface and supports roaming.

An application error can prevent the SMF service, acting as an HTTP server, from completing the HTTP request. In this case, the SMF service maps the application error to the similar 4xx or 5xx HTTP status.

An HTTP status code determines the cause of the error. However, sometimes these status codes don't have adequate information about an error. In this case, the SMF service acting as the HTTP server provides more application-related error information to the SMF service acting as an HTTP client. This SMF service provides the additional information by including the representation of "ProblemDetails" data structure in the response body.

3GPP specification defines JSON as one of the document formats. HTTP APIs reuse this format to identify various problem types based on the requirement.

The ProblemDetails structure specified for N11 interface is sent on the N16 interface for roaming call flows on hSMF. After receiving ProblemDetails from hSMF, the vSMF rejects the corresponding message from AMF and saves the ProblemDetails that vSMF receives from hSMF.

Supported Attributes

For this feature, SMF supports the following attributes:

- **status**—Specifies the HTTP status code for the occurrence of a problem. The HTTP status has the format of 4xx and 5xx, such as 403 and 504.
- **cause**—Specifies a machine-readable application error cause based on the occurrence of a problem. The 5G core SBI API specifications define the application error causes. As per the specifications, this attribute uses the UPPER_WITH_UNDERSCORE case format, such as UNSPECIFIED_NF_FAILURE", "DNN_NOT_SUPPORTED.
- **title**—Provides the summary of the problem type. This attribute remains same from one occurrence of the problem to another occurrence. This attribute includes summary, such as invalid parameters, network failure, and mandatory, optional, or conditional IE is missing.
- **detail**—Provides the human-readable information that is specific to the occurrence of the problem. This attribute includes information, such as UDM registration failure, UDM subscription failure, and sending of invalid parameter in SM Context Create.



Note

- For this feature, SMF supports the title and detail attributes.
- For this feature, SMF does not support the invalidParams attribute.

How it Works

This section describes how this feature works.

If a response includes a payload body with the ProblemDetails data structure, then the SMF service includes a "Content-Type" header field configured to "application/problem+json". The SMF service generates the HTTP response.

Sending Problem Details

SMF sends the problem details to AMF in the following N11 messages.

- SM Context Create Error
- SM Context Update Error

- POST Response to SM Context Release
- POST Response to SM Context Retrieve

Handling Problem Details

SMF handles the problem details structure that SMF receives from AMF and provides roaming support on other SMFs.

EBI Assignment Error with Problem Details

SMF handles this N11 message by not storing any EBIs for the ARP values with the failed EBI assignment. For example, SMF handles an EBI assignment error from AMF with problem details and “EBI_EXAUSTED” cause along with failure details.

N1N2 Transfer Acknowledgment with Problem Details

SMF handles the acknowledgment N11 message according to the HTTP status and cause values in the problem details. For example, SMF handles the N1N2 acknowledgment message with HTTP status as 404 and cause as “CONTEXT_NOT_FOUND” from AMF.

Roaming Between SMFs

The home SMF (hSMF) and visited SMF (vSMF) communicate with each other over the N16 interface. The following sections describe how the ProblemDetails structure specified for N11 interface is sent on N16 interface for roaming call flows for hSMF and vSMF.

Call Flows

This section describes the following call flows:

- Create Service Operation on hSMF Call Flow
- Create Service Operation on vSMF Call Flow
- Update Service Operation towards hSMF Call Flow
- Update Service Operation towards vSMF Call Flow

Create Service Operation on hSMF Call Flow

The Create service operation creates a PDU session in the hSMF for home-routed roaming scenarios. The NF Service Consumer, such as vSMF, creates a PDU session by using the HTTP POST method.

This section describes the Create service operation on hSMF call flow.

Figure 2: Create Service Operation on hSMF Call Flow



Table 17: Create Service Operation on hSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as vSMF, sends a POST request to create a PDU session in hSMF.
2	If the PDU session creation is successful, the hSMF sends the "201 Created" to NF Service Consumer.
3	If the PDU session establishment fails, the hSMF sends the HTTP status code, as listed in the HTTP Status Codes for PDU Session Creation Error table. For the 4xx or 5xx response, the message body contains a PDU Session Create Error structure, including a ProblemDetails structure with the "cause" attribute.

Table 18: HTTP Status Codes for PDU Session Creation Error

Data Type	HTTPS Status Code	Cause	Details	Title
PDU Session Create Error	403	SUBSCRIPTION_DENIED	UDM_Subscription_Fetch_Failed	Network_Failure
PDU Session Create Error	403	SNSSAI_DENIED	SNSSAI_Not_Supported_By_SMF	Network_Failure
PDU Session Create Error	500	UNSPECIFIED_NF_FAILURE	UDM_Notification_Failed	Network_Failure
PDU Session Create Error	404	SUBSCRIPTION_NOT_FOUND	UDM_Subscription_Failed	Network_Failure
PDU Session Create Error	504	NETWORK_FAILURE	SLA_Txn_Timeout	Network_Failure
PDU Session Create Error	403	DNN_DENIED	DNN_Not_Subscribed	Network_Failure

Data Type	HTTPS Status Code	Cause	Details	Title
PDU Session Create Error	403	SSC_NOT_SUPPORTED	SSC_Mode_Not_Supported_By_SMF	Network_Failure
PDU Session Create Error	403	SSC_DENIED	SSC_Mode_Denied_From_UDM	Network_Failure
PDU Session Create Error	403	PDUTYPE_DENIED	UDM_Rejected_PDU_Type	Network_Failure

Create Service Operation on vSMF Call Flow

The Create SM Context service operation creates an SM context for a PDU session either in the SMF or in the vSMF for home-routed roaming scenarios. The NF Service Consumer, such as AMF, creates an SM context by using the HTTP POST method.

This section describes the Create service operation on vSMF call flow.

Figure 3: Create Service Operation on vSMF Call Flow

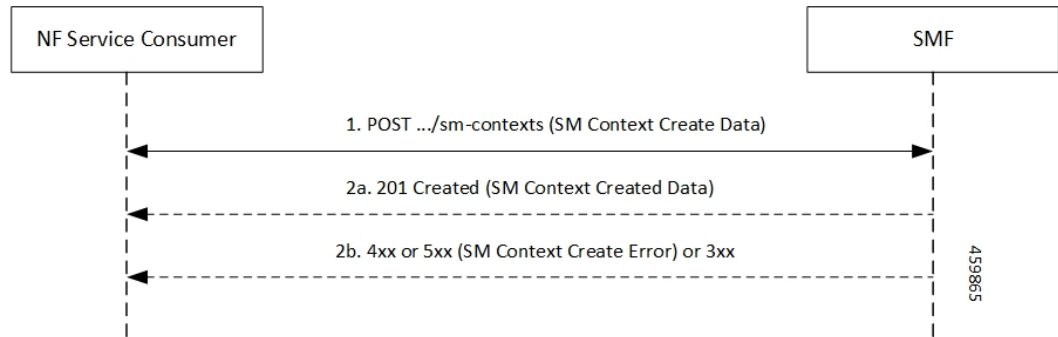


Table 19: Create Service Operation on vSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as AMF, sends a POST request to create SM Context to the resource that represents the SM contexts collection resource of the vSMF.
2	If the PDU session creation is successful, the SMF sends the "201 Created" to the NF Service Consumer.
3	If the PDU session establishment fails, the SMF sends the HTTP status code, as listed in the HTTP Status Codes for SM Context Creation Error table. For the 4xx or 5xx response to the NF Service Consumer, the message body contains an SM Context Create Error structure, including a ProblemDetails structure with the "cause" attribute.

Table 20: HTTP Status Codes for SM Context Create Error

Data Type	HTTPS Status Code	Cause	Details	Title
SM Context Create Error	403	PDUTYPE_NOT_SUPPORTED	PDU_Type_Not_Supported_By_SMF	Network_Failure
SM Context Create Error	500	REQUEST_REJECTED_UNSPECIFIED	Charging_Response_Failure	Network_Failure
SM Context Create Error	504	NETWORK_FAILURE	SLA_txn_timeout	Network_Failure
SM Context Create Error	400	MANDATORY_IE_MISSING	PDU_Session_ID_Not_Sent	Mandatory_IE_Missing

Update Service Operation Towards hSMF Call Flow

The NF Service Consumer, such as vSMF, updates a PDU session in the hSMF. The NF Service Consumer also provides the hSMF with information that NF Service Consumer receives from vSMF in the N1 SM signalling from the UE. The NF Service Consumer uses the HTTP POST method to receive this information.

This section describes the Update service operation towards hSMF call flow.

Figure 4: Update Service Operation Towards hSMF Call Flow

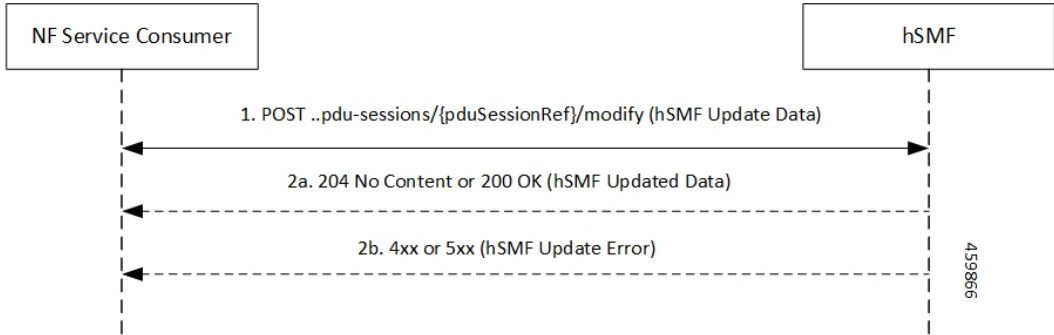


Table 21: Update Service Operation Towards hSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as vSMF, sends a POST request to modify a PDU session to the resource representing a PDU session resource in the hSMF.
2	If the PDU session update is successful, the hSMF sends "204 No Content" or "200 OK" to the NF Service Consumer.

Step	Description
3	If the PDU session update fails, the hSMF sends the HTTP status code, as listed in the HTTP Status Codes for hSMF Update Error table. For the 4xx or 5xx response, message body contains a hSMF Update Error structure, including the ProblemDetails structure with the "cause" attribute.

Table 22: HTTP Status Code for hSMF Update Error

Data Type	HTTPS Status Code	Cause	Details	Title
hSMF Update Error	404	CONTEXT_NOT_FOUND	PDU_Context_Not_Found	Network_Failure

Update Service Operation Towards vSMF Call Flow

The NF Service Consumer, such as hSMF, updates a PDU session in the vSMF. The NF Service Consumer also provides the required information for the V-SMF to send the N1 SM signalling to the UE by using the HTTP POST method.

This section describes the Update service operation towards vSMF call flow.

Figure 5: Update Service Operation Towards vSMF Call Flow

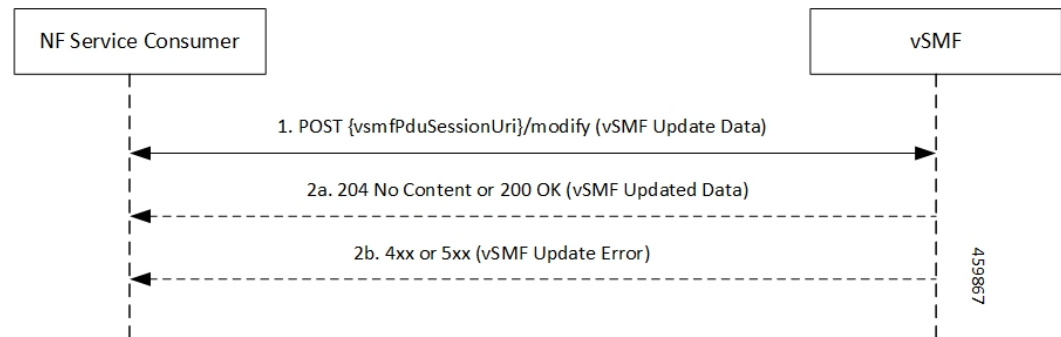


Table 23: Update Service Operation Towards vSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as hSMF, sends a POST request to modify a PDU session to the resource representing a PDU session resource in the vSMF.
2	If the PDU session update is successful, the vSMF sends "204 No Content" or "200 OK" to the NF Service Consumer.
3	If the PDU session update fails, the vSMF sends the HTTP status code, as listed in the HTTP Status Codes for vSMF Update Error table. For the 4xx or 5xx response, the message body contains a vSMF Update Error structure, including a ProblemDetails structure with the "cause" attribute.

Table 24: HTTP Status Codes for vSMF Update Error

Data Type	HTTPS Status Code	Cause	Details	Title
vSMF Update Error	400	UNSPECIFIED_NF_FAILURE	Ngap_Decode_failed	Invalid_Param
vSMF Update Error	500	UNSPECIFIED_NF_FAILURE	Failure_N4_Response	Network_Failure
vSMF Update Error	500	SYSTEM_FAILURE	Procedure_Aborted	Network_Failure
vSMF Update Error	500	INSUFFICIENT_RESOURCES	Failed_Due_To_Insufficient_Resouces_At_Gnb	Network_Failure
vSMF Update Error	400	UNSPECIFIED_NF_FAILURE	Qfi_Failed_List_Invalid	Network_Failure

Supported Status and Cause Codes

The following table lists the supported status and cause codes for this feature.

Table 25: Supported Status and Cause Codes

Title	Details	HTTP Status	Cause	Message
Network Failure	UDM_Registration_Failed	403	SUBSCRIPTION_DENIED	SMContext CreateError
Network Failure	SNSSAI_Not_Supported_By_SMF	403	SNSSAI_DENIED	
Network Failure	UDM_Subscription_Failed	404	SUBSCRIPTION_NOT_FOUND	
Network Failure	SLA_Txn_Timeout	504	NETWORK_FAILURE	
Network Failure	PDU_Type_Not_Supported_By_SMF	403	PDUTYPE_NOT_SUPPORTED	
Network Failure	UDM_Rejected_PDUTYPE	403	PDUTYPE_DENIED	
Network Failure	DDN_Not_Supported_By_SMF	403	DNN_NOT_SUPPORTED	
Network Failure	DDN_Denied_By_UDM_Or_UDM_Sent_Different_DNN	403	DDN_DENIED	
Network Failure	SSC_Not_Supported_By_SMF	403	SSC_NOT_SUPPORTED	
Network Failure	SSC_Denied_From_UDM	403	SSC_DENIED	
Network Failure	N26_HO_Failure_N4_Response	504	NETWORK_FAILURE	
Mandatory_IE_Missing	PDU_Session_ID_Not_Sent	400	MANDATORY_IE_MISSING	
Network Failure		403		

Title	Details	HTTP Status	Cause	Message
	N26_HO_Movement _Default_Bearer _Inactive		DEFAULT_EPS_ BEARER_ INACTIVE	
Network Failure	Failed_Due_To _Insufficient_ Resources_At _Gnb	500	INSUFFICIENT _RESOURCES	SMContext UpdateError
Network Failure	No_Resource_Is_ Allocated_By_The _Target_NGRAN	403	HANDOVER_ RESOURCE_ ALLOCATION_ FAILURE	
Network Failure	SLA_Txn_Timeout	500	UNSPECIFIED_ NF_FAILURE	
Network Failure	N2HO_N4_Reject	500	UNSPECIFIED_ NF_FAILURE	
Network Failure	XNHO_N4_Reject	500	UNSPECIFIED_ NF_FAILURE	
Network Failure	SLA_Txn_Timeout	500	UNSPECIFIED_ NF_FAILURE	POST Response SMContext Release
Network Failure	SLA_Txn_Timeout	504	NETWORK_ FAILURE	POST Response to SMContext Retrieve

Standards Compliance

The ProblemDetails JSON object support feature complies with the following standards.

- *3GPP TS 29.502—5G System; Session Management Services*
- *3GPP TS 29.518—5G System; Access and Mobility Management Services*
- *3GPP TS 29.571—5G System; Common Data Types for Service Based Interfaces*
- *3GPP TS 29.501—5G System; Principles and Guidelines for Services Definition*

Cause Information Elements

Feature Description

SMF supports cause IE on N11 interface message. With this feature:

- SMF supports sending and handling the received causes, which are available in Cause IE. For this support, SMF complies with the 3GPP TS 29.502 version 15.4.0.0, section 6.1.6.3.8.
- SMF supports the following 3GPP Change Requests (CR):
 - 3GPP TS 29.502, CR 0097 to send the new "INSUFFICIENT_UP_RESOURCES" cause information.
 - 3GPP TS 29.518 CR 161 not to support the UE_IN_NON_ALLOWED_AREA cause in N1N2 Message Transfer Error from AMF.
- SMF supports the statistics for the causes on the N11 interface messages.

How it Works

This feature works with the following support:

- Cause sending and handling support
- 3GPP CR support for CR0097 and CR 161
- Statistics support

Cause Sending and Handling

SMF supports sending and handling of the following received causes:

- REL_DUE_TO_HO
- EPS_FALLBACK
- REL_DUE_TO_UP_SEC
- DNN_CONGESTION
- S_NSSAI_CONGESTION
- REL_DUE_TO_REACTIVATION
- 5G_AN_NOT_RESPONDING
- REL_DUE_TO_SLICE_NOT_AVAILABLE
- REL_DUE_TO_DUPLICATE_SESSION_ID
- PDU_SESSION_STATUS_MISMATCH
- HO_FAILURE
- INSUFFICIENT_UP_RESOURCES
- PDU_SESSION_HANDED_OVER

Cause Description and Scenarios

This section provides information on the causes that SMF receives from AMF through N11 interface messages and the relevant scenarios of those causes.

REL_DUE_TO_HO

The following table describes the release due to handover cause and scenario.

Table 26: Release due to Handover Cause and Scenario

Cause	REL_DUE_TO_HO
Cause Description from 3GPP TS 29.502	Release due to handover
Scenario of occurrence	Handover from 5GS to EPG or ePDG during roaming
Message Used	vsmfUpdateData
Message Direction	H-SMF to V-SMF
Comments and Specification References	<p>3GPP TS 29.502</p> <ul style="list-style-type: none"> • 5.2.2.8.3 Update service operation towards V-SMF • 5.2.2.8.3.4 Handover between 3GPP and untrusted non-3GPP access, from 5GC-N3IWF to EPS or from 5GS to EPC/ePDG <p>If the request indication in the request is configured to NW_REQ_PDU_SES_REL and if the Cause IE indicates the release due to handover cause, then the V-SMF initiates the release of RAN resources reserved for the PDU session, if any. However, SMF doesn't send a PDU session release command to the UE.</p> <p>The V-SMF doesn't release the SM context for the PDU session.</p> <p>Note</p> <ul style="list-style-type: none"> • SMF doesn't support the roaming feature for this cause. • This cause is available in the SmContext release request after the N2 handover. SMF supports this scenario.

EPS_FALLBACK

The following table describes the mobility due to EPS fallback for IP Multimedia Subsystem (IMS) voice cause and the scenario of occurrence of the cause:

Table 27: Release due to EPS Fallback Cause and Scenario

Cause	EPS_FALLBACK
Cause description from 3GPP TS 29.502	Mobility due to ongoing EPS fallback for IMS voice.
Scenario of occurrence	IMS voice configuration in roaming scenario

Message used	VsmfUpdatedData This message is used in the qosFlowsFailedToAddModList attribute, which is the Cause IE of QosFlowItem.
Message direction	V-SMF to H-SMF
Comments and Specification References	<p>SMF supports the following scenarios for this cause as per the specification:</p> <ul style="list-style-type: none"> • 3GPP TS 23.502, Section 4.13.6.1 for EPS fallback for IMS voice. <p>The PDU Session Response message towards the PGW-C+SMF receives the QoS flow for IMS voice through AMF. For roaming scenario, this message is sent towards H-SMF+PGW-C through V-SMF. NG-RAN rejects the PDU Session modification to configure the QoS flow for IMS voice indicating the ongoing mobility due to fallback for IMS voice.</p> <ul style="list-style-type: none"> • 3GPP TS 23.502 <p>If the NG-RAN rejects the establishment of a voice QoS flow due to EPS Fallback for IMS voice, as defined in 3GPP TS 23.502 [3], clause 4.13, the V-SMF returns the cause. V-SMF indicates the cause as ongoing mobility due to EPS fallback for IMS voice for the corresponding flow in the qosFlowsFailedToAddModifyList IE.</p> <p>Note This scenario doesn't support roaming.</p>

REL_DUE_TO_UP_SEC

The following table describes the release due to unfulfilled security requirements from User Plane cause and the scenario of occurrence of the cause:

Table 28: Release due to User Plane Cause and Scenario

Cause	REL_DUE_TO_UP_SEC
Cause description from 3GPP TS 29.502	Release due to unfulfilled User Plane security requirements.
Scenario of occurrence	AMF-initiated release when the NG-RAN is unable to fulfill the required User Plane security enforcement.
Message used	Release SM Context service operation
Message direction	AMF to SMF
Comments or Specification References	<p>3GPP 29.502, Section 5.2.2.4, Release SM Context service operation</p> <p>The REL_DUE_TO_UP_SEC cause is available in SM Context Release Request when NG-RAN is unable to fulfill the required User Plane security enforcement.</p>

DNN_CONGESTION

The following table describes the release due to the DNN-based congestion control cause and the scenario of occurrence of the cause:

Table 29: Release due to DNN Congestion Cause and Scenario

Cause	DNN_CONGESTION
Cause Description from 3GPP TS 29.502	Release due to the DNN-based congestion control.
Scenario of occurrence	SMF detects congestion for the requested DNN and performs an overload control for the DNN that restricts the establishment of the PDU session.
Message Used	SM Context Create Error and SM Context Update Error
Message Direction	SMF to AMF
Comments or Specification References	Not supported.

S_NSSAI_CONGESTION

The following table describes the release due to the S-NSSAI-based congestion control cause and the scenario of occurrence of the cause:

Table 30: Release due to S NSSAI Cause and Scenario

Cause	S_NSSAI_CONGESTION
Cause description from 3GPP TS 29.502	Release due to the S-NSSAI-based congestion control.
Scenario of occurrence	SMF detects congestion for the requested S-NSSAI and performs overload control for the S-NSSAI that restricts the establishment of the PDU session.
Message used	SM Context Create Error and SM Context Update Error
Message direction	SMF to AMF
Comments or specification references	Not supported.

REL_DUE_TO_REACTIVATION

The following table describes the release due to PDU session reactivation cause and scenario of its occurrence:

Table 31: Release due to Reactivation Cause and Scenario

Cause	REL_DUE_TO_REACTIVATION
Cause Description from 3GPP TS 29.502	Release due to PDU session reactivation.

Scenario of occurrence	3GPP TS 29.502, Section 5.2.2.3.10, P-CSCF Restoration Procedure via AMF. The POST request contains the release IE configured to True and the cause IE configured to REL_DUE_TO_REACTIVATION.
Message used	Update SM Context service operation
Message direction	AMF to SMF
Comments or specification references	After receiving the cause from AMF, SMF sends the 5GSM cause as Reactivation Required towards UE.

5G_AN_NOT_RESPONDING

The following table describes the cause when 5G access network (AN) doesn't respond to network-initiated request and the scenario of occurrence of the cause:

Table 32: Release due to 5G AN Not Responding Cause and Scenario

Cause	5G_AN_NOT_RESPONDING
Cause Description from 3GPP TS 29.502	The 5G AN doesn't respond to the network-initiated request.
Scenario of occurrence	None.
Message Used	SM Context Status Notification or Status Notification
Message Direction	SMF to AMF
Comments or Specification References	SMF supports the following scenarios for this cause: <ul style="list-style-type: none"> • When UE is activated on network, SMF sends the SM Context Status Notification or Status Notification message in the statusInfo cause during UE or network-initiated PDU session release. • While the activation of UE PDU session from a deactivated state, SMF waits for the PDU RES STP RES from gNB and if GNB doesn't respond to AMF or SMF, AMF sends the SM Context Update with UP CXT State as DEACTIVATED with this cause. AMF sends the Update SM Context service operation to SMF.

REL_DUE_TO_SLICE_NOT_AVAILABLE

The following table describes the release due to unavailability of the associated S-NSSAI cause and the scenarios of the occurrence of the cause:

Table 33: Release due to Slice not Available Cause and Scenario

Cause	REL_DUE_TO_SLICE_NOT_AVAILABLE
Cause Description from 3GPP TS 29.502	Release due to the associated S-NSSAI is unavailable.

Scenario of occurrence	The following are the scenarios of the occurrence of the cause: <ul style="list-style-type: none"> • Scenario 1—UDM-initiated slice information change notification to AMF when PDU is activated. • Scenario 2—UDM-initiated slice information change notification to AMF when PDU is deactivated.
Message Used	The following are the messages used for these scenarios: <ul style="list-style-type: none"> • Scenario 1—Update SM Context service operation. • Scenario 2—Release SM Context service operation.
Message Direction	AMF to SMF
Comments or Specification References	SMF supports the following scenarios for this cause as per the specification: <ul style="list-style-type: none"> • 3GPP TS 29.502, Section 5.2.2.3.12 AMF requested PDU Session Release due to slice not available. The POST request includes the release IE configured to True and the the cause IE configured to REL_DUE_TO_SLICE_NOT_AVAILABLE. • 3GPP TS 29.502, Section 5.2.2.4, Release SM Context service operation. As defined in 3GPP TS 23.501 [2], clause 5.15.5.2.2, a change of the set of network slices occur for a UE where a network slice instance is unavailable and the PDU session isn't activated.

REL_DUE_TO_DUPLICATE_SESSION_ID

The following table describes the release due to UE request for new PDU session establishment cause and the scenario of the occurrence of the cause:

Table 34: Release due to Duplicate Session ID Cause and Scenario

Cause	REL_DUE_TO_DUPLICATE_SESSION_ID
Cause Description from 3GPP TS 29.502	Release due to a UE request to establish a new PDU session with an identical PDU session ID.
Scenario of occurrence	AMF-requested PDU Session Release due to duplicate PDU Session ID.
Message Used	Update SM Context service operation
Message Direction	AMF to SMF

Comments or Specification References	<p>SMF supports the following scenario:</p> <p>As defined in 3GPP TS 24.501 [7], clause 5.4.5.2.5, when the AMF receives an initial request with the existing PDU Session ID in the PDU session context of the UE, AMF requests the SMF to release the existing PDU Session. After receiving the SM context status notification indicating that the deletion of the SM context in the SMF, the AMF releases the stored context for the PDU session. Then, the AMF sends the initial request with the PDU Session ID.</p> <p>The POST request includes the release IE configured to True and the cause IE configured to REL_DUE_TO_DUPLICATE_SESSION_ID.</p> <p>Note SMF doesn't send the NAS signaling to UE for the PDU session release in this procedure.</p>
--------------------------------------	--

PDU_SESSION_STATUS_MISMATCH

The following table describes the release due mismatch of PDU session status between UE and AMF cause and the scenario of the occurrence of the cause:

Table 35: Release due to PDU Session Status Mismatch Cause and Scenario

Cause	PDU_SESSION_STATUS_MISMATCH
Cause Description from 3GPP TS 29.502	Release due to mismatch of PDU Session status between UE and AMF.
Scenario of occurrence	UE service request procedure.
Message Used	SM Context Release Data
Message Direction	AMF to SMF
Comments or Specification References	<p>SMF supports the following scenario:</p> <p>As defined in 3GPP TS 24.501, Section 5.2.2.4, Release SM Context service operation, in case of mismatch of the PDU session status between the UE and the AMF, the AMF starts Release operation towards SMF to release the PDU context from network.</p>

HO_FAILURE

The following table describes the handover preparation failure cause and the scenario of the occurrence of the cause:

Table 36: Release due to HO Failure Cause and Scenario

Cause	HO_FAILURE
Cause Description from 3GPP TS 29.502	Handover preparation failure.

Scenario of occurrence	5GS to EPS handover over N26 interface and if no resources can be assigned in EPS for any attempted PDU session to be handed over.
Message Used	SM Context Update
Message Direction	AMF to SMF
Comments or Specification References	SMF supports the following scenario: AMF updates the SMF with the information that the handover preparation failed by sending a POST request with the cause attribute configured to HO_FAILURE and with an empty list of EPS bearer contexts. This procedure doesn't include the dataForwarding IE. Then, SMF releases the resources prepared for the handover and proceeds with the PDU session.

INSUFFICIENT_UP_RESOURCES

The following table describes the activation failure for User Plane connection due to insufficient resources cause and the scenario of the occurrence of the cause:

Table 37: Release due to Insufficient UP Resources Cause and Scenario

Cause	INSUFFICIENT_UP_RESOURCES
Cause Description from 3GPP TS 29.502	Failure to activate the User Plane connection of a PDU session due to insufficient user plane resources.
Scenario of occurrence	During an idle mode exit procedure.
Message Used	SM Context Updated Data
Message Direction	SMF to AMF
Comments or Specification References	3GPP TS 129.502 , Section 5.2.2.3.2.2, Activation of User Plane connectivity of a PDU session SMF supports the following scenario: As defined in 3GPP TS 38.413 [9], clause 9.3.4.16 5G-AN sends the N2 SM information to SMF including the cause of the failure or if the resources failed to establish the PDU session. After SMF receives this information, SMF considers that the activation of the User Plane connection has failed and configures the upCnxState attribute to DEACTIVATED. In case the activation of the User Plane connection fails due to insufficient resources, the cause is included in the problem details response and configured to INSUFFICIENT_UP_RESOURCES with status code as 500.

PDU_SESSION_HANDED_OVER

The following table describes the handover of PDU session cause and the scenario of the occurrence of the cause:

Table 38: Release due to PDU Session Handed Over Cause and Scenario

Cause	PDU_SESSION_HANDED_OVER
Cause Description from 3GPP TS 29.502	The PDU session is handed over to another system or access.
Scenario of occurrence	5GC to EPS mobility without N26 interface Handover from 5GS to EPC or ePDG
Message Used	SM Context Status Notification
Message Direction	SMF to AMF
Comments or Specification References	<p>SMF supports the following specification for this cause:</p> <ul style="list-style-type: none"> As defined in 3GPP TS 23.502, SMF supports Section 4.11.2.2 5GC to EPS mobility without N26 interface and 4.11.4.2 Handover from 5GS to EPC or ePDG As defined in 3GPP TS 29.502, Section 5.2.2.5 Notify SM Context Status service operation, SMF sends a POST request to the SM Context Status callback reference that the NF Service Consumer provides during the subscription of this notification. The payload body of the POST request contains the notification payload. If the PDU session handover triggers the notification, the notification payload contains the Cause IE with the PDU_SESSION_HANDED_OVER value. <p>Note</p> <ul style="list-style-type: none"> SMF doesn't support the 5GC to EPS mobility without N26 interface SMF supports sending of SM Context Status Notification with this cause during handover from 5GS to EPC or ePDG.

3GPP Change Requests

SMF supports the following change requests (CR) as per 3GPP specification:

- SMF complies with 3GPP TS 29.502 CR 0097 to support sending of the "INSUFFICIENT_UP_RESOURCES" cause to AMF. The INSUFFICIENT_UP_RESOURCES table describes this cause and scenario.
- SMF complies with 3GPP TS 29.518 CR 161 not to support the UE_IN_NON_ALLOWED_AREA cause in N1N2 Message Transfer Error from AMF. This transfer error occurs due to gateway timeout.

Statistics

SMF supports statistics for the following causes on the N11 interface messages that it receives from AMF.

SM Context Release Request:

- REL_DUE_TO_UP_SEC
- PDU_SESSION_STATUS_MISMATCH

SM Context Update Request when you configure the Release flag to True:

- REL_DUE_TO_SLICE_NOT_AVAILABLE
- REL_DUE_TO_REACTIVATION
- REL_DUE_TO_DUPLICATE_SESSION_ID

The following is an example showing the statistics for the REL_DUE_TO_SLICE_NOT_AVAILABLE cause:

```
smf_service_amf_msg_total{app_name="smf",cause_code="REL_DUE_TO_SLICE_NOT_AVAILABLE",cluster="smf",data_center="smf",direction="inbound",instance_id="1",message_type="pdu_session_release_request_amf",procedure_type="PDU Session Release - AMF initiated Mod Req",service_name="smf-service"} 2
```

Standards Compliance

The cause IE support on N11 interface feature complies with the following standards:

- *3GPP TS 29.502 version 15.4.0.0 (section 6.1.6.3.8) —5G; 5G System; Session Management Services; Stage 3*
- *3GPP TS 29.502 (CR 0097)—5G; 5G System; Session Management Services; Stage 3*
- *3GPP TS 29.518 (CR 161)—5G; 5G System; Access and Mobility Management Services; Stage 3*

N16 Interface

The N16 interface is the reference point between two SMFs in a roaming scenario, where one SMF is in the visited network and the other SMF is in the home network.

For details on roaming between SMFs, see [Roaming Between SMFs, on page 31](#).

ProblemDetails JSON Object

Feature Description

SMF supports sending and receiving the ProblemDetails JSON object on the N11 interface and supports roaming.

An application error can prevent the SMF service, acting as an HTTP server, from completing the HTTP request. In this case, the SMF service maps the application error to the similar 4xx or 5xx HTTP status.

An HTTP status code determines the cause of the error. However, sometimes these status codes don't have adequate information about an error. In this case, the SMF service acting as the HTTP server provides more application-related error information to the SMF service acting as an HTTP client. This SMF service provides the additional information by including the representation of “ProblemDetails” data structure in the response body.

3GPP specification defines JSON as one of the document formats. HTTP APIs reuse this format to identify various problem types based on the requirement.

The ProblemDetails structure specified for N11 interface is sent on the N16 interface for roaming call flows on hSMF. After receiving ProblemDetails from hSMF, the vSMF rejects the corresponding message from AMF and saves the ProblemDetails that vSMF receives from hSMF.

How it Works

This section describes how this feature works.

If a response includes a payload body with the ProblemDetails data structure, then the SMF service includes a "Content-Type" header field configured to "application/problem+json". The SMF service generates the HTTP response.

Handling Problem Details

SMF handles the problem details structure that SMF receives from AMF and provides roaming support on other SMFs.

Roaming Between SMFs

The home SMF (hSMF) and visited SMF (vSMF) communicate with each other over the N16 interface. The following sections describe how the ProblemDetails structure specified for N11 interface is sent on N16 interface for roaming call flows for hSMF and vSMF.

Call Flows

This section describes the following call flows:

- Create Service Operation on hSMF Call Flow
- Create Service Operation on vSMF Call Flow
- Update Service Operation towards hSMF Call Flow
- Update Service Operation towards vSMF Call Flow

Create Service Operation on hSMF Call Flow

The Create service operation creates a PDU session in the hSMF for home-routed roaming scenarios. The NF Service Consumer, such as vSMF, creates a PDU session by using the HTTP POST method.

This section describes the Create service operation on hSMF call flow.

Figure 6: Create Service Operation on hSMF Call Flow

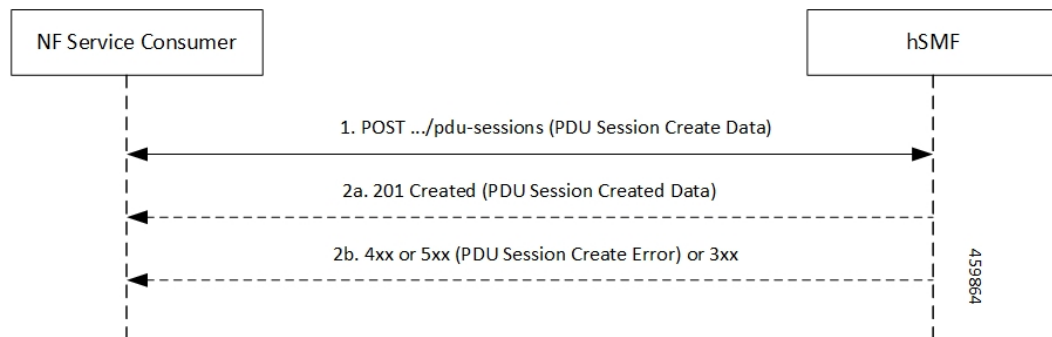


Table 39: Create Service Operation on hSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as vSMF, sends a POST request to create a PDU session in hSMF.
2	If the PDU session creation is successful, the hSMF sends the "201 Created" to NF Service Consumer.
3	If the PDU session establishment fails, the hSMF sends the HTTP status code, as listed in the HTTP Status Codes for PDU Session Creation Error table. For the 4xx or 5xx response, the message body contains a PDU Session Create Error structure, including a ProblemDetails structure with the "cause" attribute.

Table 40: HTTP Status Codes for PDU Session Creation Error

Data Type	HTTPS Status Code	Cause	Details	Title
PDU Session Create Error	403	SUBSCRIPTION_DENIED	UDM_Subscription_Fetch_Failed	Network_Failure
PDU Session Create Error	403	SNSSAI_DENIED	SNSSAI_Not_Supported_By_SMF	Network_Failure
PDU Session Create Error	500	UNSPECIFIED_NF_FAILURE	UDM_Notification_Failed	Network_Failure
PDU Session Create Error	404	SUBSCRIPTION_NOT_FOUND	UDM_Subscription_Failed	Network_Failure
PDU Session Create Error	504	NETWORK_FAILURE	SLA_Txn_Timeout	Network_Failure
PDU Session Create Error	403	DNN_DENIED	DNN_Not_Subscribed	Network_Failure
PDU Session Create Error	403	SSC_NOT_SUPPORTED	SSC_Mode_Not_Supported_By_SMF	Network_Failure
PDU Session Create Error	403	SSC_DENIED	SSC_Mode_Denied_From_UDM	Network_Failure
PDU Session Create Error	403	PDUTYPE_DENIED	UDM_Rejected_PDU_Type	Network_Failure

Create Service Operation on vSMF Call Flow

The Create SM Context service operation creates an SM context for a PDU session either in the SMF or in the vSMF for home-routed roaming scenarios. The NF Service Consumer, such as AMF, creates an SM context by using the HTTP POST method.

This section describes the Create service operation on vSMF call flow.

Figure 7: Create Service Operation on vSMF Call Flow

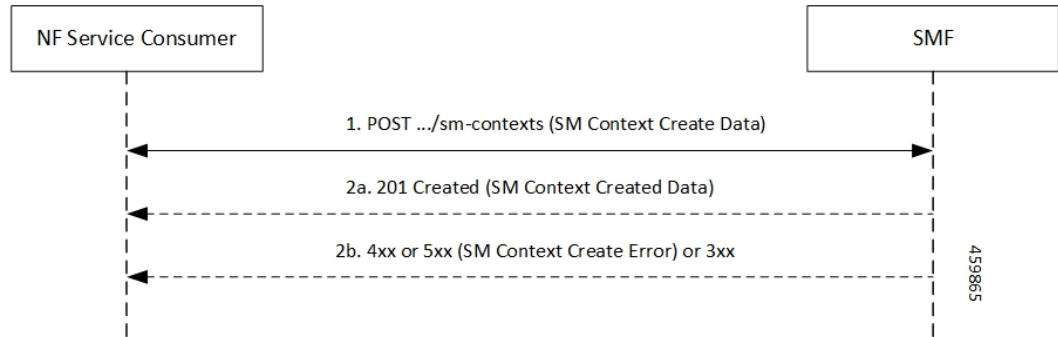


Table 41: Create Service Operation on vSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as AMF, sends a POST request to create SM Context to the resource that represents the SM contexts collection resource of the vSMF.
2	If the PDU session creation is successful, the SMF sends the "201 Created" to the NF Service Consumer.
3	If the PDU session establishment fails, the SMF sends the HTTP status code, as listed in the HTTP Status Codes for SM Context Creation Error table. For the 4xx or 5xx response to the NF Service Consumer, the message body contains an SM Context Create Error structure, including a ProblemDetails structure with the "cause" attribute.

Table 42: HTTP Status Codes for SM Context Create Error

Data Type	HTTPS Status Code	Cause	Details	Title
SM Context Create Error	403	PDUTYPE_NOT_SUPPORTED	PDU_Type_Not_Supported_By_SMF	Network_Failure
SM Context Create Error	500	REQUEST_REJECTED_UNSPECIFIED	Charging_Response_Failure	Network_Failure
SM Context Create Error	504	NETWORK_FAILURE	SLA_txn_timeout	Network_Failure
SM Context Create Error	400	MANDATORY_IE_MISSING	PDU_Session_ID_Not_Sent	Mandatory_IE_Missing

Update Service Operation Towards hSMF Call Flow

The NF Service Consumer, such as vSMF, updates a PDU session in the hSMF. The NF Service Consumer also provides the hSMF with information that NF Service Consumer receives from vSMF in the N1 SM signalling from the UE. The NF Service Consumer uses the HTTP POST method to receive this information.

This section describes the Update service operation towards hSMF call flow.

Figure 8: Update Service Operation Towards hSMF Call Flow

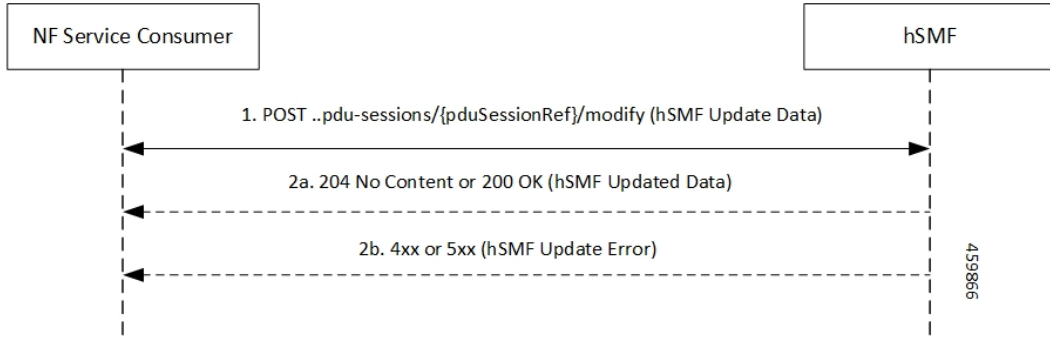


Table 43: Update Service Operation Towards hSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as vSMF, sends a POST request to modify a PDU session to the resource representing a PDU session resource in the hSMF.
2	If the PDU session update is successful, the hSMF sends "204 No Content" or "200 OK" to the NF Service Consumer.
3	If the PDU session update fails, the hSMF sends the HTTP status code, as listed in the HTTP Status Codes for hSMF Update Error table. For the 4xx or 5xx response, message body contains a hSMF Update Error structure, including the ProblemDetails structure with the "cause" attribute.

Table 44: HTTP Status Code for hSMF Update Error

Data Type	HTTPS Status Code	Cause	Details	Title
hSMF Update Error	404	CONTEXT_NOT_FOUND	PDU_Context_Not_Found	Network_Failure

Update Service Operation Towards vSMF Call Flow

The NF Service Consumer, such as hSMF, updates a PDU session in the vSMF. The NF Service Consumer also provides the required information for the V-SMF to send the N1 SM signalling to the UE by using the HTTP POST method.

This section describes the Update service operation towards vSMF call flow.

Figure 9: Update Service Operation Towards vSMF Call Flow

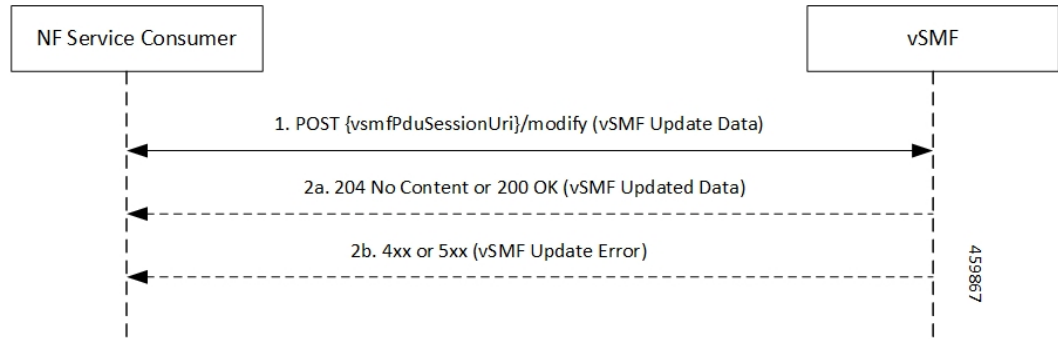


Table 45: Update Service Operation Towards vSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as hSMF, sends a POST request to modify a PDU session to the resource representing a PDU session resource in the vSMF.
2	If the PDU session update is successful, the vSMF sends "204 No Content" or "200 OK" to the NF Service Consumer.
3	If the PDU session update fails, the vSMF sends the HTTP status code, as listed in the HTTP Status Codes for vSMF Update Error table. For the 4xx or 5xx response, the message body contains a vSMF Update Error structure, including a ProblemDetails structure with the "cause" attribute.

Table 46: HTTP Status Codes for vSMF Update Error

Data Type	HTTPS Status Code	Cause	Details	Title
vSMF Update Error	400	UNSPECIFIED_NF_FAILURE	Ngap_Decode_failed	Invalid_Param
vSMF Update Error	500	UNSPECIFIED_NF_FAILURE	Failure_N4_Response	Network_Failure
vSMF Update Error	500	SYSTEM_FAILURE	Procedure_Aborted	Network_Failure
vSMF Update Error	500	INSUFFICIENT_RESOURCES	Failed_Due_To_Insufficient_Resouces_At_Gnb	Network_Failure
vSMF Update Error	400	UNSPECIFIED_NF_FAILURE	Qfi_Failed_List_Invalid	Network_Failure

N40 Interface

The N40 interface is the reference point between SMF and the Charging Function (CHF). The communication between SMF and CHF enable online and offline charging.

As the N40 interface is located between the SMF and CHF in the HPLMN, home routed roaming and non-roaming scenarios are supported in the same manner.

Nnrf Interface

For NF management, the Network Repository Function (NRF) system provides the service processing functions through HTTP2-based Nnrf Service-based interface (SBI). The Nnrf interface is displayed by NRF on 3GPP 5G system architecture. NRF provides the following services processing functions:

- NF Service Registration—Manage 5G Core service information that an NF instance provides.
- NF Service Discovery—Provide NF instance information that supports 5G Core SBI.
- Access Token—Provide authentication and authorization tokens for use of 5G Core services.

RADIUS Interface

Remote Authentication Dial-In User Service (RADIUS) is a protocol that manages network access. This protocol provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.

For authentication and authorization, when a user sends a request to NAS to gain access to a network resource using access credentials, the credentials are passed to the NAS device through the link layer protocol. For example, Point-to-Point Protocol (PPP). Then, the NAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access through the RADIUS protocol.

For accounting, when NAS grants network access to the user, NAS sends an Accounting Start packet to the RADIUS server to signal the start of the user network access.

S2b Interface

In wireless applications, the S2b interface is a 4G interface between the Packet Data Network Gateway (PGW) and Evolved Packet Data Gateway (ePDG). This interface uses the PMIPv6 protocol to establish WLAN sessions between the UE and the PGW.

S5 Interface

The S5 interface provides user plane tunnelling and tunnel management between Serving Gateway (SGW) and PDN gateway. It is used for SGW relocation due to UE mobility and if the SGW needs to connect to a non-located PDN gateway for the required PDN connectivity.

S5 and S8 Interfaces

Both the S5 and S8 interfaces are used within the Evolved Packet Core (EPC) for LTE and exist between the SGW and PGW. Based on functionality, both the S5 and S8 are same interfaces except that S8 interface is used when roaming between different operators while S5 interface is a internal to the network.

SBA Interface

The 5G architecture is based on a Service-Based Architecture (SBA). This architecture provides a modular framework from which you can deploy common applications using components of multiple sources and suppliers. The 3GPP defines the SBA for a 5G core network as delivered by a set of interconnected Network Functions (NFs), such as SMF. A network function can access services of other network functions.

The NFs communicate with each other through Service Based Interfaces (SBI). The SBI is the Application Programming Interface (API)-based communication (REST interface) that uses the HTTP/2 protocol.

HTTP/2 with TLS

Feature Description

The HTTP/2 TLS Support for SBA Interfaces feature enables support for SMF with HTTP/2 over a TLS secure channel for all the SBA interfaces toward the other NFs, for example, PCF, AMF, and so on.

This feature supports the following functionality:

- A CLI support to configure HTTPS (Hypertext Transfer Protocol Secure) Port on SBA interfaces.
- SMF uses TLS version 1.2 for transport layer protection and all inbound and outbound HTTP/2 transport.
- A CLI support to enter a TLS certificate for each SBA interface.
- HTTP/2 over a TLS secure channel for all the SBA interfaces toward the other NFs.



Note SMF also supports HTTP without TLS for backward compatibility. This is the default behaviour.

- Server and Client HTTPS requests for SMF.
- If there is no signed certificate available, the default behavior is to support a self-signed certificate.



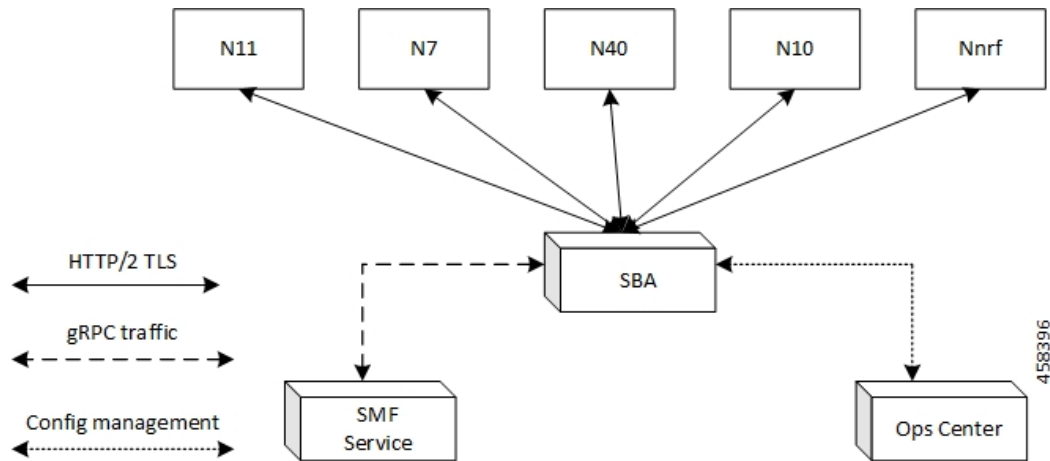
Note Currently, there is no support for persisting configured certificates.

- Generate appropriate alarms when a certificate is about to expire.

Architecture

The SMF Ops Center supports the HTTP/2 REST endpoints, which have TLS enabled for all the outbound interfaces, for example, N7, N10, N11, N40, Nnrf. If a multi-vendor support is required, each of the NF endpoints can independently select the TLS certificate.

Figure 10: SMF HTTP2 TLS Support for SBA Interfaces



Configuring HTTP/2 TLS for SBA Interfaces

This section describes the commands for configuring the HTTP/2 TLS support for SBA interfaces.

Configuring CA Certificates

Use the following sample configuration to configure the CA certificates:

```

config
  nf-tls ca-certificates certificate_name
    cert-data certificate_data
  exit
exit

```

NOTES:

- **nf-tls ca-certificates** *certificate_name*: Specifies the CA certificate name.
- **cert-data** *certificate_data*: Specifies the CA certificate data in the PEM format.

Configuring Server or Client Certificates

Use the following sample configuration to configure the server or client certificates:

```

config
  nf-tls certificates certificate_name
    cert-data certificate_data
    private-key certificate_private_key
  exit
exit

```

NOTES:

- **nf-tls ca-certificates** *certificate_name*: Specifies the CA certificate name.
- **cert-data** *certificate data*: Specifies the CA certificate data in the PEM format.
- **private-key** *certificate_private_key*: Specifies the CA certificate private key in the PKCS 8 format.

To obtain a private key from a certificate, perform the following steps:

1. Convert the certificate from PEM to PKCS12 format.

```
openssl pkcs12 -export -out pkcscertificate.p12 -inkey certificatekey.pem in
inputcertificate.pem
```

2. Extract the private key from PKCS12 certificate created in the preceding step.

```
openssl pkcs12 -in pkcscertificate.p12 nocerts -nodes -out privatekey.pem
```

3. Convert the private key to PKCS8 key.

```
openssl pkcs8 -in privatekey.pem -topk8 -nocrypt -out privatekey.p8
```

To enable HTTPS, the rest-endpoint uri-scheme is configured to HTTPS. The default value of the uri-scheme is HTTP. If the uri-scheme is configured as HTTPS, then the SMF requires the server certificate name.

Associating Configured Certificate to Interface

Use the following sample configuration to associate a configured certificate to an interface. You can view the configured certificate names through the **nf-tls certificates** CLI command.

```
config
  endpoint sbi certificate-name configured_certificate_name
  exit
exit
```

NOTES:

- **endpoint sbi certificate-name configured_certificate_name**: Shows the list of configured certificate names.

SMF uses the server certificate name for the SBI messages. These certificates are used during the starting of smf-rest-ep pod to configure SSL context for the REST SBI server. When SMF as a client initiates requests, such as N7, N10, and nNRF requests, the protocol is mentioned in the endpoint profile.

Verifying Configured Certificates

Use the **show running-config endpoint sbi** command to verify the certificates configured on the SBA interface.

The following is an example output of the **show running-config endpoint sbi** command.

```
smf# show running-config endpoint sbi
  endpoint sbi
    replicas          2
    uri-scheme        https
    certificate-name  smf-server
    vip-ip 209.165.200.225
  exit
```

Monitoring and Troubleshooting

This section provides information for troubleshooting any issues that might arise during the feature operation.

The SMF maintains various logs such as trace logs, event logs, and so on. Check the datastore pod health and the logs for any issues that are related to failures with message routing. Use information in the logs for diameter-ep-rx and datastore or session DB pods to debug issues with this feature.

show nf-tls certificate-status

To see the list of certificates, which are configured and their remaining validity period in days, use the following command:

```
show nf-tls certificate-status
```

Following is the sample output:

```
CERTIFICATE
NAME          DAYS
-----
ca            3631
smf-server    355
smfclient     355
```

Configuring Interfaces

To configure the endpoints for SMF service and the interfaces to facilitate communication with other network functions, use the following sample configuration:

```
config
  instance instance-id instance_id
    endpoint { bgpspeaker | dns-proxy | geo | gtp | gtpprime | li |
nodemgr | pfcf | protocol | radius | radius-dns | sbi | service |
sgw-service }
    interface { bfd | bgp | coa-nas | geo-external | geo-internal |
gtpu | n4 | n7 | n10 | n11 | n16 | n40 | nrf | s2b | s5 | s5e | s8 | s11
| sxa }
  vip-ip ipv4_address vip-port ipv4_port_number
  vip-ipv6 ipv6_address vip-ipv6-port ipv6_port_number
end
```

NOTES:

- **endpoint { bgpspeaker | dns-proxy | geo | gtp | gtpprime | li | nodemgr | pfcf | protocol | radius | radius-dns | sbi | service | sgw-service }**: Configure the endpoint based on the desired service.
- **interface { bfd | bgp | coa-nas | geo-external | geo-internal | gtpu | n4 | n7 | n10 | n11 | n16 | n40 | nrf | s2b | s5 | s5e | s8 | s11 | sxa }**: Specify the interface for the configured endpoint.
- **vip-ip *ipv4_address* vip-port *ipv4_port_number***: Specify the IPv4 address and port of the interface.
ipv4_address must be an IPv4 address in dotted decimal notation.
- **vip-ipv6 *ipv6_address* vip-ipv6-port *ipv6_port_number***: Specify the IPv6 address and port of the interface.
ipv6_address must be an IPv6 address in colon-separated hexadecimal notation.

Configuring IP Address for Interfaces

To enable the IPv4 or IPv6 communication between SMF and the other network functions, such as PCF, NRF, CHF, and UPF, use the following sample configuration:

```

config
  instance instance-id instance_id
    endpoint { protocol | sbi }
      replicas replica_id
      instancetype Dual
      nodes node_id
      interface { n4 | n7 | n10 | n11 | n40 | nrf }
        loopbackPort port_number
        vip-ip ipv4_address vip-port ipv4_port_number
        vip-ipv6 ipv6_address vip-ipv6-port ipv6_port_number
      end

```

NOTES:

- **interface { n4 | n7 | n10 | n11 | n40 | nrf }**: Specify the interface for the configured endpoint.
- **vip-ip ipv4_address vip-port ipv4_port_number**: Specify the IPv4 address and port of the interface.
ipv4_address must be an IPv4 address in dotted decimal notation.
- **vip-ipv6 ipv6_address vip-ipv6-port ipv6_port_number**: Specify the IPv6 address and port of the interface.
ipv6_address must be an IPv6 address in colon-separated hexadecimal notation.
- All the SMF interfaces support IPv4 address but only the SBI (N7, N10, N11, N40), N3, and N4 interfaces support either IPv4 or IPv6 address.
- Configure the ports, IPv4 and IPv6 addresses at both endpoint and interface levels. The VIP IP and port combination must be unique across the interfaces. If the interface level configuration is not available, the endpoint level configuration is considered.

Configuration Example

The following is an example of the IPv4 or IPv6 configuration for the interfaces.

```

config
  instance instance-id 1
    endpoint sbi
      replicas 1
      instancetype Dual
      nodes 1
      loopbackPort 7091
      vip-ip 209.165.200.225 vip-port 1234
      vip-ipv6 2001:DB8:1::1 vip-ipv6-port 2345
    interface nrf
      loopbackPort 7096
      vip-ip 209.165.200.226 vip-port 1235
    interface n11
      loopbackPort 7094
      vip-ipv6 2001:DB8:0:ABCD::1 vip-ipv6-port 1212
      exit
    interface n7
      loopbackPort 7092
      vip-ipv6 2001:DB8:1::FFFF vip-ipv6-port 1233
      exit
    interface n10
      loopbackPort 7093
      vip-ip 209.165.200.227 vip-port 4321

```

```

exit
interface n40
  loopbackPort 7095
  vip-ip 209.165.200.228 vip-port 4231
end

```

Since dual stack is not supported, the NRF discovery address transport type must be the same as the transport type configured at endpoint or interface level configuration.

In the preceding configuration example, the PCF uses IPv6 address which is the same transport type as configured within the PCF profile.

```

config
profile nf-client nf-type pcf
pcf-profile PP100
  locality LOCl
  priority 30
  service name type npcf-smpolicycontrol
  endpoint-profile EP1
  capacity 30
  uri-scheme http
  endpoint-name EP1
  priority 56
  primary ip-address ipv6 2001:DB8:1::FEFF
  primary ip-address port 2223
  exit
  endpoint-name exit
  exit
  exit
  exit
  exit
  exit
  exit
  exit

```

The following is an example of IPv6 configuration within UPF profile for the N4 interface.

```

config
profile network-element upf UPF1
  node-id SSI-UPF1
  n4-peer-address ipv6 2001:DB8:0:ACBD::1
  n4-peer-port 8805
  upf-group-profile upg1
  dnn-list [ emergency intershat test ]
  capacity 1
  priority 100
  exit
  exit
  exit

```

Configuration Verification

To verify the interface configuration, use the following command:

```
show running-config instance instance-id instance_id endpoint endpoint_name
interface interface_name
```

```

[smf] smf# show running-config instance instance-id 1 endpoint sbi interface nrf
instance instance-id 1
endpoint sbi
interface nrf
  loopbackPort 9050
  dscp 24

```

```
    vip-ip 209.165.200.232 vip-port 8095
    exit
    exit
    exit
[smf] smf#
```

This example output shows the configuration for NRF interface. The value for **vip-ip** command indicates that the IPv4 address is configured for the NRF interface.

