Emergency SoS Support

- Feature Summary and Revision History, on page 1
- SoS Emergency Service Fallback to LTE, on page 2
- Emergency Services Support, on page 6

Feature Summary and Revision History

Summary Data

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

Revision History

Table 1: Revision History

Revision Details	**Release**
First introduced.	2020.02.5.t1

SoS Emergency Service Fallback to LTE

Feature Description

The Emergency SoS Support feature enables the co-located cloud-native SMF and PGW-C to support SoS emergency over LTE for subscribers camped on the 4G network and SoS emergency service fallback to LTE for subscribers camped on the 5G network.

The Emergency SoS Support feature supports the following functionalities:

- Provides a new configuration to skip UDM interaction.
- Enables an emergency PDN connection creation in 4G (LTE) for PGW-C.
- Supports emergency service fallback to LTE requirement for SMF serving subscriber in NR.
- Supports interworking with an existing charging interface failure handling to ‘continue’ emergency call creation upon failure.
- Supports interworking with an existing secondary authentication using radius to skip radius authentication for emergency calls when not configured.
- Provides inter-RAT handover support (4G to 5G and 5G to 4G) for EPS interworking capable subscribers.

How it Works

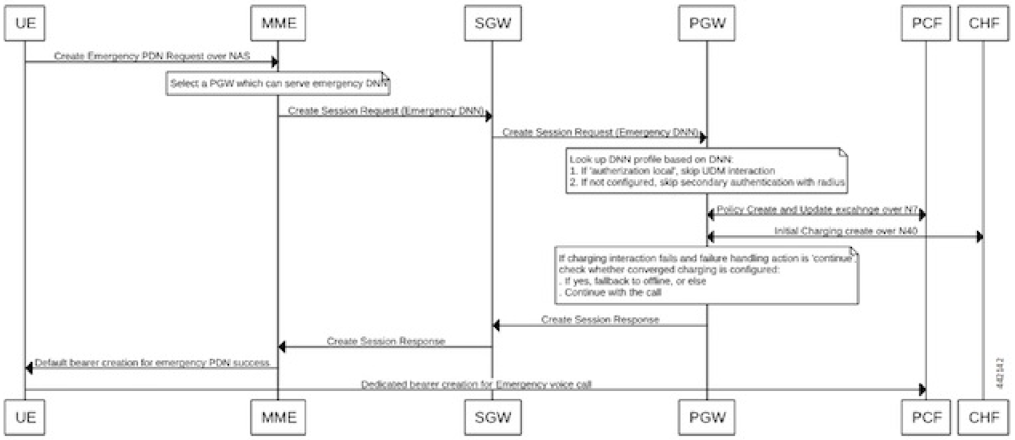
This section provides a brief of how the Emergency SoS Support feature works.

Call Flows

This section includes the following call flows.

Emergency Session Creation in LTE Call Flow

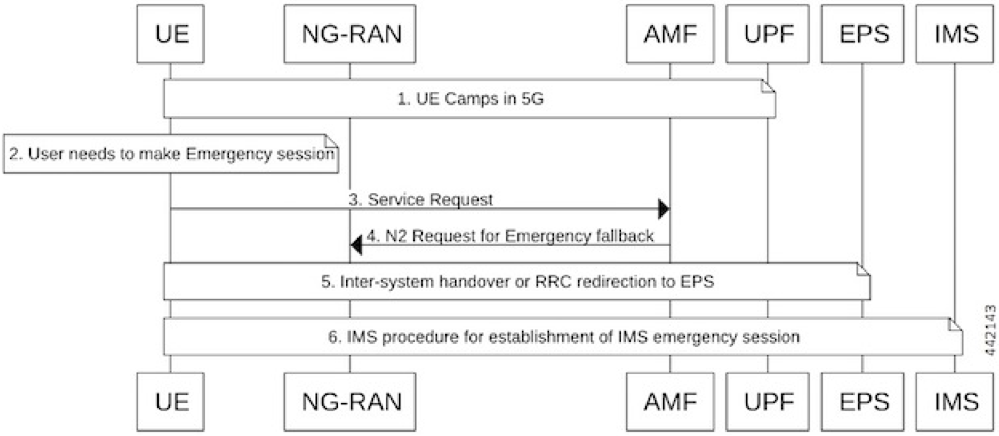
Figure 1: Emergency Session Creation in LTE


UE
MME
SGW
PGW
PCF
CHF
Create Emergency PDN Request over NAS
Select a PGW which can serve emergency DNN
Create Session Request (Emergency DNN)
Create Session Request (Emergency DNN)
Look up DNN profile based on DNN:
1. If 'autherization local', skip UDM interaction
2. If not configured, skip secondary authentication with radius
Policy Create and Update excahnge over N7
Initial Charging create over N40
If charging interaction fails and failure handling action is 'continue',
check whether converged charging is configured:
. If yes, fallback to offline, or else
. Continue with the call
Create Session Response
Create Session Response
Default bearer creation for emergency PDN success
Dedicated bearer creation for Emergency voice call
442142
UE
MME
SGW
PGW
PCF
CHF

Step	Description
1	When an emergency service is required and an emergency PDU session is not already established, the UE initiates the UE-requested PDU session establishment procedure with a request type indicating, "Emergency Request" in LTE.
2	The MME selects an APN or DNN for the emergency PDN creation, and sends a ‘Create Session Request’ to the PGW-C via the S-GW.
3	The DNN profile lookup at PGW-C is based on the subscriber policy or DNN policy. These policies are associated in the SMF profile. The subscriber policy has higher precedence over DNN policy when both the configurations are present.
4	The DNN policy can have the DNN profile configuration for each of the UE-requested APN or DNN received in the “Create Session Request” from the MME or S-GW.
5	When a new configuration ‘authorization local’ under the selected DNN profile is present: • PGW-C skips the UDM interaction for fetch subscription and uses the values received in the ‘Create Session Request’ message from the MME. • PGW-C skips the UDM interaction to ‘Subscribe-for-Notification’ from the UDM.
6	When the ‘Secondary Authentication Radius’ under the selected DNN profile is not present, the PGW-C rejects the RADIUS-based secondary authentication.
7	When ‘failure handling’ for charging interaction is set as ‘action continue’: • PGW-C continues the call if converged charging is not configured. • PGW-C falls back to offline charging and continues the call.
8	During handover from 4G to 5G using N26, if the emergency PDN gets handed over, the SMF checks the DNN profile and if ‘authentication local’ is present, it skips the UDM interactions for registration and deregistration.

Emergency Services Fallback to LTE Call Flow

Figure 2: Emergency Services Fallback to LTE


UE
NG-RAN
AMF
UPF
EPS
IMS
1. UE Camps in 5G
2. User needs to make Emergency session
3. Service Request
4. N2 Request for Emergency fallback
5. Inter-system handover or RRC redirection to EPS
6. IMS procedure for establishment of IMS emergency session
442143
UE
NG-RAN
AMF
UPF
EPS
IMS

Step	Description
1	UE camps on E-UTRA or NR cell in the 5GS (in either CM_IDLE or CM_CONNECTED state).
2	UE has a pending IMS emergency session request (example, voice) from the upper layers.
3	If the AMF has indicated support for emergency services using fallback via the “Registration Accept” message for the current RAT, the UE sends a “Service Request” message indicating that it requires an emergency services fallback.
4	The 5GC executes an NG-AP procedure in which it indicates to the NG-RAN that this is a fallback for emergency services. This procedure triggers the “Emergency Services Fallback” request. Currently the Cisco SMF and PGW-C supports Emergency Services in the EPC core Network (LTE). The AMF includes the EPC as a target CN to trigger inter-RAT fallback. When the AMF initiates the redirection for UEs that are successfully authenticated, AMF includes the security context in the request to trigger fallback towards the NG-RAN.
5	The NG-RAN initiates the handover or redirection to the E-UTRAN connected to the EPS (N26 interface based handover or redirection procedure). The NG-RAN uses the security context that the AMF to secure the redirection procedure. If the redirection procedure is used, the target CN is also conveyed to the UE to enable it to perform the S1 mode NAS procedures. The UE uses the emergency indication in the RRC message and E-UTRAN provides the emergency indication to the MME during the “Tracking Area Update”.
6	After handover to the target cell, the UE establishes a PDU session or PDN connection for IMS emergency services and performs the IMS procedures for establishment of an IMS emergency session (example, voice).

Configuring Emergency SoS Support

This section describes how to configure the Emergency SoS Support feature.

Configuring the Emergency SoS Support involves the following steps:

- Local authorization configuration under DNN profile
- Secondary authentication configuration under DNN profile
- Charging failure handling configuration under Charging profile

Configuring Local Authorization

Use the following sample configuration to configure local authorization under the DNN profile, use the following commands:

```
config
  profile dnn pool_name
    [ no ] authorization local
    end
```

NOTES:

- **profile dnn**: Specifies the DNN profile name. *profile_name* must be an alphanumeric string.

- **no**: Disables the local authorization under the DNN profile.

Configuring Secondary Authentication

Use the following sample configuration to configure secondary authentication under the DNN profile:

```
config
  profile dnn pool_name
    [ no ] secondary authentication radius
    end
```

NOTES:

- **no**: Disables the secondary authentication under the DNN profile.
- **secondary authentication**: Enables secondary-authentication under the DNN profile and sets method as RADIUS.
- **radius**: Specifies RADIUS for secondary authentication.

Configuring Charging Failure Handling

To configure failure handling action for both converged charging and offline charging failure cases under the charging profile, use the following sample configuration:

```
config
  profile network-element chf charging_profile_name
    nf-client-profile offline_charging_profile_name
    failure-handling-profile failure_handling_profile_name
    end
```

NOTES:

- **profile network-element chf** *charging_profile_name*: Specify the charging function (CHF) as the network element profile. *charging_profile_name* must an alphanumeric string representing the corresponding network element profile name.
- **nf-client-profile** *offline_charging_profile_name*: Specify the local NF client profile.*offline_charging_profile_name* must an alphanumeric string representing the corresponding NF client profile name.
- **failure-handling-profile** *failure_handling_profile_name*: Specify the NRF failure handling network profile for the configured NF type. *failure_handling_profile-name* must an alphanumeric string representing the corresponding NRF failure handling network profile name.

Configuration Example

The following is an example configuration of the failure handling action for converged charging:

```
profile nf-client-failure nf-type chf
profile failure-handling fh1
service name type nchf-convergedcharging
message type ChfConvergedchargingCreate
status-code httpv2 0
action continue
exit
```

Emergency Services Support

Feature Description

Emergency Services refer to functionalities provided by the serving network when the network is configured to support Emergency Services. Emergency Services are provided to support IMS emergency sessions.

To implement IMS emergency services in 4G and 5G, the SMF performs the following functions:

- Identifies 5G emergency session based on Request Type in SmContextCreate message or emergency configuration in DNN.
- Identifies 4G emergency session based on emergency configuration in DNN.
- Interacts with UDM if SUPI/IMSI is authenticated and **authorization local** command is not configured in the DNN profile. Else, skips the interaction with UDM.
- Enables PDU session establishment for Emergency Services with PEI or IMEI.
- Employs a new configuration to classify DNN as an Emergency DNN.
- Configures P-CSCF profile for Emergency Services
- Configures UPF for Emergency Services
- Configures default QoS profile for Emergency Services and flow-only timer used during tear down of dedicated bearer from PCF.

How it Works

Identification of Emergency Service Sessions

5G

SMF identifies the emergency session based on request type "Initial Emergency Request" or "Existing Emergency PDU Session" received in SmContextCreate Message from AMF or if the DNN is configured as an Emergency DNN.

4G

SMF identifies the emergency session based on the authentication status of IMSI. If the IMSI is unauthenticated (UIMSI is set to 1), the session is considered as an emergency session.

If IMSI is authenticated (UIMSI is set to 0), and DNN is configured as an emergency DNN (using new CLI) in SMF, the session is identified as an emergency session.

- For non-emergency session, SUPI or IMSI is mandatory.
- For emergency session:
  - For an authenticated SUPI or IMSI, SUPI or IMSI is used as the session-key based on the current implementation.
  - For an unauthenticated SUPI or IMSI, PEI or IMEI is always used as the session-key, If PEI or IMEI is not present, then the call is rejected.

UDM Interaction for Emergency Sessions

1. SMF skips UDM interaction if SUPI or IMSI is unauthenticated.
2. SMF skips UDM interaction if SUPI/IMSI is authenticated and if “authorization” in DNN configuration is set to “local”.
3. SMF interacts with UDM if SUPI or IMSI is authenticated and if “authorization” in DNN configuration is not set to local.
    - If UDM rejects, then the call will be rejected.
    - If UDM exchanges fail, further handling is done based on UDM failure handling template provisioning.

Important SMF does not consider whether “authorization local” is configured in DNN profile or not.

Configuring Emergency Sessions

1. Existing DNN, P-CSCF, UPF, and QoS Profile configuration works for emergency sessions.
2. Use CLI classify a DNN as Emergency DNN.
3. If "**authorization**" is set (using CLI) to local under DNN, UDM interaction is not required.
4. Use default Flow Only timer configuration to retain the default bearer to enable PSAP Callback session.

Support for Emergency Services if Request Type is “Existing Emergency PDU Session”

1. If the request type indicates "Existing Emergency PDU Session", the SMF determines that the request is HO from EPS (4G and WiFi). Current implementation supports emergency sessions mobility in WiFi to 5G HO using request type as “Existing Emergency PDU Session” and in 4G to 5G HO using N26 interface.
2. The SMF identifies the existing PDU session based on the PDU Session ID.
3. SMF updates the existing SM context to provide the representation of the updated SM context to the AMF in the response instead of creating new SM, which is equivalent to handling of “Existing PDU Session”.

Default Flow Only Timer for an Emergency Service (Dedicated Bearer)

At reception of an HTTP POST message that removes one or several PCC Rules from a PDU Session restricted to emergency services:

- When all PCC Rules bound to a QoS flow are removed, SMF initiates a QoS flow termination procedure.
- When not all PCC Rules bound to a QoS flow are removed, SMF initiates QoS flow modification procedure.

In addition, the SMF initiates a default flow only if timer if all PCC Rules with a 5QI other than the 5QI of the default QoS flow or the 5QI used for IMS signalling are removed from the PDU session restricted to Emergency Services (example - to enable public safety answering point (PSAP) Callback session). When the default flow only timer expires, the SMF initiates a PDU session termination procedure.

1. The SMF initiates default flow only timer when a PCF initiated modify procedure removes a dedicated bearer(voice/video). The main intension of this timer is to hold the emergency session for some more time to facilitate a PSAP callback.
2. When default flow only timer expires, the PCEF initiates termination of the IMS Emergency session.
3. The SMF stops the default flow only timer on receiving a PCF-initiated modification request for creating a new bearer.

EPS FB

If gNB rejects the QFI and EPS fall back is armed. SMf performs the EPS fallback as a it is done for a normal non-emergency session.

Use of PEI as Session Key

SMF uses PEI as session key if SUPI is not present or it is not authenticated. Following conditions must be met for PduContext on SMF:

1. The REST-EP, when the message is received, checks affinity based on SUPI and PEI. First lookup will be done with SUPI. If it fails, checks with the PEI.

   Or

   Both SUPI and PEI keys can be looked up.
2. When Smf-Service chooses PEI as key, it sets affinity in cache-pod using PEI.
3. When Smf-Service inserts CDL record using PEI as key, PEI will be added as Primary Key type. Either Primary key is SUPI+PduSessionid or PEI+PduSessionID.
4. After first transaction, CDL lookup will happen both with SUPI or PEI which ever is available.
5. SEID is generated using PEI hashing.

Configuring Emergency Service Support

This section describes how to configure Emergency Service Support.

Configuring Default Flow Only Timer in DNN Profile

Use the following sample configuration to configure Default Flow Only Timer:

```
config
   profile dnn profile_name
      timeout default-flow-only flow_only_timer
     end
```

NOTES:

- **timeout default-flow-only** *flow_only_timer* : Maximum allowed idle duration for a PDU/PDN session before system automatically terminates it. *flow_only_timer* must be an integer between 0 and 2147483647 milli seconds. Default is 0, which indicates the function is disabled.

Configuring Emergency DNN

Use the following sample configuration to configure Emergency DNN:

```
config
   profile dnn profile_name
     emergency { false | true }
     end
```

NOTES:

- **emergency {** *false* | *true* **}**: indicates whether dnn is emergency DNN or not, *false* | *true* must be false or true, default is false.

Verifying Emergency DNN

Use the following show command to verify Emergency DNN configuration:

```
show subscriber all
```

The following is an example output of the **show subscriber all** command.

```
subscriber-details
{
  "subResponses": [
    [
      "supi:imsi-123456789012345",
      "gpsi:msisdn-9999988888",
      "pei:imei-123456786666660",
      "psid:5",
      "dnn:intershat",
      "emergency:false",
      "rat:nr",
      "access:3gpp access",
      "connectivity:5g",
      "udm-uecm:209.165.202.131",
      "udm-sdm:209.165.202.151",
      "pcfGroupId:PCF-dnn=;",
      "pcf:209.165.202.151",
      "policy:2",
      "upf:209.165.202.151",
      "upfEpKey:209.165.202.151:209.165.202.150",
      "ipv4-addr:poolv4/209.165.200.225",
      "ipv4-pool:poolv4",
      "ipv4-range:poolv4/209.165.200.225",
      "ipv4-startrange:poolv4/209.165.200.225",
      "amf:209.165.202.151",
      "peerGtpuEpKey:209.165.202.151:209.165.202.158"
    ],
    [
      "gpsi:msisdn-9999988888",
      "pei:imei-352099001761480",
      "psid:6",
      "dnn:intershat",
      "emergency:true",
      "rat:nr",
      "access:3gpp access",
      "connectivity:5g",
      "pcfGroupId:PCF-dnn=;",
      "pcf:209.165.202.151",
      "policy:2",
      "upf:209.165.202.151",
      "upfEpKey:209.165.202.151:209.165.202.150",
      "ipv4-addr:poolv4/209.165.200.234",
      "ipv4-pool:poolv4",
      "ipv4-range:poolv4/209.165.200.225",
      "ipv4-startrange:poolv4/209.165.200.234",
      "amf:209.165.202.151",
      "peerGtpuEpKey:209.165.202.151:209.165.202.158"
    ]
  ]
}
```

Use the value of "emergency" to determine if the emergency services feature is enabled or disabled for the subscriber.

OAM Support for Emergency Services

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

Bulk Statistics Support

The following statistics are supported for the Emergency SoS Support feature.

- smf_session_counters: Indicates that the gauge is updated to show the number of current active sessions.

  This statistics includes "emergency_call" label. If the flag for this label is set to true, it indicates that it is an emergency call.

- smf_service_stats: Indicates the SMF call flow procedure counters.

  This statistics includes "emergency_call" label. If the flag for this label is set to true, it indicates that it is an emergency call.

- smf_service_resource_mgmt_stats: Indicates the SMF Service Resource Management Statistics.

  This statistics includes "emergency_call" label. If the flag for this label is set to true, it indicates that it is an emergency call.

For information on bulk statistics support for SMF, see the *UCC 5G SMF Metrics Reference*.