



Emergency Call Support on the ePDG and P-GW

This feature provides emergency call support on the ePDG and P-GW.

- [Feature Description, on page 1](#)
- [How it Works, on page 2](#)
- [Configuring AAA Failure Handling for s2b Emergency Calls, on page 6](#)

Feature Description

The ePDG and P-GW support emergency call establishment over untrusted WiFi for the P-GW as per 3GPP Release 13. Emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving network when the network is configured to support emergency services. Emergency bearer services are provided to normal attached UEs and, depending on local regulation, to UEs that are in limited service state. Receiving emergency services in a limited service state does not require a subscription.

Authentication Authorization Requests (AAA) to Diameter now carry the new Emergency-Indication AVP for Untrusted WiFi emergency calls. Diameter requests related to PDN connections for emergency services have the highest priority. Depending on regional/national requirements and network operator policy, these Diameter requests are the last to be throttled, in the event that the 3GPP AAA Server has to apply traffic reduction.

Supported Functionality

3GPP Release 13 Emergency Call Support on the ePDG and P-GW includes the following functionality:

- Emergency call establishment over untrusted WiFi for the P-GW. The P-GW includes the new **Emergency-Indication** AVP over the AAA s6b interface only during Emergency PDN connection establishment.
- Lawful Intercept is supported for Emergency PDNs over the s2b interface.
- Various Create Session Request message IEs have been modified to support all four different behaviors of emergency bearer establishment.
- Intra- and Inter-chassis recovery are supported for emergency call over the s2b interface.
- Network initiated dedicated bearer creation is supported for emergency calls over the s2b interface.
- The maximum APN restriction is ignored for emergency APN.

- Multiple PDNs are supported for emergency calls over the s2b interface.
- Context replacement for emergency calls over the s2b interface without IMSI with same IMEI is supported.
- P-GW emergency related statistics and bulkstats are available.
- Graceful shutdown of s2b emergency calls is supported.

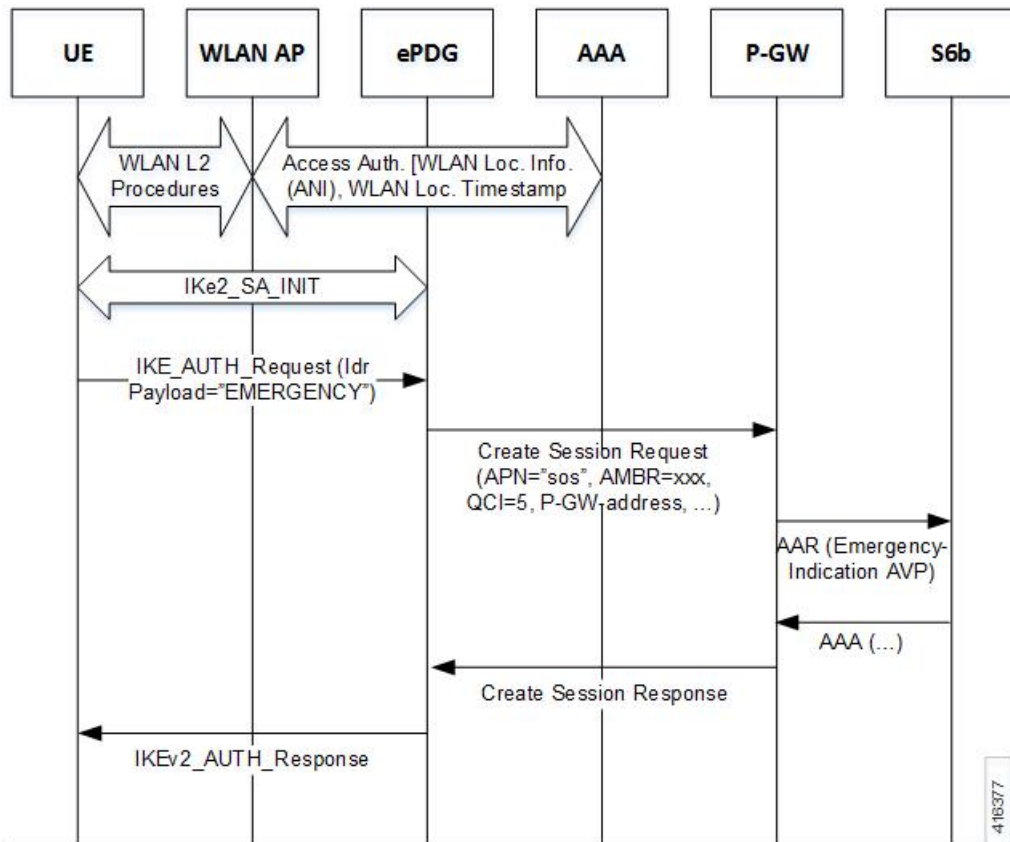
Previous Behavior: Emergency calls were not supported for the s2b interface. Also, handoff between the s2b interface and LTE was not supported for emergency calls.

New Behavior: Emergency calls are now supported on the s2b interface and handover is also supported for emergency calls from the s2b interface to LTE and vice-versa for "authenticated imsi" only.

How it Works

The ePDG sends a Create Session Request (CSReq) message to the P-GW. The P-GW deduces the emergency related policies to apply from the Access Point Name (APN) received in the CSReq message. For emergency attached User Equipment (UE), if the International Mobile Station Identifier (IMSI) cannot be authenticated or the UE has not provided it, then the International Mobile Equipment Identifier (IMEI) is used as UE identifier.

Figure 1: Call Flow: 3GPP R13 Emergency Call Support on the ePDG and P-GW



The P-GW sends the **Emergency-Indication** AVP over the s6b interface so that the 3GPP AAA server only applies specific policies for emergency services. For an unauthenticated UE, the 3GPP AAA server does not update the Home Subscriber Server (HSS) with the identity of the P-GW. For an authenticated UE, this indication is sent together with the "PDN GW currently in use for emergency services" message, which comprises the PDN GW address and the indication that the PDN connection is for emergency services to the HSS, which stores it as part of the UE context for emergency services.

Support is available for all four different behaviors of emergency bearer establishment:

- Valid UEs only.
- Only UEs that are authenticated are allowed.
- IMSI required, authentication optional.
- All UEs are allowed.

This section describes the new Attribute Value Pair (AVP) and modified Information Elements that support the feature.

Emergency-Indication AVP

A new **Emergency-Indication** AVP is defined in the Authentication and Authorization Request to signal a request to establish a PDN connection for emergency services.

The P-GW signals a new Emergency-Indication AVP to the 3GPP AAA Server in the Authorization Request over the S6b interface. In this case, the 3GPP AAA Server does not check the APN received from the P-GW (which contains an emergency APN) against the APNs authorized in the user subscription. This AVP is supported in the standard S6b dictionary **aaa-custom21**.

Information Elements

This section describes other important elements in a Create Session Request that have been modified to work properly with the feature.

Table 1: Information Elements in a Create Session Request

Information Elements	P	Condition/Comment	IE Type	Ins.
IMSI	C	<p>The IMSI is included in the message on the S4/S11 interface, and on the S5/S8 interface if provided by the MME/SGSN, except for the case:</p> <ul style="list-style-type: none"> - If the UE is emergency attached and the UE is UICCless. <p>The IMSI shall be included in the message on the S4/S11 interface, and on the S5/S8 interface if provided by the MME/SGSN, but not used as an identifier.</p> <ul style="list-style-type: none"> - If UE is emergency attached but IMSI is not authenticated. <p>The IMSI is included in the message on the S2a/S2b interface.</p>	IMSI	0

Information Elements	P	Condition/Comment	IE Type	Ins.
MSISDN	C	<p>For an E-UTRAN Initial Attach and a Handover from Trusted or Untrusted Non-3GPP IP Access to E-UTRAN the IE is included when used on the S11 interface, if provided in the subscription data from the HSS. For a PDP Context Activation procedure and a Handover from Trusted or Untrusted Non-3GPP IP Access to UTRAN/GERAN the IE is included when used on the S4 interface, if provided in the subscription data from the HSS.</p> <p>The IE is included for the case of a UE Requested PDN Connectivity, if the MME has it stored for that UE. It is included when used on the S5/S8 interfaces if provided by the MME/SGSN.</p> <p>The ePDG includes this IE on the S2b interface during an Attach with GTP on S2b , UE initiated Connectivity to Additional PDN with GTP on S2b and a Handover to Untrusted Non-3GPP IP Access with GTP on S2b, Initial Attach for emergency session (GTP on S2b), if provided by the HSS/AAA.</p> <p>The TWAN includes this IE on the S2a interface during an Initial Attach in WLAN on GTP S2a, UE initiated Connectivity to Additional PDN with GTP on S2a and a Handover to TWAN with GTP on S2a, if provided by the HSS/AAA.</p>	MSISDN	0
ME Identity (MEI)	C	<p>The MME/SGSN includes the ME Identity (MEI) IE on the S11/S4 interface:</p> <ul style="list-style-type: none"> - If the UE is emergency attached and the UE is UICCless. - If the UE is emergency attached and the IMSI is not authenticated. <p>For all other cases the MME/SGSN includes the ME Identity (MEI) IE on the S11/S4 interface if it is available.</p>	MEI	0
	CO	The TWAN/ePDG shall include the ME Identity (MEI) IE on the S2a/S2b interface, if it is available.		
Serving Network	C	This IE is included on the S4/S11, S5/S8 and S2b interfaces for an E-UTRAN initial attach, a Handover from Trusted or Untrusted Non-3GPP IP Access to E-UTRAN, a PDP Context Activation, a Handover from Trusted or Untrusted Non-3GPP IP Access to UTRAN/GERAN, a UE requested PDN connectivity, an Attach with GTP on S2b, a UE initiated Connectivity to Additional PDN with GTP on S2b, a Handover to Untrusted Non-3GPP IP Access with GTP on S2b and an Initial Attach for emergency session (GTP on S2b).	Serving Network	0

Information Elements	P	Condition/Comment	IE Type	Ins.
Indication Flags	C	This IE shall be included if any one of the applicable flags is set to 1. Applicable flags are: - Unauthenticated IMSI: This flag is set to 1 on the S4/S11 and S5/S8 interfaces if the IMSI present in the message is not authenticated and is for an emergency attached UE.	Indication	0
Selection Mode	C	This IE is included on the S4/S11 and S5/S8 interfaces for an E-UTRAN initial attach, a Handover from Trusted or Untrusted Non-3GPP IP Access to E-UTRAN, a PDP Context Activation, a Handover from Trusted or Untrusted Non-3GPP IP Access to UTRAN/GERAN and a UE requested PDN connectivity This IE is included on the S2b interface for an Initial Attach with GTP on S2b, a Handover to Untrusted Non-3GPP IP Access with GTP on S2b, a UE initiated Connectivity to Additional PDN with GTP on S2b and an Initial Attach for emergency session (GTP on S2b) The IE indicates whether a subscribed APN or a non-subscribed APN chosen by the UE/MME/SGSN/ePDG/TWAN was selected. This IE is included on the S2a interface for an Initial Attach in WLAN on GTP S2a, a Handover to TWAN with GTP on S2a and a UE initiated Connectivity to Additional PDN with GTP on S2a. The value is set to "MS or network provided APN, subscription verified".	Selection Mode	0
	CO	When available, this IE is sent by the MME/SGSN on the S11/S4 interface during TAU/RAU/HO with S-GW relocation.		
UE Local IP Address	CO	The ePDG includes this IE on the S2b interface during an Initial Attach for emergency session (GTP on S2b). Otherwise the ePDG shall include this IE on the S2b interface based on local policy.	IP Address	0
UE PDP Port	CO	The ePDG includes this IE on the S2b interface if NAT is detected and the UE Local IP Address is present.	Port Number	0
WLAN Location Information	CO	This IE is included on the S2b interface if the WLAN Location Information is available.	TWAN Identifier	1
WLAN Location Timestamp	CO	This IE is included on the S2b interface, if the WLAN Location Timestamp is available.	TWAN Identifier Timestamp	0

Emergency Handover Support

Two types of emergency call handovers are supported:

- **Handover of Emergency Calls from Untrusted WiFi to LTE:** Handover of s2b emergency calls to LTE is supported. Since an emergency call in LTE does not have s6b interface authorization enabled, handover of emergency calls from untrusted WiFi to LTE triggers a Session Termination Request (STR) to the s6b server.
- **Handover of Emergency Calls from LTE to S2b:** Handovers from LTE to S2b are supported. While the UE moves from LTE to untrusted WiFi, LTE triggers an Authentication Authorization Request (AAR) to the s6b server with the AVP *Emergency-Indication* sent in that Authentication and Authorization Request (AAR). Also, an STR is sent when a WiFi (s2b) call is cleared.

Configuring AAA Failure Handling for s2b Emergency Calls

Emergency calls over the s2b interface should not be rejected due to a failure from the S6b server. To ensure this, failure handling must be configured in the APN which is used for emergency calls .

Handling is configured in the **aaa group** so that emergency calls continue regardless of failures as indicated by the result code.

To configure AAA failure handling for s2b emergency calls:

configure

```

context ingress_context_name
  aaa group default
    diameter authentication failure-handling authorization-request
result-code 3000 to 5999 action continue
    diameter authentication failure-handling authorization-request
request-timeout action continue
  end

```

Note the following assumptions:

- If an IP-CAN Session Modification Request triggered by the PCRF removes all PCC rules with a QCI other than the default bearer QCI and the QCI used for IMS signaling, then the PCEF starts a configurable emergency inactivity timer. When the configured period of time expires, the P-GW initiates an IP-CAN Session Termination Request for the IP-CAN session serving the IMS Emergency session
- If the Gx/S6b interface returns a Virtual APN, which is not configured as an emergency APN, then the call is rejected with the cause code "APN_DENIED_NO_SUBSCRIPTION"