Emergency Communication

Version 1.2

29 May 2023

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

The GSMA makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.34 - Policy and Procedures for Official Documents.

Table of Contents

1 Introduction 4
1.1 Overview 4
1.2 Scope 4
2 Definitions 4
3 Abbreviations 5
4 References 7
5 Emergency service 8
5.1 Requirements 8
5.2 Emergency call type 8
5.2.1 UE detectable emergency c 8
5.2.2 Non UE detectable emergency call 9
5.3 2G/3G network 9
5.4 4G network 11
5.4.1 Download of Emergency Numbers to the UE 11
5.4.2 UE detectable emergency call 12
5.4.3 Non UE detectable emergency call 13
5.4.4 Video media in emergency call 13
5.5 5G network 15
6 Advanced Mobile Location 15
6.1 Rationale for better location 15
6.2 AML definition 15
6.3 Device and Operating System 16
6.4 2G/3G network 16
6.4.1 SMS requirements to support AML for roamers 17
6.4.2 Option for Visited SMSC to support AML for roamers 17
6.5 4G network 19
6.5.1 AML Procedures for 4G Core Networks 19
6.6 5G network 20
6.6.1 SMS in 5G Non Stand Alone (Option 3 deployment) 20
6.6.2 SMS in 5GS 20
7 eCall 21
7.1 Definition 21
7.2 Requirements 21
7.3 Circuit-Switched eCall 21
7.4 NGeCall (eCall over IMS) 22
8 Emergency calls over WLAN 24
8.1 General 24
8.2 IMS emergency services using WLAN access to EPC 25
8.2.1 Download of Emergency Numbers to the UE 25
8.2.2 UE detectable EC 25
8.2.3 NON-UE detectable EC 27
Annex A AML in 2G/3G networks 29

A.1 SMS 29
A.1.1 Home network 29
A.1.2 Roaming impact 29
A.2 DATA Push 29
A.2.1 Home 29
A.3 Roaming impact 30
A.4 SMS and DATA push comparison 30
Annex B AML in 4G/5G network – alternatives to SMS 31
B.1 DATA Push 31
B.2 SIP INVITE 31
Annex C AML: Location information format 32
C.1 Location information 32
C.2 Transport method 32
Annex D AML Implementation Examples 33
D.1 Devices 33
D.2 Networks / Countries 33
D.3 Implementation example: Orange Belgium 34
D.3.1 Initial AML design for Orange Belgium users 34
D.3.2 Roaming AML design for inbound Roamers 34
Annex E ETSI proposals for AML related to Roamers 35
Annex F List of Non UE detectable emergency numbers 37
Annex G Document Management 38
G.1 Document History 38
G.2 Other Information 38

1 Introduction

1.1 Overview

The present document describes the emergency communication for roamers in different technologies.

1.2 Scope

The scope of this document is to describe:

- Emergency calls for different technologies (2/3/4/5G networks)
- Improvement in term of location accuracy using Advanced Mobile Location (AML)
- eCall for different technologies (2/3/4/5G networks).

2 Definitions

Term	Description
AML	AML (Advanced Mobile Location) is a supplemental service that makes handset location available to emergency services when an emergency call is placed. The user’s location is sent directly to a Public Safety Answering Point or emergency call centre. GPS coordinates are sent using SMS or HTTPS. AML was standardised by the European Telecommunications Standards Institute (ETSI) Emergency Telecommunications Subcommittee (EMTEL)
eCall	A manually or automatically initiated emergency call (TS12) from a vehicle, supplemented with a minimum set of emergency related data (MSD), as defined under the EU Commission's eSafety initiative

3 Abbreviations

Term	Description
5GC	5G Core
AML	Advanced Mobile Location
CBOIExHC	Call Baring Except Home Country
CC	Country Code
CDR	Call Detail Record
CS	Circuit Switch
CSFB	Circuit Switched Fall Back
ECS	Emergency Call Server
E-CSCF	Emergency Call Session Control Function
EENA	European Emergency Number Association
ELS	Emergency Location Service
EMS	Emergency Medical Services
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
EU	European Union
FRS	Fire & Rescue Service
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GPRS	General Packet Radio Service
HTTPS	Hypertext Transfer Protocol Secure
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
ISIM	IMS (IP Multimedia Subsystem) Subscriber Identity Module
LBO	Local Breakout
LBS	Location Base Service
LRF	Location Retrieval Function
MAP	Mobility Application Part
MCC	Mobile Country Code
MME	Mobility Management Entity
MNC	Mobile Network Code
MSC	Mobile Switch Centre
MSD	Minimum Set of Data
MSISDN	Mobile Subscriber
NAS	Network Access Stratum
NR	New Radio
OS	Operating System

Term	Description
PDN	Public Data Network
P-CSCF	Proxy Call Session Control Function
PDU	Protocol Data Unit
PS	Packet Switch
PSAP	Public Safety Answering Point
RDF	Routing Determination Function
S8HR	S8 Home Routing
SCCP	Signalling Connection Control Part
SIM	Subscriber identity module
SMS	Short Message Service
SMSoIMS	SMS over IMS
SMSoNAS	SMS over NAS
SMS_MO	SMS Mobile Originated
SMSC	Short Message Service Centre
SIP	Session Initiation Protocol
STP	Service Transfer Point
TP	Transaction Processing
UE	User Equipment
URL	Universal Resource Locator
US	United States
USIM	Universal Subscriber Identity Module
VoIMS	Voice over IMS
VoLTE	Voice over LTE
VoNR	Voice over New Radio

4 References

Ref	Doc Number	Title
	GSMA IR.21	GSM Association Roaming Database, Structure and Updating Procedures
	ETSI TS 203 178 V1.1.1	Functional architecture to support European requirements on emergency caller location determination and transport
	ETSI TS 103 625	EMTEL; Transporting Handset Location to PSAPs for Emergency Calls - Advanced Mobile Location
[4]	ITU-T Q.713	Signalling connection control part formats and codes
[5]	3GPP TS 23.040	Technical realization of the Short Message Service (SMS)
[6]	EENA_2019_03_01	AML_Report_Card
[7]	3GPP TS 22.101	Service Aspect; Service principle
[8]	3GPP TS 22.003	Circuit Teleservices supported by a Public Land Mobile Network (PLMN)
[9]	GSM 4.08	Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification
[10]	3GPP TS 24.008	Mobile radio interface Layer 3 specification; Core network protocols; Stage 3
[11]	3GPP TS 24.229	IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
[12]	3GPP TS 23.167	IP Multimedia Subsystem (IMS) emergency sessions
[13]	3GPP TS 24.301	Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3
[14]	IR.65	IMS Roaming, Interconnection and Interworking Guidelines
[15]	3GPP TS 26.267	eCall Data Transfer; In-band modem solution; General description
[16]	GSMA IR.92	IMS Profile for Voice and SMS
[17]	3GPP TS 23.401	General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
[18]	3GPP TS 23.501	System architecture for the 5G System (5GS);Stage 2
[19]	ETSI TR 103.140	Mobile Standards Group (MSG); eCall for VoIP
[20]	GSMA NG.114	Profile for Voice, Video and Messaging over 5GS
[21]	GSMA PRD IR51	IMS Profile for Voice, Video and SMS over untrusted Wi-Fi
[22]	GSMA PRD IR61	WiFi Roaming Guidelines
[23]	3GPP TS 24.302	Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks
[24]	IETF RFC 5996	Internet Key Exchange Protocol Version 2 (IKEv2)
[25]	3GPP TS 33.402	Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks
[26]	3GPP TS 23.402	Architecture enhancements for non-3GPP accesses

5 Emergency service

5.1 Requirements

Emergency communication requirements are listed hereafter:

- Emergency call shall be established by dialling specific emergency numbers identified by the UE (User Equipment).
- Emergency call shall be established by dialling specific emergency numbers identified by the network (and not by the UE).
- Emergency call shall be established by using UE “red button”, without the need to dial a dedicated number in order to minimize miss-connection in roaming case.
- Emergency call must be supported by UE without a Subscriber identity module/ Universal Subscriber Identity Module (SIM/USIM/ISIM) being present.
- Emergency call must be free of charge for the user.
- Emergency calls shall be routed to the emergency services in accordance with national regulations where the subscriber is located.

5.2 Emergency call type

UE detectable emergency c

When an end user dials a number related to an emergency, or a, the UE shall check if this number is identified as a valid emergency number.

The following nominal cases are identified by the UE as valid emergency scenarios:

- Red button usage
- Emergency Numbers as defined in section 10 of [7]:
  - Standard emergency numbers dialled by the user (112 and 911)
  - Any emergency call number stored on a SIM/USIM (only possible if SIM/USIM present)
  - 000, 08, 110, 999, 118 and 119 when a SIM/USIM is not present (these numbers are stored in the UE).
  - Additional emergency numbers that may have been downloaded by the serving network when the SIM/USIM is present.

If the UE has identified an emergency number (as defined above), the UE initiates a emergency call setup procedure, enabling high priority in case of network congestion.

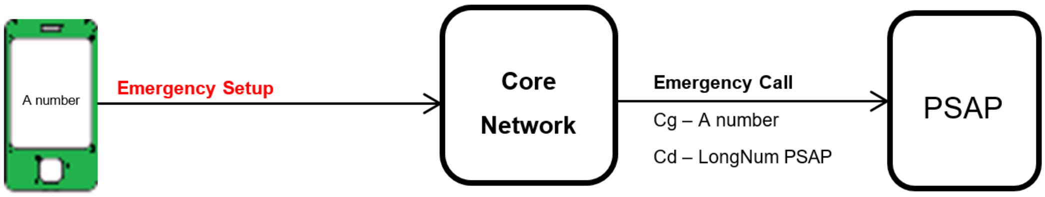

Figure 1 Emergency Call Setup

Non UE detectable emergency call

If telecommunication operators need to support “Local Emergency number” to comply with their legislation and these numbers are not made UE detectable as described in section 2.2.1, then the UE is not able to identify the emergency number dialed by the end user. The UE does not setup an emergency call but a normal call.

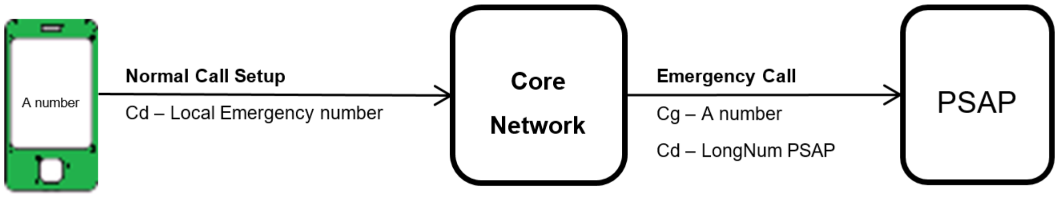

Figure 2 Normal Call Setup for Local Emergency number.

The local emergency call will not be prioritized and could be dropped in case of network congestion.

The core network translates the dialed short number and routes the call to the right PSAP (Public Safety Answering Point). As such, for an identified emergency number, the call will be free of charge for the end user.

5.3 2G/3G network

As defined in 3GPP TS22.003 [8], an emergency call is initiated by the UE using:

- 3GPP TS12 (Emergency Call) for Emergency calls identified by UE.
- 3GPP TS11 (Telephony) for local emergency calls (not identified by the UE)

When an emergency setup is received, the MSC (Mobile Switch Centre) will generate a call to the PSAP. The right PSAP will be chosen based on the Service Category and Location of the calling party. Called Party will contain the long number to access the PSAP.

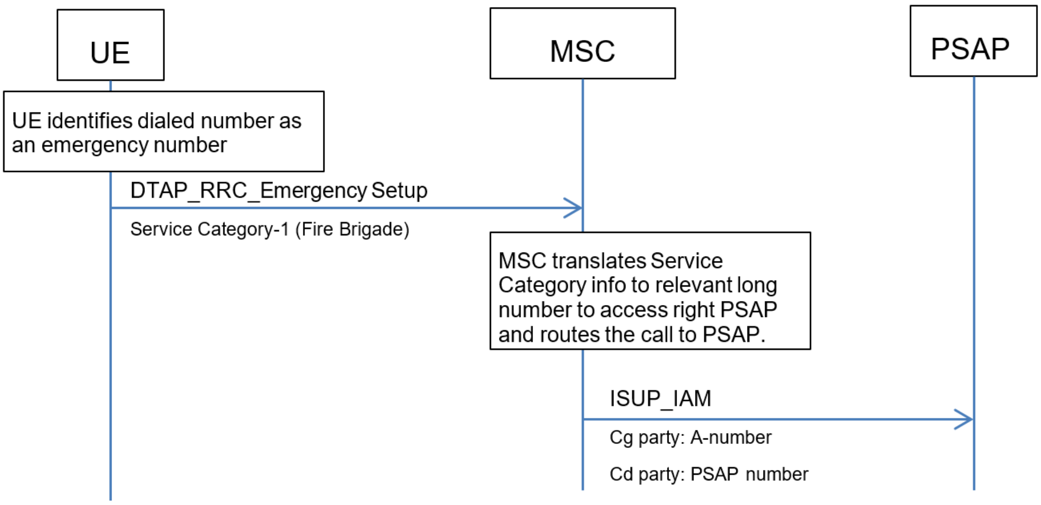
UE
MSC
PSAP
UE identifies dialed number as an emergency number
DTAP_RRC_Emergency Setup
Service Category-1 (Fire Brigade)
MSC translates Service Category info to relevant long number to access right PSAP and routes the call to PSAP.
ISUP_IAM
Cg party: A-number
Cd party: PSAP number

Figure 3 2G/3G Emergency Call (UE detectable)

Remarks:

- Emergency call setup has no Service Category in 2G [9]
- 3G Service Category [10] is used to indicate the Emergency category 1 which makes possible call routing to the right PSAP by the Core Network [7].

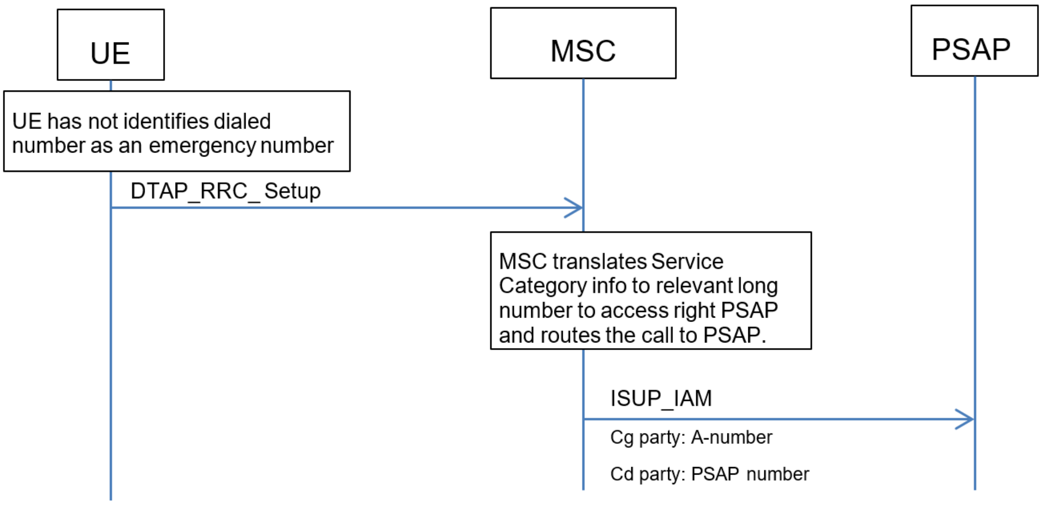
UE
MSC
PSAP
UE has not identifies dialed number as an emergency number
DTAP_RRC_ Setup
MSC translates Service Category info to relevant long number to access right PSAP and routes the call to PSAP.
ISUP_IAM
Cg party: A-number
Cd party: PSAP number

Figure 4 2G/3G Emergency Call (non UE detectable)

[1] Emergency category: Auto Initiated eCall, Manu Initiated eCall, Mountain Rescue, Marine Guard, Fire Brigade, Ambulance, Police

5.4 4G network

In 4G, 2 major technologies could be used for emergency call management:

- CSFB - Circuit Switched Fall Back: mobile operators could decide to use CSFB capability to manage the emergency call (see previous section related to 2G/3G).
- IMS- Voice over LTE (VoLTE): Emergency call is managed by the IP Multimedia Subsystem IMS Core Network. If the visited network has implemented an IMS subsystem supporting emergency calls, it is possible to set up emergency calls initiated by an emergency call number as described in the simplified call flow hereunder.

A CS (Circuit Switch) and IMS capable UE attempting an emergency call follows TS 23.167 [12] for initiating an emergency call.

Download of Emergency Numbers to the UE

As described in section 2.2.1, the serving network can download additional emergency numbers to the UE in order to enable UE detection of an emergency session.

These additional emergency numbers are downloaded in 4G during the Attach procedure included in Attach Accept message sent by the network (3GPP TS 24.301 [13]).

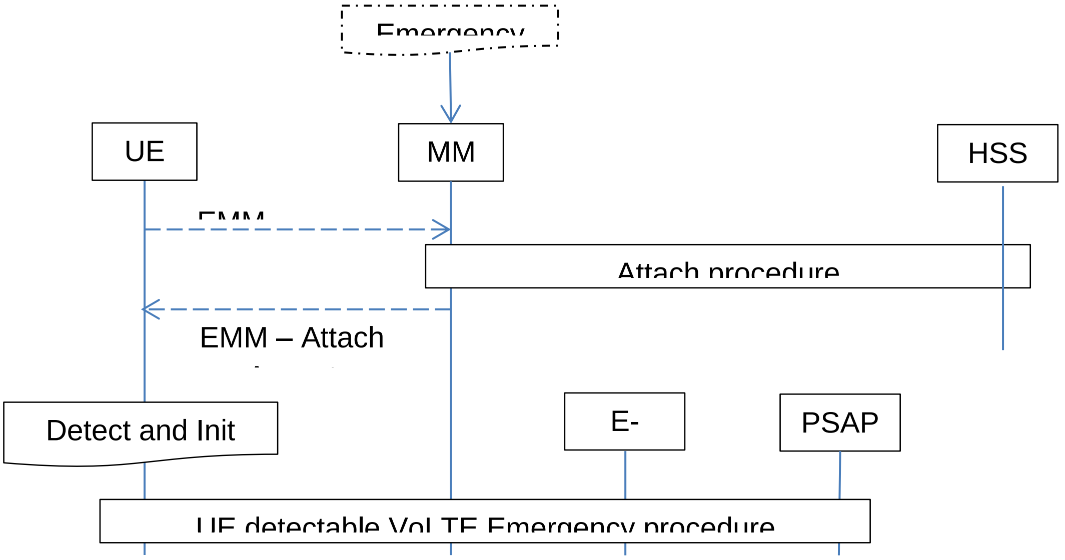

Figure 5 MME downloads emergency number list to UE

In case of roaming, the visited MME downloads the local Emergency list to visited UE. Emergency numbers are linked to countries defined by Mobile Country Code (MCC) and the Emergency list is discarded by the UE when entering in a new country .See also IR.65 [14]

If the UE of a roaming subscriber is not made aware of the emergency number, the call will be handled via normal session establishment.

UE detectable emergency call

When the UE detects an emergency number based on the mechanism described in section 2.2.1, the UE shall initiate the IMS emergency session establishment using the IMS session establishment procedures containing an emergency session indication and any registered Public User Identifier [12].

In case of roaming, Local Breakout (LBO) shall be always used.

In either of the above scenarios, the UE may or may not be normally registered in IMS network.

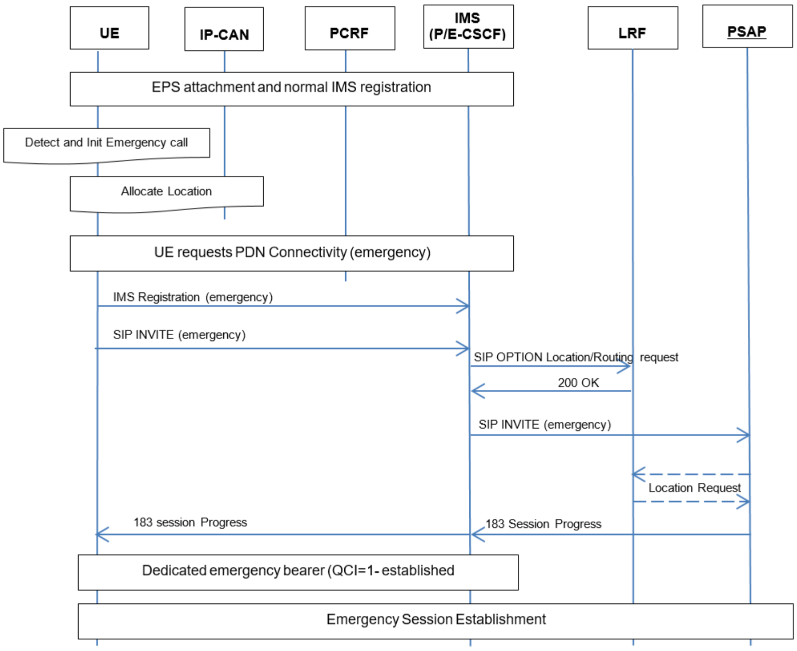
UE
IP-CAN
PCRF
IMS (P/E-CSCF)
LRF
PSAP
EPS attachment and normal IMS registration
Detect and Init Emergency call
Allocate Location
UE requests PDN Connectivity (emergency)
IMS Registration (emergency)
SIP INVITE (emergency)
SIP OPTION Location/Routing request
200 OK
SIP INVITE (emergency)
Location Request
183 session Progress
183 Session Progress
Dedicated emergency bearer (QCI=1- established
Emergency Session Establishment

Figure 6 VoLTE Emergency Call (UE detectable)

The UE shall comply to TS 23.167 [12] for initiating the emergency registration procedure

The emergency attach procedure described above is especially important in context of roaming. Via the emergency registration, the emergency session shall be managed by the visited network.

SIP INVITE (emergency) arrives at the Visited IMS (Emergency Call Session Control Function (E-CSCF) is the visited IMS network).

E-CSCF utilises the UE provided location information (transported in the P-Access-Network-Info header) and/or queries the LRF (Location Retrieval Function) to retrieve the proper routing information for PSAP.

E-CSCF routes the emergency session establishment request to an appropriate PSAP taking also into account the UE emergency type (if provided, e.g. Marine Guard, Fire Brigade, Ambulance, Police).

Non UE detectable emergency call

If telecommunication operators need to support "Local Emergency numbers" to comply with their legislation and these numbers are not made UE detectable as described in section 2.2.1 and the UE cannot detect this Emergency number, then the session establishment request is sent to the P-CSCF (Home P-CSCF in case of S8 Home Routing, S8HR roaming) as per a normal session establishment procedure.

In case the P-CSCF can detect that this is a request to establish a session related to an Emergency call, the P-CSCF rejects the session initiation request with an indication that this is for an emergency session via Session Initiation Protocol (SIP) 380 Alternative Response (3GPP 24.229 [11]). When the UE receives the session rejection then the UE establishes the Emergency session to E-CSCF (Visited E-CSCF in case of roaming). The VoLTE emergency call procedure could take place as described before when the UE detects Emergency number.

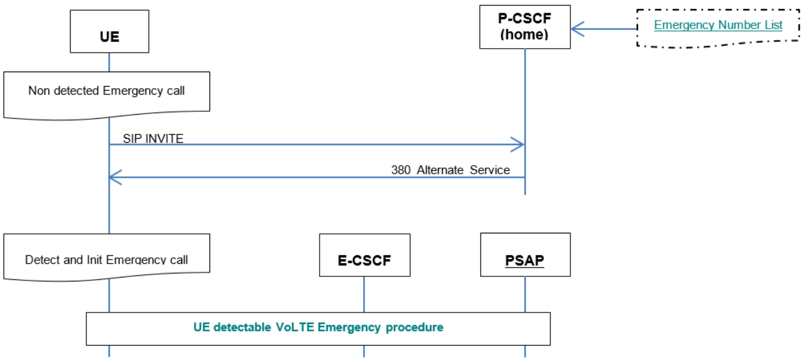
UE
P-CSCF (home)
Emergency Number List
Non detected Emergency call
SIP INVITE
380 Alternate Service
Detect and Init Emergency call
E-CSCF
PSAP
UE detectable VoLTE Emergency procedure

Figure 7 P-CSCF detects Emergency Call

This solution compared to the MME downloading additional emergency numbers to the UE has the disadvantage to try to establish a normal session as a first step. This session is rejected and before Emergency session is established

This mechanism should be used to complement the procedures for UE detected emergency numbers, e.g. in cases where the UE has limited support of the management of UE detectable emergency numbers as described in section 2.2.1, both for domestic as well as roaming cases

5.4.1 Video media in emergency call

This clause provides guidance and recommendation for predicable performance for video, where regulators require support of video, in addition to speech (VoIMS) and SMS media, in IMS emergency communication. This complements support for commercial IMS video service based on GSMA IR.94/NG.114, which can equally provide predictable performance, independent of the recommendation in this clause

Note 1: Legacy UEs are not expected to fully comply with the recommendations in this clause

The UE and the network must support IMS emergency services as specified in 3GPP Release 11 of TS 23.167 [12], clause 6 and Annex H.

The UE, PSAP, and network deployments supporting video must be capable to use video media from start of the emergency call, add video media to an ongoing emergency call (without video), and drop video media from an ongoing emergency call (with video).

The UE, PSAP, and network deployments supporting video must be capable to use uni-directional (send-only or receive-only, respectively) video, as well as bi-directional video in an emergency call, both from start of the call and resulting from a call modification. The UE and the PSAP must provide means for the user to selectively reject the use (or addition, in case of call modification) of video media in the emergency call while still accepting the call (or call modification).

The video media guaranteed bitrate (GBR) for the dedicated bearer used for video in emergency calls in network deployments supporting video, should either be set to zero (no guarantee) or to a low value (corresponding to minimum usable video quality).

The UE, PSAP, and network deployments supporting video must be capable to work with adaptive bitrate video. The video sender (UE or PSAP) must, during the session, be capable to dynamically restrict the video bitrate resulting from video encoding to a level that can be sustained by the current end-to-end network conditions. The video sender must be capable to dynamically estimate that sustainable video bitrate based on feedback from the video receiver. The video receiver must observe received video traffic and continuously during the session provide feedback to the video sender. Both video sender and video receiver must support RTCP feedback for congestion control, as described by IETF RFC 8888 [22], including the there described use of ECN with RTP [23]. Both video sender and video receiver must support reduced-size RTCP [24], as described by 3GPP TS 26.114 [21] clause 7.3.6. It is recommended to use reduced-size RTCP for the congestion control RTCP feedback packets whenever possible. Congestion control RTCP feedback packets may be included in regular RTCP reports when the send time of such feedback coincides with sending of regular RTCP reports.

The UE, PSAP, and network deployments supporting video shall support RTP retransmission, as described by 3GPP TS 26.114 [21] clause 9.3. If all call participants support Congestion Control RTCP feedback, as described by IETF RFC 8888 [22], it shall be used instead of the generic NACK feedback that is described for use with RTP retransmission by 3GPP TS 26.114. As described by 3GPP TS 26.114 clause 9.3.3, it is recommended to retransmit RTP packets that the video sender deems beneficial for timely recovery. It is not recommended to retransmit all RTP packets that were reported as lost, unless very few packets are lost and the overhead from retransmission is marginal. The video sender must keep the aggregate of original and retransmitted RTP packets below the negotiated maximum bitrate (MBR), by dynamically accounting for retransmitted packets when setting the adaptive video bitrate.

The UE, PSAP, and network deployments supporting video should support RTCP feedback signaling of video temporal/spatial trade-off (TSTR/TSTN), as described by IETF RFC 5104 [25] sections 3.5.2, 4.3.2, and 4.3.3. A UE supporting TSTR/TSTN must be capable to adjust the video encoding according to received TSTR messages and shall respond with a corresponding TSTN message with the used trade-off value when the video encoding adjustment is complete. A TSTR value of 0 shall correspond to the highest video detail the video sender can achieve within the limits negotiated for the session, and a TSTR value of 31 shall correspond to the highest video framerate the video sender can achieve within the limits negotiated for the session. A PSAP supporting TSTR/TSTN should include user interface means to control the TSTR value and sending the message to the UE. Before any TSTR is sent for the session, both UE and PSAP should assume that a value of 15 is used, representing neither extreme detail nor extreme motion.

5.5 5G network

With 5G Core (5GC), the only way to manage the voice service is Voice over IMS (VoIMS). CS Fall-back is not supported with 5GC. Nevertheless, the overall logic and principles to manage Voice over New Radio VoNR remain unchanged.

It is recommended to use the same approach as 4G to manage the IMS emergency call (section 2.4).

Only small updates related to 5G need to be implemented.

- Emergency calls over 5GC rely on dedicated emergency PDU session (counterpart of Emergency PDN connection in EPC).
- Functions in charge of retrieving or using trustable user location (network provided) like LRF (Location Retrieval Function) and RDF (Routing Determination Function) need to be updated to support New Radio NR Cell-ID format.

6 Advanced Mobile Location

6.1 Rationale for better location

Better location accuracy for emergency calls could save thousands of lives in the world:

- United States (US): The Federal Communications Commission has estimated that improving location services for 911 could save more than 10,000 lives annually
- European Union (EU): reducing the intervention time by 30 secs could save 800 lives / year in EU

Some regulators require better location accuracy in case of emergency calls:

- US: Federal Communications Commission requires carriers to locate callers within 50 m. in at least 80% of the cases by 2021
- EU: Now, the European Commission turns the spotlight to smartphone manufacturers: a legislative text published end 2018 will require all smartphones sold in the EU to support technical solutions that provide accurate handset-derived location information (Global Navigation Satellite System (GNSS), Wi-Fi) to emergency services (e.g. Advanced Mobile Location (AML)) for 2022.

6.2 AML definition

AML is a supplemental service that makes handset location available to emergency services when an emergency call is placed.

The user’s location (example: Global Positioning System (GPS) coordinates) is sent directly to the Public Safety Answering Point or emergency call centre) using SMS (Short Message Service) or Hypertext Transfer Protocol Secure (HTTPS).

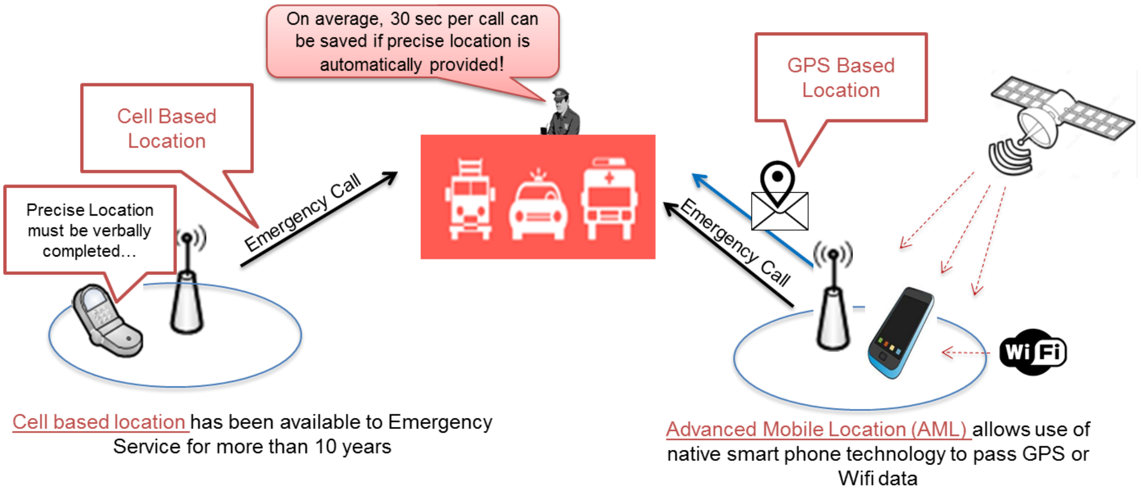
On average, 30 sec per call can be saved if precise location is automatically provided!
Cell Based Location
Precise Location must be verbally completed…
Emergency Call
GPS Based Location
Emergency Call
Wi Fi
Cell based location has been available to Emergency Service for more than 10 years
Advanced Mobile Location (AML) allows use of native smart phone technology to pass GPS or Wifi data

Figure 8 AML Global Context

AML will increase significantly the location accuracy compare to the Cell information.

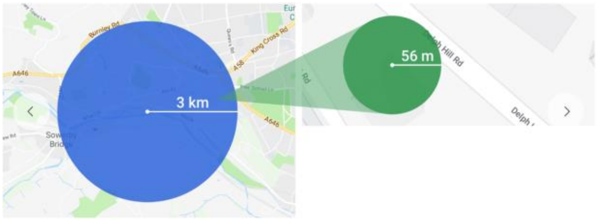

Figure 9 AML improve accuracy.

6.3 Device and Operating System

AML is supported by the Operating System (OS) of different smartphones (see Annex D.1).

AML is not an applet. However, the technology is activated by the OS provider on a country-

by-country basis once the national authorities are technically and operationally ready to receive location information sent from the terminal.

6.4 2G/3G network

AML functionality is triggered by a TS12 emergency call (which is unaffected), and is designed to supplement the basic network location feed wherever possible, i.e. with some acknowledgement of limitations in GNSS or Wi-Fi availability for the handset and the time required to acquire location using GNSS.

Location information established by the handset, using its built-in GNSS and Wi-Fi connectivity, together with user plane assistance data from a handset-selected service where available, is transported service PSAPs.

Two options to transport location information: SMS or DATA (SMS is the recommended option – see Annex A for more information).

ETSI (ETSI TS 103 625 [3]) defined two SMS options to support AML for inbound Roamers (Annex E) but these options are not efficient.

This document recommends another alternative to be put in place to support AML for inbound roamers based on visited SMSC (SMS Centre) usage and compatible with solution put in place for national users.

SMS requirements to support AML for roamers

The following requirements shall be taken into account in order to define a “roaming compliant “AML solution:

- [Req 1] AML shall be FREE of charge for customers
- [Req 2] AML shall work on 2G/3G/4G and 5G networks
- [Req 3] AML shall work also if Call Baring Outgoing International Except Home Country (CBOIExHC) is activated
- [Req 4] AML shall work in case of Customer Suspension (*)

(*) depending on the subscriber suspension (i.e. in case of bad payement) solution retained by the home network (all cases could not be covered and must be reviewed use case by use case).

Option for Visited SMSC to support AML for roamers

When a device generates the SMS associated with the emergency call, the SMS will use a specific SMSC address, enabling routing to the visited SMSC.

In this option, SMSC = <visited>CC + 112 (or CC+911) is configured in order to be able to submit SMS if Call Baring Outgoing International Except Home Country CBOIexHC is activated, it will be mandatory to prefix 112 with CC (Country Code)

MSC will be responsible to route the SMS to the visited SMSC. The SMSC will deliver Location information to visited PSAP as described in the figure hereunder.

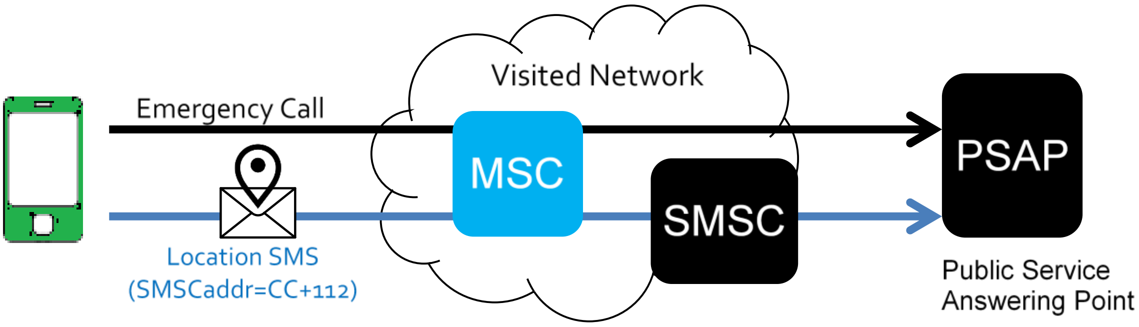

Figure 10 AML proposal for roamers

Based on principles described previously; the corresponding SMS flow is illustrated in Figure 11

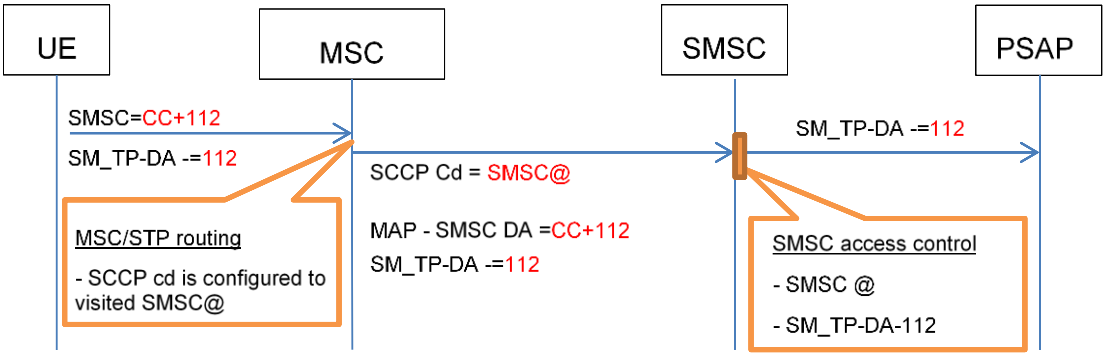

Figure 11 AML SMS flow for roamers

The devices (supporting AML for roamers), will replace the current **SMSC address** with the visited SMSC address (CC+112/911). **Destination number** is still unchanged (Transaction Processing TP-Destination-Address=112/911 or local emergency numbers).

The MSC will be responsible to route the SMS to the visited SMSC. Signaling Connection Control Part (SCCP) called party will be derived from the SMSC address (CC+112), and will be translated to the visited SMSC address. Depending to the network topology, MSC or Service Transfer Point (STP) could be used. In any case the Mobility Application Part (MAP) parameters will remain unchanged.

It is also important to control the SMS_MO (SMS Mobile Originated) billing record generation to avoid any charging to the customer (see Req1).

- Avoid billing generation at MSC for this specific event. This solution is not recommended. Local authorities need to retrieve a call detail record (CDR) in case of a request.
- Or if it is not possible rate the Transferred Account Procedures (TAP) file generated based on this event, to zero

The SMSC will deliver the Location information to visited PSAP. With the introduction of the AML-SMS for visitors, the visited SMSC needs to accept SMS coming from ALL visitors. SMSC control needs to be changed and could be based on the following checks:

- MAP - Service centre address DA =CC+ 112
- TP-Destination-Address (TP-DA) =112 or local emergency numbers

An implementation example is provided in Annex D.3

6.5 4G network

In 4G, two major technologies could be used for handling emergency calls:

- Circuit Switched Fall Back: mobile operators could decide to use CSFB capability to manage an emergency call. AML procedures described in the previous section related to 2G/3G are applicable. AML procedures for 4G core networks is described below.
- IMS (VoLTE): emergency call is handledby the IMS Core Network as described in chapter 2.4.

In addition to SMS, other mechanisms to transport location information are defined for 4G/IMS with the possibility in case of Emergency session establishment, to include the location information provided by the UE (based on GNSS or Wi-Fi connectivity) in the SIP INVITE.

As explained in Annex B, DATA push and SIP INVITE options are not recommended.

AML Procedures for 4G Core Networks

SMS over NAS

The figure below describes the two possible options to manage AML SMS over NAS in the Core Network:

- SMS over SGs will reuse the MSC approach and the 2/3G proposition to support AML in roaming (section 3.4.2 is still applicable).
- With SMS over Diameter, the proposition to support AML in roaming (section 3.4.2) is still applicable if the Mobility Management Entity (MME) is able to translate SMSC address received from UE to the Visited SMSC.

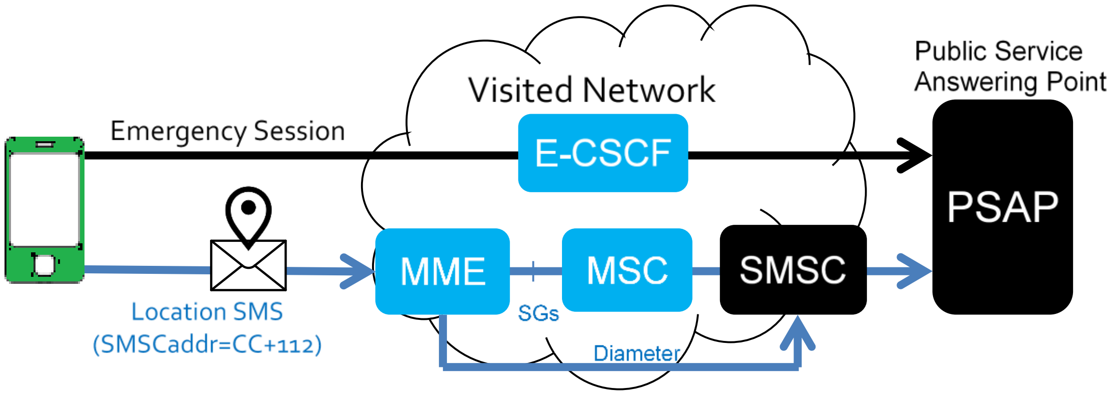

Figure 12 AML with SMSoNAS

SMSoNAS is the recommended solution and is compatible with the 2/3G approach.

SMS over IMS

SMS over IMS (SMSoIMS) in roaming situation requires that SMS SIP Session is established from the UE to the Home IP-SM Gateway. A complex solution must be then put in place to reroute SMS from the home Network to the visited network.

SMSoIMS is not recommended.

6.6 5G network

With 5GC, the only way to manage voice service is VoIMS. CS Fall-back is not supported with 5GC

SMS in 5G Non Stand Alone (Option 3 deployment)

5G NSA is similar to 4G, (see section 3.5).

SMS in 5GS

For deployment of a new 5G core network (5GC), the 5G system still supports the SMS feature by providing means to communicate with the legacy SMSC environment, with the same Mobility Application Part (MAP) or DIAMETER interfaces.

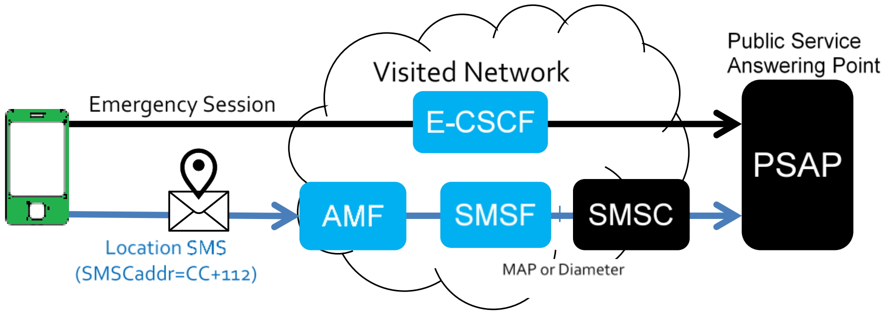

Figure 13 SMS over NAS and SMS over IP are possible

SMS over NAS (SMSoNAS) is the recommended solution and is compatible with the 2/3/4G approach.

Alternatives like DATA Push and SIP INVITE are not recommended ‘(see Annex B).

7 eCall

7.1 Definition

‘eCall’ refers to an in-vehicle emergency call to 112, made either automatically, by means of the activation of in-vehicle sensors or manually, which includes a minimum set of data (MSD) and establishes an audio channel between the vehicle and the eCall PSAP via public mobile wireless communication networks as described in clause 4.1 in 3GPP TS 26.267[15]

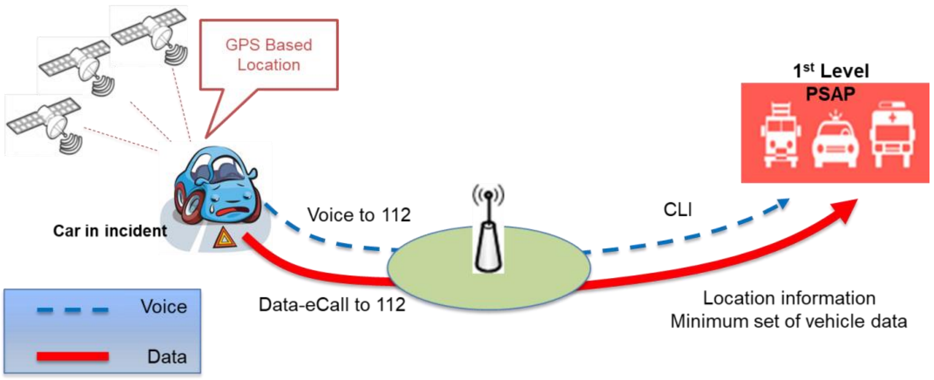

Figure 14 eCall system overview

The eCall equipped vehicle also sends an emergency message known as the minimum set of data (MSD), including key information about the accident, such as number of vehicle occupants, time, accurate location, driving direction resulting from accurate satellite-based data and vehicle description.

Optionally, the PSAP should be able to call back the car if the original 112 call is broken.

The deployment of eCall devices (CS eCall) was made mandatory in all new cars sold in the European Union since 1 April 2018.

7.2 Requirements

The eCall service requirements have been defined in Annex 27 in 3GPP TS 22.101[7]

7.3 Circuit-Switched eCall

Circuit-Switched eCall is applicable on 2G/3G and 4G (using CS Fallback)

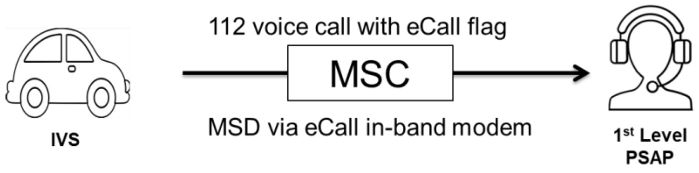

Figure 15 eCall over CS

In case of an eCall, the Network Access Device shall commence an emergency call set-up in accordance with ETSI TS 24 008[10] and included in the TS12 service category request message; the "eCall Flag" as specified in ETSI TS 22 10[7] and ETSI TS 24 008[10].

Data-eCall is based on in-band modem architecture. This means that the voice circuit is also used to transport Data information to PSAP as defined in clause 4.3 in 3GPP TS 26.267[15].

The present eCall In-Band Modem (eIM) solution consists of an In-vehicle System (IVS) data modem and a PSAP data modem, employing signals that have been designed to pass through modern speech codecs with only moderate distortion, yet providing sufficiently high data rates for quick MSD transmission.

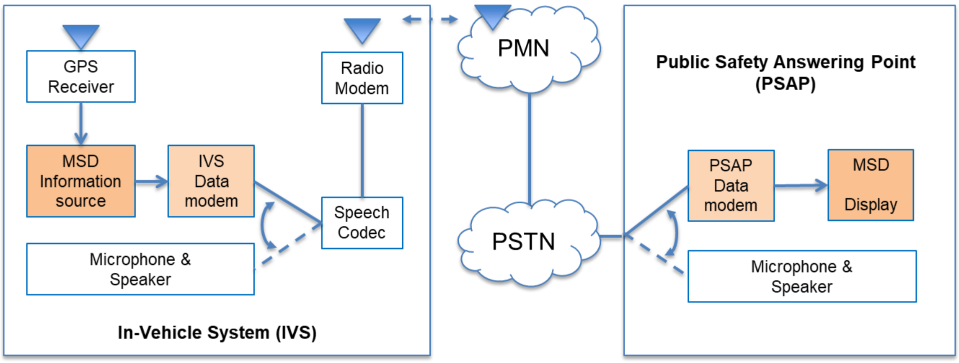

Figure 16 eCall system within the cellular system architecture

7.4 NGeCall (eCall over IMS)

NGeCall is applicable to 4G and 5G

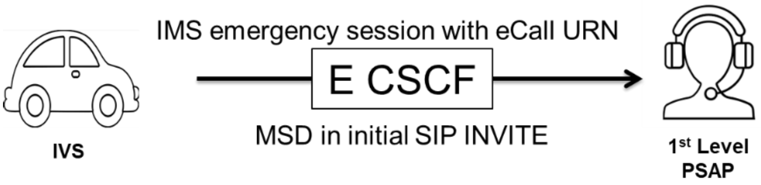
IMS emergency session with eCall URN
E CSCF
MSD in initial SIP INVITE
IVS
1st Level PSAP

Figure 17 eCall over IMS

IMS eCall aligns with normal IMS emergency call procedures as specified in 3GPP TS 23.167 [12]

The failure of receiving eCall service in one domain does not prohibit the UE from triggering the service in the other domain.

SIP profile for eCall over IMS is described in GSMA IR.92 [16] / GSMA NG.114[20].

Two use cases are identified with eCall over IMS depending on the PSAP capability to support NGeCall.

- PSAP supporting NE-eCall ➔MSD via initial SIP-INVITE
- UE has received the "eCall supported" indication as specified in 3GPP TS 23.401[17] / 3GPP TS 23.501[18].

UE includes eCall Flag (automatic, manual).

The voice session follows the normal IMS emergency services procedures. The SIP INVITE message carries the IMS eCall flag in the URN "urn:service:sos.ecall.automatic/or urn:service:sos.ecall.manual". "SOS.eCall" URNs instead of the service category in the CS emergency call setup message as described in clause 7.7.1 in 3GPP TS 23.167[12]

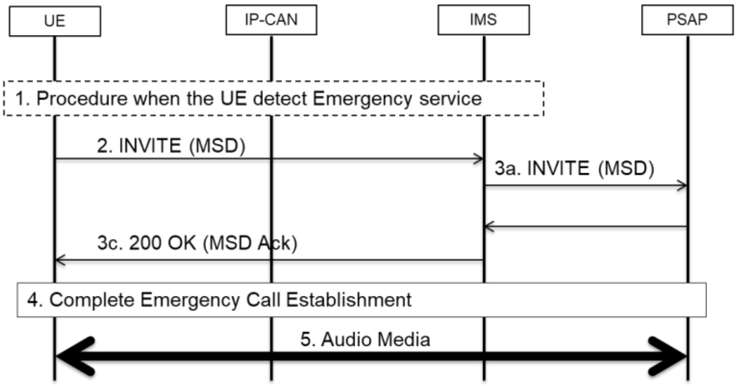
UE
IP-CAN
IMS
PSAP
1. Procedure when the UE detect Emergency service
2. INVITE (MSD)
3a. INVITE (MSD)
3c. 200 OK (MSD Ack)
4. Complete Emergency Call Establishment
5. Audio Media

Figure 18 NG-eCall Scenario with PSAP supporting NG-eCall

- PSAP not supporting NGeCall ➔ MSD via In-Band modem over VoIP
  This scenario may occur, when PS access is available, but the UE does not detect that the NG-eCall is supported and CS is not available. It may also occur when the UE detects that the IP-CAN supports NG-eCall and initiates an NG eCall but the session is handled by a PSAP not supporting NG-eCall.

The next figure illustrates a high level call flow for an interworking scenario between a UE and a PSAP via the CS domain as described in clause 7.7.2 in 3GPP TS 23.167[12]

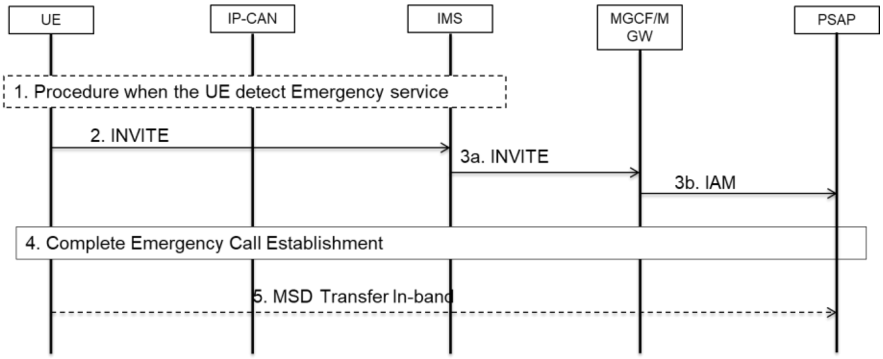
UE
IP-CAN
IMS
MGCF/M GW
PSAP
1. Procedure when the UE detect Emergency service
2. INVITE
3a. INVITE
3b. IAM
4. Complete Emergency Call Establishment
5. MSD Transfer In-band

Figure 19 eCall Scenario with PSAP not supporting NG-eCall

Note: Given the sensitivity of the in-band modem to time-warping that may be employed in commercial VoIP networks, the use of the eCall in-band modem is not recommended for operation over IMS. Besides jitter problems, the other limitations of CS eCall would remain with this option such as only 140 octets MSD, loss of voice channel, and delay in establishing a voice path.

8 Emergency calls over WLAN

8.1 General

The main issue related to Emergency Call using WLAN access is to provide relevant and trusted location information about the UE to the network to make possible routing to the appropriate PSAP.

Using WLAN access, it is only possible to rely on UPLI (User Provided Location Information), as it might be impossible to retrieve NPLI (Network Provided Location information) which is not standardized for VoWiFi.

A key question is to know if UPLI can be considered as a trusted information or not in case of EC.

It should be noted that GSMA PRD IR.51[21] already recommends that the UE shall not issue an emergency session over WLAN access to EPC if the emergency session can be established via 3GPP access like defined in 3GGP TS 23.402 [26].

But some operators may decide to block Emergengy Call using VoWiFi considering UPLI as a non trusted information.

It is recommended that the network should not block emergency calls over WiFi where it is unable to determine that the Ue has a cellular connection available.

8.2 IMS emergency services using WLAN access to EPC

The IMS emergency service using WLAN access to EPC described in the following section is based on 3GPP TS 23.167 V17.0.0 – Annex J (normative) [12] is only applicable to trusted WLAN access (S2a) and Untrusted WLAN access (S2b).

Note: The “roaming” use case is not include in 3GPP specification

Download of Emergency Numbers to the UE

Solution described in 3GPP TS 24.301 [13] still applicable but only occurs whenthe UE registers in a 3GPP network to download Emergency Number list.

This solution has drawbacks: for users flying to a foreign country and keeping the airplane mode enabled while activating Wi-Fi, the list in the device is not updated with the visited emergency number list. In consequence, a local dialed number might be wrongly considered as an emergency by device or an emergency call to a local number might be handled as a normal call in the HPLMN.

UE detectable EC

When the UE detects an emergency number, based on the mechanism described in section above, the UE shall initiate the IMS emergency session establishment using the IMS session establishment procedures containing an emergency session indication and any registered Public User Identifier . IMS emergency session is established after the UE selection via DNS query of ePDG able to support Emergency call like described in GSMA PRD IR.51

ePDG for EC selection and PDN connection for emergency services.

The UE performs ePDG selection for emergency bearer services based on the ePDG configuration information provided by the home operator in the UE via H-ANDSF[2] or via USIM, or via implementation specific means as specified in 3GPP TS 24.302 in section 7.2.1A [23].

The ePDG IP address to which the UE needs to from IPsec tunnel is discovered via DNS query (GSMA PRD IR.61[22]):

- If the UE is not roaming or cannot determine if it is roaming, the UE shall create a FQDN with the HPLMN ID.

Note: In such cases, there is no standardized solution for the UE to obtain the vPLMN ID.

- If it is known the UE is roaming and VPLMN ID is known, the UE shall create a FQDN with the VPMLN ID. DNS queries for ePDG selection are sent to the DNS server provided on the Wi-Fi Internet connection.

[2] ANDSF server is not available in any Orange affiliate’s network

Once the ePDG has been selected the UE shall initiated IPsec tunnel establishment procedure using the IKEv2protocol as defined in IETF RFC 5996 [24] and 3GPP TS 33.402 [25] and illustrated in the next figure.

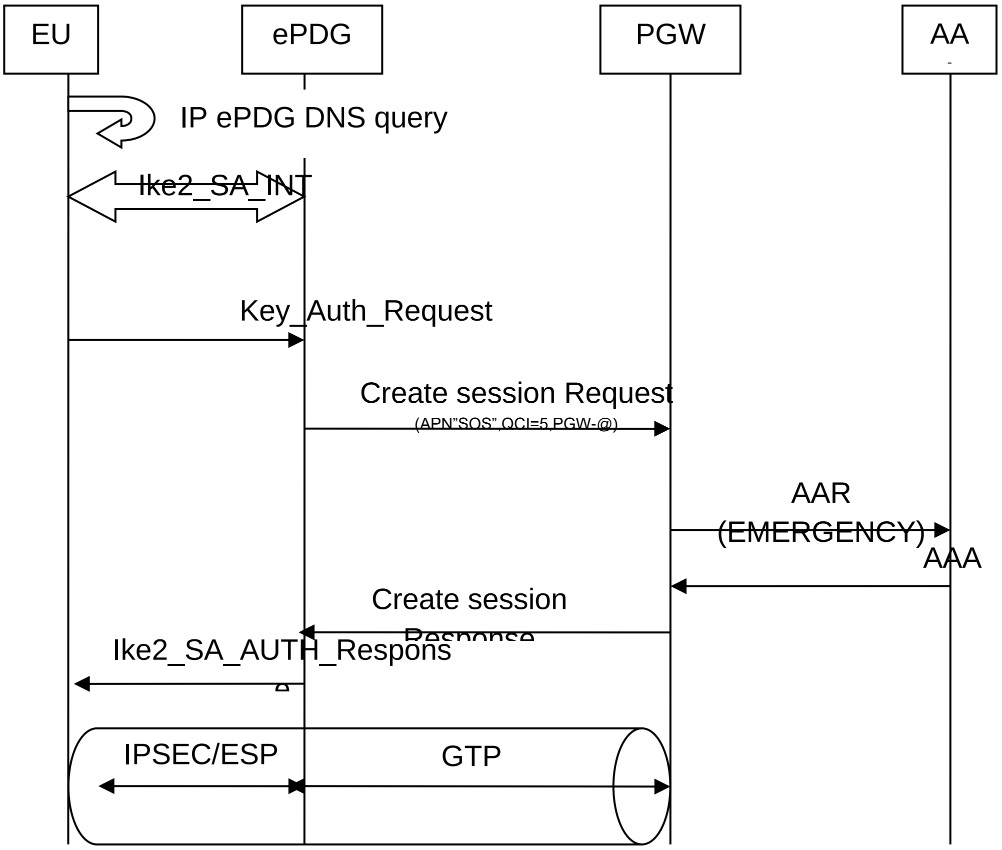

Figure 20- ePDG selection and Session creation

IMS Emergency session

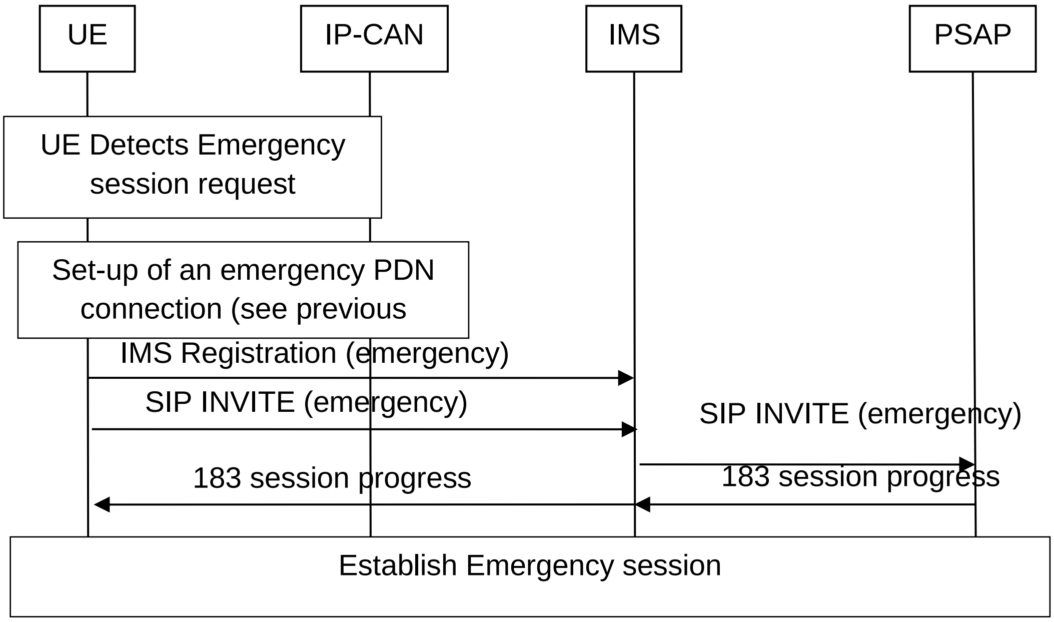
UE
IP-CAN
IMS
PSAP
UE Detects Emergency session request
Set-up of an emergency PDN connection (see previous
IMS Registration (emergency)
SIP INVITE (emergency)
SIP INVITE (emergency)
183 session progress
183 session progress
Establish Emergency session

Figure 21- IMS Emergency Session

When IMS network detects that the UE is establishing an emergency session over WLAN access to EPC while UE is not in its Home country, local policies in the Home IMS network may determine whether to nevertheless handle the emergency session.

In case of VoWiFi EC in abroad situation, Visited ePDG could apply LBO and connect Visited PGW to establish ims emergency session using Visited IMS network.

Note: LBO is only possible if Visited ePDG could be selected. In case ePDG selection in VPLMN fails, UE may be configured by the HPLMN (e.g. via H-ANDF, USIM, etc) with FQDN or IP address of an ePDG in the HPLMN as described in 3GPP TS 23.402 [26] in clause 4.5.4.3 to select HPLMN ePDG.

8.2.1 NON-UE detectable EC

UE can realize that a number need to be considered as an Emergency Number after being informed by the P-CSCF via SIP 380 Alternative Response (3GPP 24.229 [11]).

Note1:only relevant if LBO for Emergency call could be applied(see section above).
Note2:In case of VoWiFi EC in abroad situation, the P-CSCF could not be aware that UE is abroad (e.g., WiFi enabled in flight mode) making P-CSCF not be able to recognize all the ECN in the countries where the user is be located and making EC inefficient to connect visited PSAP.

Note 3: case of emergency over WLAN, no procedure exists in 3GPP specification to detect emergency number while UE is in roaming.

Annex A AML in 2G/3G networks

This annex describes AML in 2G/3G networks, comparing SMS and data cases.

A.1 SMS

Home network

In case of an emergency call, and after requesting voice call establishment to relevant PSAP, the device collects GNSS or Wi-Fi information and generates automatically one SMS to the PSAP including location information thus collected.

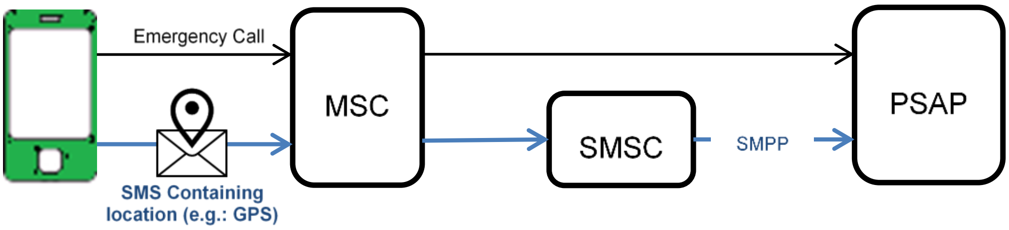

Figure 22 AML via SMS

It is important to notice that if GPS service is not active, the device will be able to activate GPS without any user action and then collect the location information.

Roaming impact

A major constraint with the SMS solution is related to the SMS home routing mechanism used in case of roaming. European Telecommunications Standards Institute (ETSI) proposes two options which are not recommended from the operational point of view (see Annex E). If SMS is used in case of roaming, it is recommended to use the visited network SMSC (see section 3.4.1).

A.2 DATA Push

Home

Instead of usingSMS to transport location information, data push across the network could be adopted if the data connectivity is considered to be sufficiently widespread and reliable. It relies on the end users having a data subscription and for data to be enabled in the handset.

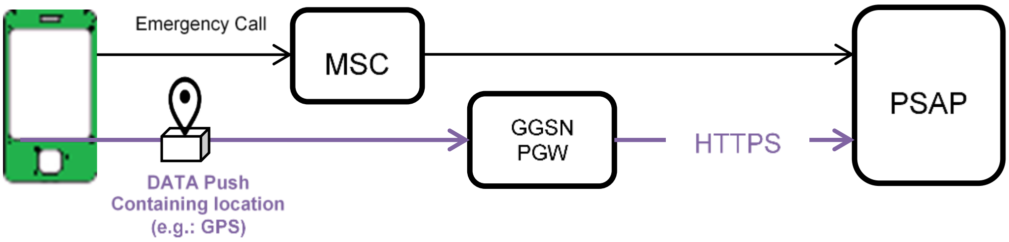

Figure 23 AML via DATA Push

A.3 Roaming impact

There is also a limitation which is; users are likely to disable use of data to avoid roaming charges (no more relevant in Europe – EU regulation “roaming like home”). This method has also the disadvantage that data cannot be zero-rated.

Advantage

The visited country in which the mobile handset is currently operating can be determined using the Mobile Country Code (MCC) component of the current cell ID. Based on this information, the device AML application embedded in operationg system could determine the Universal Resource Locator (URL) for a national location processing server to which the data may be pushed using the HTTPS message.

A.4 SMS and DATA push comparison

The table below outlines advantages and disadvantage for each solution.

SMS will be preferred to DATA push. SMS is a universal service offered by all mobile operators and not linked to DATA service availability and possibly disabled by customer when roaming abroad.

	SMS	DATA Push (HTTPS)
Advantages	Doesn’t require a data connection More reliable, lower failure rate (may vary by country)	More secure Unlimited size (can transmit more information than Data SMS, e.g. altitude, device model, etc.)
Disadvantages	May be more difficult to set up SMSC to correctly handle data SMS Not visible to other apps but still unencrypted over the network	Requires a data plan Unable to retrieve Mobile Subscriber (MSISDN) if not stored on SIM card In GPRS, CS and packet Switch (PS) traffic cannot happen simultaneously! Less reliable (varies by country) – unreliable on bad connection, higher failure %

Table 1advantages and disadvantage

Annex B AML in 4G/5G network – alternatives to SMS

This annex describes alternative solutions to SMS to transport location information.

B.1 DATA Push

DATA Push could be used but presents the same drawbacks as 2/3G already described in Annex A.3.

B.2 SIP INVITE

In the context of Emergency call management, four scenarios are defined in 3GPP TS 23.167 [12] to retrieve the caller location information:

- the UE knows its own location;
- the UE retrieves its location information from the network;
- the IMS core retrieves the location information. The related high level procedures are described below;
- location information is not needed to route the emergency call by the IMS core. Optionally the emergency routing determination and location information retrieval may be performed by the Emergency Call Server (ECS)

The objective of these four scenarios is to provide routing information based on customer location to make possible the Emergency session connection to the predefined PSAP determined by authority for the current customer location.

In the AML context, it is possible to use the first scenario and insert GPS information as geographical location information in the SIP INVITE (emergency). By using this proposition, PSAP receives the call and the caller location information in a single message, as illustrated on the next figure.

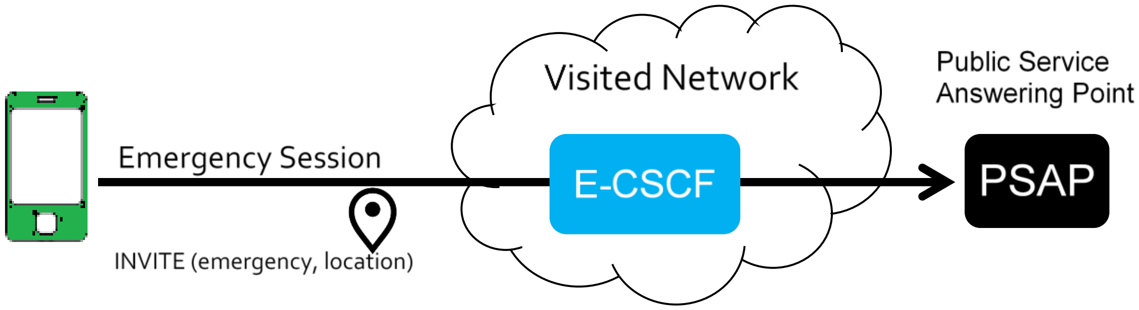

Figure 24 AML with SIP

This proposal has major drawbacks Device AML application needs to collect GPS information prior to initiating an emergency session, which could induce delay in the emergency session establishment AML application needs to interact with device dialler application to update SIP message with location information

Annex C AML: Location information format

This Annex describes the information conveyed in an AML.

C.1 Location information

The most important information transported in AML message is:

- Latitude
- Longitude
- Radius
- Time of Positioning (TOP)
- Level of Confidence (LOC)
- Positioning Method (G-GNSS or AGNSS, W-Wi-Fi signals, C-Cell, N- No possibility to determine the location)
- International Mobile Subscriber Identity (IMSI)
- International Mobile Equipment Identity (IMEI)
- MCC
- Mobile Network Code (MNC)

C.2 Transport method

AML location information could be transported to the PSAP using any of the following three options below:

- Regular SMS
- “Data SMS” (*)
- HTTPs protocol

(*) The reason for choosing this type of SMS is to ensure that the Operating System (OS) will not automatically store a data SMS in the user’s “send messages”.

All details regarding AML transport method and information format are defined in ETSI (ETSI TS 103 625 [3].

Annex D AML Implementation Examples

This annex provides the AML implementation status for smartphones and networks.

D.1 Devices

AML is supported in smartphones that use Android or IOS operating systems:

- Google announced in July 2016 that all Android phones from Gingerbread OS version include AML. Google call their implementation ELS (Emergency Location Service).
- Apple devices running iOS 11.3 or later also support AML as 30 March 2018.

AML is not an applet. However, the technology is activated by the OS provider (Google and Apple) on a country per country basis once the national authorities are technically and operationally ready to receive such information.

D.2 Networks / Countries

Country	EMA	FRS	Police	Other services	Activated numbers
Austria	X	X		Mountain rescue, Water rescue, HEMS	122,128,144,140,141
Belgium	X	X	X		112,100,101
Estonia	X	X	X		112
Finland	X	X	X		112
Iceland	X	X	X		112
Ireland	X	X	X	Coastguard	112,999
Lithuania	X	X	X		112,101,011,102,022
Moldova	X	X	X		112,901,902,903
New Zeeland	X	X	X		111,001,112,999,911,117
Norway	X	X	X		110,112,113
United Arab Emirates			X		999,112,911
United Kingdom	X	X	X		112,999
United States	X	X	X	Other organization processing 911 calls	911

Table 2 Table is extract from EENA document [6]

D.3 Implementation example: Orange Belgium

This Annex presents Orange Belgium implementation to provide AML for Orange Belgium customers and visitors.

Initial AML design for Orange Belgium users

The figure below describes the initial AML SMS flow limited to Orange Belgium customers. The design was based on standard SMSC address (+32495002530).

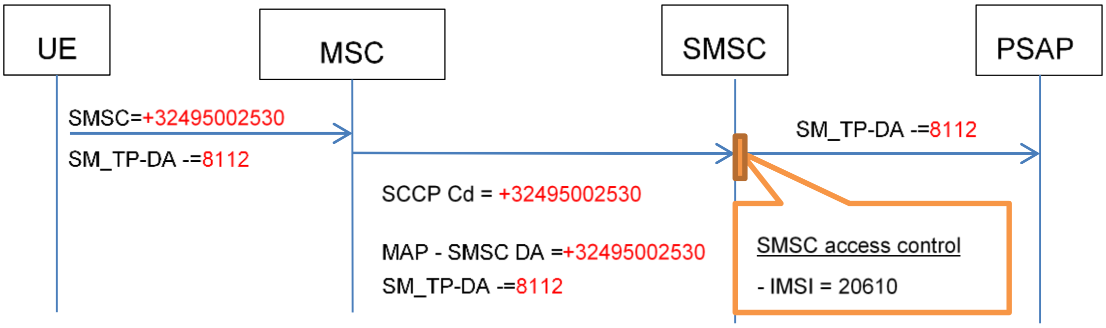

Figure 25 AML call flow for home customers

Roaming AML design for inbound Roamers

The roaming AML design is based on SMS routing within the Visited Network.

- Google devices use new SMSC address (+32112) for the AML SMS
- MSC adapts Called SCCP Address and SMSC address (+32112 to +32495008112) and routes the SMS to the local SMSC (+32495008112)
- SMSC access is limited to AML SMS: Orange Belgium visitors are just allowed to send SMS to 8112 destination.

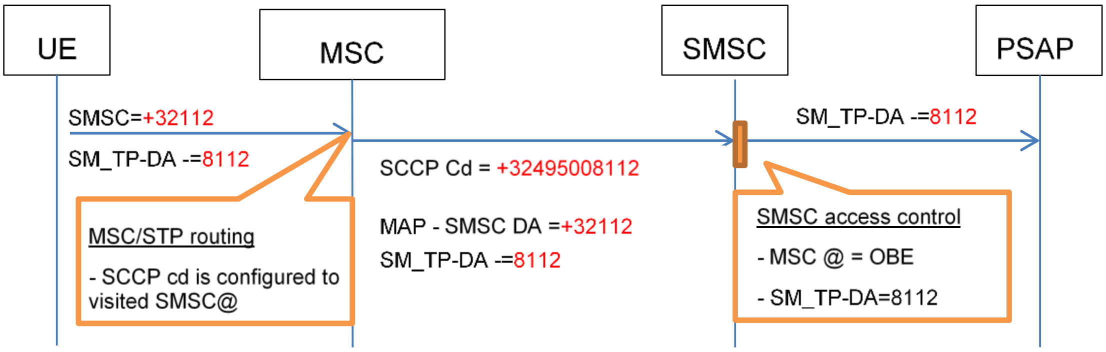

Figure 26 AML call flow for home and inbound Roaming customers

It is important to notice that the two solutions could coexist during a transition period of time.

For testing purpose, a specific SMS content is defined with the PSAP: Testreg. PSAP should automatically send back a TEST SMS OK to confirm that SMS is correctly reaching PSAP.

Finally, Call Detail Record (CDR) generated by the MSC will be rated to zero like all emergency calls (based on SMSC address = +32112).

Annex E ETSI proposals for AML related to Roamers

ETSI proposes in ETSI TS 203 178 two SMS options in case of roaming:

Option 1 - handset loop within internal AML DB containing PSAP long number for the current location. Location emergency SMS is routed to the home SMSC. As soon as long as it is a full MSISDN length Home network should be able to route back the SMS to the visited PSAP.

Note: to guarantee SMS free of charge, specific agreements should be put in place between the Visited and Home network.

Option 2 – if it not possible to use a full length MSISDN for each country, then it is mandatory to interconnect AML servers of the two countries. In this case, Visited Mobile Country Code and Visited Mobile Network Code will be used to forward the AML information form the PSAP in the Home country to the PSAP the visited country.

The two options are illustrated in the Figure 19.

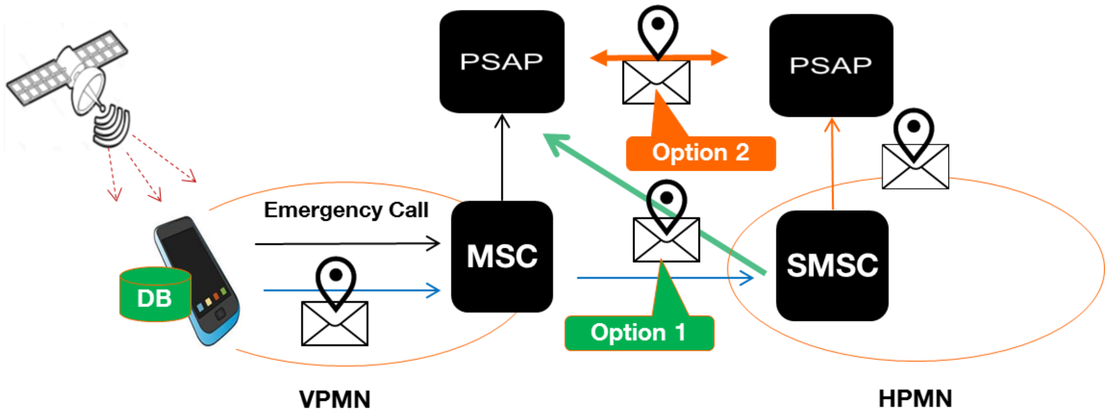

Figure 27 AML SMS Roaming options

The above solutions are not recommended from an operational point of view for the following reasons:

Option 1 - Required full length MSISDNs PSAP in each country. In addition, the maintainance of a data base will be difficult. Moreover, for the SMS, Home Routing and SMS termination on the Visited PSAP will still depend on the SMS interworking availability between the two countries.

Option 2 – To define a solution requiruing that all PSAP are interconnected together is not realistic.

For both options, a specific agreement between the parties should be put in place to make this SMS, free of charge for end users.

If SMS is not used in case of roaming other alternatives must be defined.

Annex F List of Non UE detectable emergency numbers

A list of non UE detectable emergency numbers is available hereafter.

20220303_Q_emrgency_list (report) - on

This information could be useful to provision in the Home IMS in order to reject (using 380 release cause) the non UE detectable emergency call (section 2.4.2).

The following parameters are used with the following format:

- Country: country name
- Iso-country: Iso code of the country
- MCC: Mobile Country Code
- Emergency number: contains the non UE detectable emergency number
- Type: Police, Ambulance, Fire
- URN: URN information should follow sub-clause 9.9.3.37A of 3GPP TS 24.301
- Source: IR.21 (if information validated in IR.21

Note:

The list contains only the non-UE detectable emergency number related to Police,

Ambulance or Fire which could be redirected to visited PSAP

Note:

Countries having only the UE detectable emergency numbers (112, 911) are not mentioned in this list.

Sources

- Collected with IR.21 (still not a lot …)
- EENA information
- Wikipedia

Annex G Document Management

G.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	18 June 2019	Internal version input for REGI #1 Emergency Call and AML in 2/3G		Eddy GOFFIN (ORANGE Belgium nv/SA)
0.2	7 Oct 2019	4G introduction		Eddy GOFFIN (ORANGE Belgium nv/SA)
0.3	7 January 2020	5G introduction Section 3 AML - SMS focus (Alternative solutions put in annex)		Eddy GOFFIN (ORANGE Belgium nv/SA)
0.4	8 November 2020	CR1001	GERI#7	George Foti, (Ericsson); Eddy GOFFIN (ORANGE Belgium nv/SA)
0.41	18 January 2021	Validation during NGR meeting	NGR#1	Eddy GOFFIN (ORANGE Belgium nv/SA)
1.0	2/07/2021	CR.1002	TG	Eddy GOFFIN (ORANGE Belgium nv/SA)
1.1	10/05/2022	CR1003 New section for eCALL CR1004 Update Annex F - List of Non UE detectable emergency numbers	NRG	Eddy GOFFIN (ORANGE Belgium nv/SA)
1.2	30/05/2023	NRG 015_006 - NG.119 CRxxEdGo - ECoWiFi r1.5 NRG 017_005 NG.119 CR on Video Interoperability with PSAPr2	NRG NRG	Eddy GOFFIN (ORANGE Belgium nv/SA) George Foti, (Ericsson)

G.2 Other Information

Type	Description
Document Owner	NG-NRG
Editor / Company	Eddy Goffin/Orange

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.