ETSI TS 103 625 V1.1.1 (2019-12)

Emergency Communications (EMTEL);
Transporting Handset Location to PSAPs for
Emergency Calls - Advanced Mobile Location

Reference
DTS/EMTEL-00044

Keywords
emergency, handset, location, mobile, transport

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Special Committee Emergency Communications (EMTEL).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

One of the biggest challenges facing the Emergency Services is determining the location of mobile callers. Cell based location has been available to the Emergency Services since 2003. While cell data can help with verbal establishment of a caller's location, a more precise location will allow an even quicker emergency response.

Advanced Mobile Location (AML) allows use of native smart phone technology to pass (Assisted) GNSS or Wi-Fi based location data to Emergency Service PSAPs. These technologies can provide a location precision as good as 5 m outdoors (and averaging to within circular areas of ~25 m radius for indoor locations), a significant improvement on existing cell coverage provided by mobile networks, which average (across the UK as an example) circular areas of about 1,75 km radius.

The present document builds on the Advanced Mobile Location initiative described in ETSI TR 103 393 [i.1] now being used in an increasing number of countries to improve the precision and accuracy of a caller's location information for emergency calls from mobile handsets.

1 Scope

The present document describes the transport methods used for AML messages with handset derived location information and associated data, the content of the AML messages, and allows for the data sent within the message to include further attributes than supported in current deployments.

It also considers the future evolution of transport methods as PSAPs, networks and terminals become increasingly IP based.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 123 040: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Technical realization of the Short Message Service (SMS) (3GPP TS 23.040)".

[2] ETSI ES 203 283: "Protocol specifications for Emergency Service Caller Location determination and transport".

[3] IETF RFC 6442: "Location Conveyance for the Session Initiation Protocol".

[4] IETF RFC 5491: "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations".

[5] ETSI TS 103 479: "Emergency Communications (EMTEL); Core elements for network independent access to emergency services".

[6] ETSI TS 123 038: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Alphabets and language-specific information (3GPP TS 23.038)".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 103 393 (V1.1.1): "Emergency Communications (EMTEL); Advanced Mobile Location for emergency calls".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3G (mobile) Partnership Project
AGNSS	Assisted Global Navigation Satellite System
AML	Advanced Mobile Location
ASCII	American Standard Code for Information Interchange
DCS	Data Coding Scheme
GNSS	Global Navigation Satellite System
GSM	Global System for Mobile
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICCID	Integrated Circuit Card IDentifier
IEI	Information Element Identifier
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LOC	Level Of Confidence
LS	Location Server
MCC	Mobile Country Code
MNC	Mobile Network Code
MNO	Mobile Network Operator
MSISDN	Mobile Station International Subscriber Directory Number
NG	Next Generation
NTP	Network Time Protocol
OS	Operative System
PDU	Packet Data Unit
PSAP	Public Safety Answering Point
RFC	Request For Comments
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMPP	Short Message Peer to Peer
SMS	Short Message Service
SMSC	Short Message Service Centre
UCS	Universal Character Set
UTC	Universal Time Coordinated
WGS	World Geodetic System

4 Overview

AML functionality is triggered by an emergency call (which is progressed normally by the handset and the network), and is designed to supplement the basic network location provided 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 (e.g. through use of SMS) to the Emergency Service PSAPs. Handsets can use more than one location technology to establish a location, for example the handset may combine location information from Cell and Wi-Fi sources to obtain the best possible, "hybridised", result.

It is important that AML doesn't interfere with the voice call so both the handset and mobile network shall be configured to be able to simultaneously support a standard 3GPP mobile emergency voice call, location determination using GNSS/Wi-Fi capabilities and SMS and/or HTTPS transmission of the location information over the 3GPP mobile network.

5 Handset Functionality

5.1 Positioning methods and time needed to precisely locate

GNSS, or Assisted GNSS, normally offers the best location information but is slower than other methods. At the other end of the spectrum cell based location is quick but typically returns a larger location area. The general rule is that PSAPs need the best data as long as it doesn't take too long to determine, so a 'send us what you have now' timeout [T1] is used.

T1 is the maximum time between the emergency call being initiated and the location message being sent. T1 should be configurable with a T1 value selected in consultation with the provider of the AML functionality on the handset to give best balance between quicker availability to PSAPs and the even higher precision that may become available with a longer T1.

As soon as the emergency call is initiated the handset shall immediately attempt to determine the best possible current location within the period set by the T1 timeout.

This should allow all location capabilities that the handset provides to be used, respecting the end user's preferences by enabling any capability not normally available only to assist for AML functions on an emergency call, and subject to a battery check.

If it is not been possible to get a location from any method then a message shall be sent indicating that all positioning methods have failed.

5.2 Triggered by emergency call without impacting voice

The AML software shall be integrated into all existing emergency call mechanisms available on the handset including manual dial of 112 (or any other national emergency number specified for the mobile network and country being used), and use of the Emergency Call button (as appropriate).

In an emergency callers are often stressed or panicking so it is important that the AML functionality and transmission of the AML message shall be automatically triggered without any manual intervention by the user. The handset software shall be invisible to the users so as not to cause confusion when they are trying to get help, and so as not to attract attention from those who intend to abuse the facility. No record of the AML message shall be available to the user either during or after the emergency call.

If an emergency SMS service, typically for deaf or hard of hearing users is provided in a country, then AML should also be triggered by an emergency SMS message being sent.

5.3 Availability of MSISDN

PSAPs need to be able to match the voice call with the AML data, and to do so they use the MSISDN (Mobile Subscriber ISDN). The MSISDN is included within an SMS message so this is straightforward if SMS is used for AML transport. In some instances, the MSISDN can be accessed by the handset's AML functionality and, if AML is using HTTPS to transport the location data, it shall therefore be included when possible in the HTTPS data string (see clause B.1).

5.4 Data connectivity

The mobile handset requires data connectivity to allow communication with servers operated by the providers of the phone's operating system that:

a) provide assistance information to allow quick establishment of a GNSS position (AGNSS); and

b) provide access to primarily crowd sourced databases for location information related to Wi-Fi access points.

In addition such a data connection may support one of the transport mechanisms for AML using an HTTPS message (see clause 6.3).

This data connectivity can be through the mobile network or Wi-Fi access points.

Without such a data connection AML messages are still possible using a GNSS location (without assistance) and SMS transport (see clause 6.1).

5.5 Battery life

Before invoking the AML functionality, the handset should check there is sufficient battery life so that the caller can still make a short 5 minute voice call. The priority in the emergency situation is to allow voice connection to the PSAP.

6 Location data and data transport

6.1 Location data provision by the handset

6.1.1 Data provided

AML is required to communicate a location in the form of a circle.

The location and size of the circle determined by the handset shall be communicated using the attributes of a WGS 84 latitude and longitude measured in decimal degrees for the centre of the circle, and a radius measurement for the location circle in metres. A precision of 5 decimal degrees should be provided which will equate to 1,1 m precision on the ground.

The following attributes are those that are normative for implementation using transport methods described in clauses 6.2 and 6.3:

- The Time of Positioning (TOP): The accuracy of this date and time is important as it will be used to filter out any messages that appear to be too old or have a time in the future. In the first instance the handset should attempt to use the time established by an NTP server, this should be possible if a network connection is available. If NTP is not available then GNSS can be used to give time. Only if these two methods fail then, as a last resort, the handset time and date can be used.

- The Level of Confidence is a percentage probability that the mobile handset is within the area being communicated, for example a 95 % value tells the Emergency Services that there is a 5 % probability that the caller is not within the location area specified by the latitude, longitude and radius values. It is recognized that methods for determining mobile handset location have limitations. For example, the impact of buildings, topography and weather conditions introduce a margin of error into location calculations, and different methods will have different error factors that need to be communicated to the Emergency Services.

- The predominant positioning method used to determine the location area is indicated as one of the following:
  - GNSS or AGNSS;
  - Wi-Fi signals;
  - Cell;
  - Hybridised results shall be used and should be classified according to predominant location method.

  It shall also be indicated if it has not been possible to determine the location - see annexes A and B.
- The SIM card identifier of the handset that has made the emergency call (IMSI) and the identifier of the handset that made the emergency call (IMEI).
- Mobile Country Code of the network, used to confirm/determine the country in which the emergency call was made.
- Mobile Network Code, to confirm/determine the mobile network used to make the emergency call.

NOTE 1: The MCC and MNC of the network will normally be the same as the MCC and MNC within the IMSI. Differences between them indicate if the handset is roaming.

A header attribute shall be used to differentiate AML messages from other emergency SMS messages and to also indicate a version number for the interface. For SMS transport, a Message Length attribute shall also be used - see annex A.

In future, when it becomes technically feasible and reliable, and if the transport method has sufficient space available, the following optional information should be passed and the inclusion of additional data indicated by use of a different interface version number:

- Altitude (in metres above the WGS 84 ellipsoid).

NOTE 2: The WGS 84 ellipsoid is a reasonable approximation for the shape of the earth. Altitude above the WGS 84 ellipsoid can differ from the actual altitude above mean sea level.

- Altitude Variance: Indicates the vertical variance, plus or minus, from given altitude.
- Floor number.
- Emergency number used to make the call, including whether voice or SMS activation (to assist PSAPs matching with calls).
- Source to indicate which version of the handset's AML functionality is being used. This is helpful in diagnosing any issues.

The presence of most of these optional information elements is already included for HTTPS - see annex B.

6.2 SMS transport

6.2.1 SMS transport overview

When a PSAP selects SMS transport (see clause 8), the standard mobile network SMS service shall be used to send the AML message from the phone to the SMSC (SMS Centre) within each mobile network (using normal 3GPP network standards).

The Short Message Peer-to-Peer (SMPP) open industry standard protocol for transfer of short message data outside mobile networks should then be used to transport the data from the SMSC to the SMS Aggregator (organization that aggregates SMS messages from various mobile networks).

The Aggregator should then forward the message to the PSAP using an Aggregator-defined format, typically an HTTPS post message that includes all the AML data, including the MSISDN which forms part of the SMS message. The PSAP then makes the AML location available to be used to supplement the location available from the mobile network. Either the Aggregator or the PSAP operating the AML Reception server may decode the binary data within the SMS payload - see clause 6.2.2.

Figure 1 shows how the AML location may reach a PSAP organization. The exact details for how AML information is made available to the PSAP that has received the associated voice call will vary from country to country, depending on how PSAPs are organized in that country. This is considered further in clause 8.

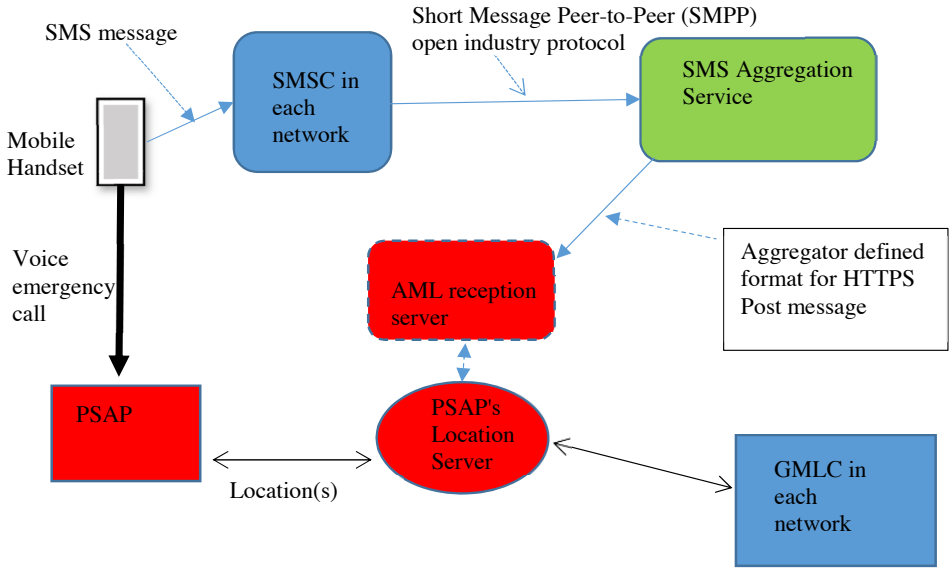

Figure 1: Example of AML location path to reach a PSAP

Figure 2 gives an example of the SMS message used in the AML solution.

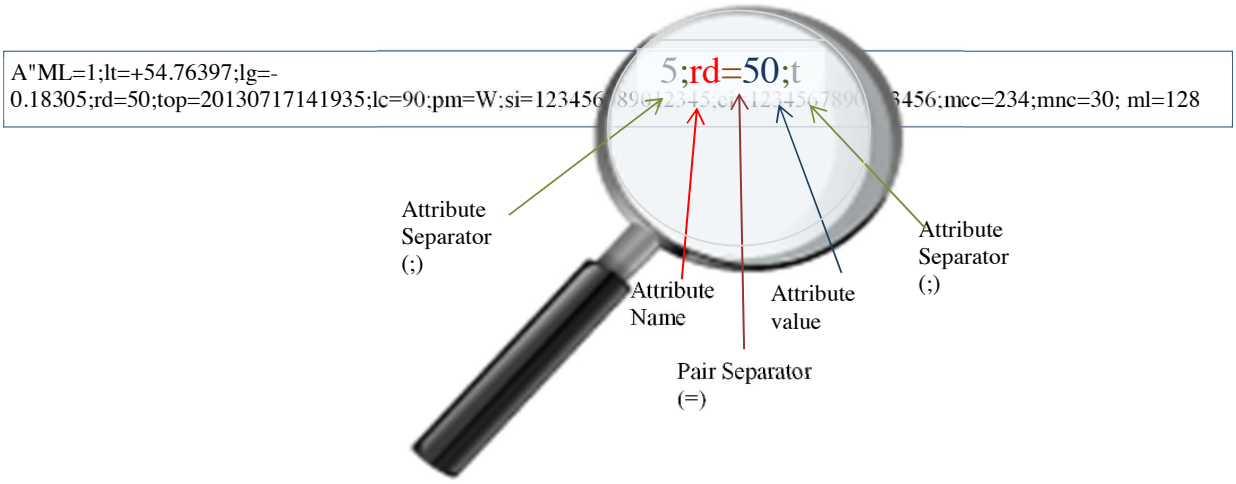

Figure 2: Example of SMS message for AML

More important attributes (latitude, longitude, radius) will appear at the beginning of the SMS with less important attributes towards the end. The tables in annex A give a detailed description of each attribute with the ordering of attributes in the table also how they should normally appear in the SMS.

To assist with compatibility, servers shall be able to process the attributes in any order in which they are received. Servers shall also be able to ignore any attributes that are not recognized while still processing the other attributes.

6.2.2 SMS Formats

It is important to note that 2 types of SMS are used to provide the AML location information. Which type of SMS is used may depend on the options open to handset manufacturers or Operating System (OS) providers to suppress a record of a sent AML location message on the handset:

a) Regular SMSs are used by handset manufacturers providing their own OS and AML service. These handset manufacturers can readily suppress the AML messages from the "sent messages" section of the smartphone. The processing of such regular SMSs is widely known and not discussed further in the present document.

b) So-called "Data SMS". The reason for choosing this type of SMS is to ensure that the Operative System (OS) will not automatically store a data SMS into the user's "sent messages" section. "Data SMS" is a particular subset of the SMS standard (ETSI TS 123 040 [1]). It is important to note that this is NOT an SMS message sent through a data connection, this is simply an SMS which contains a particular type of binary data format as a payload, and is addressed to a particular port on the receiving end (calling it a Data SMS is a bit of a misnomer for this reason). These types of SMS are not as familiar but are in common use by mobile networks, for example in setting the Voice Mail waiting indicator on a phone (or other network services), or for over the air handset updates, or for changes to SIM card settings.

As these "Data SMSs" are less familiar more detail is provided. The SMS sent from the handset to the mobile service centre (SMSC) is an SMS-SUBMIT (mobile originated) PDU type message. SMSCs are required to receive these messages without problems as they are part of the normal SMS standard. In the following, an SMS-SUBMIT message from the handset to the SMSC is considered, which follows normal SMS standards (ETSI TS 123 040 [1]).

The fields within an SMS message include: the SMSC number, sending address (caller's MSISDN), as well as the Protocol Data Unit type with a protocol identifier (00 - default short message), the DCS (data coding scheme), a time stamp and user data length. This is then followed by the User Data which is the AML message in this case.

The "Data SMS" is a subset of normal SMS that:

- Has the User-Data-Header-Indicator flag set in the PDU type field of the SMS message.
- Contains a User-Data-Header within the User-Data of the SMS.
- The User-Data-Header contains an application port address Information-Element-Identifier (IEI). The port number shall be fixed by each OS provider and made known to the PSAPs receiving AML messages.

Note that the particular Data-Coding-Scheme (DCS) is not specified here. The DCS is used to identify the encoding within the User-Data segment. There are three options currently for the DCS:

- GSM 7-bit default alphabet (which includes national language shift tables) and is used for regular text messages in Europe.
- UCS-2 (for 16 bit characters).
- 8-bit data.

If the selected DCS is 8-bit data, the standard does not make any particular guarantees about the details of the encoding. Given that the User-Data segment has a maximum of 140 bytes, and that the minimum size of a User-Data-Header that includes port information is 7 bytes (a length field plus 6 bytes to indicate the port number), this leaves a maximum of 133 bytes to encode the actual AML emergency message. In order to maximize the amount of information in the AML message, even if the 8-bit DCS flag is set, the encoding used by the OS provider should be the GSM 7-bit alphabet, with each 7-bit encoded element occupying only 7 bits, not 8 bits. So the AML information is packed using 7-bit characters, giving a maximum of 152 characters for the AML message, so the first 7 bits of the first byte make the first character, then the last bit of the first byte and the first 6 of the second make the second character and so on. The definition of the 7 bit encoding can be found in ETSI TS 123 038 [6] (see clause 6.1.2.1.1 specifically).

NOTE 1: The 7 bit encoding originally used by the AML in legacy implementations of Data SMS differs in one aspect from that expected in that when the AML message is encoded with ETSI TS 123 038 [6], it is done so in big endian byte order, rather than the expected little endian byte order. While continuing to support the originally used version, any new country implementations should follow the expected byte order of the ETSI TS 123 038 [6].

The PSAP receiving the AML SMS message forwarded by the SMSC (and any SMS Aggregator in the chain) should decode the AML payload found in the User Data segment of the SMS using the above knowledge of how the message is constructed.

NOTE 2: Handsets do not store a "Data SMS", because these are addressed not only to a particular destination through the destination number, but to a particular port, and normally need particular data decoding. That port usually means a specific application of some sort on the receiver. It would therefore be inappropriate to store/show this as a regular SMS, as the "Data SMS" may only have been intended for one particular application, not the handset in general.

6.2.3 Security of SMS transport

SMS access to the mobile network is authenticated and is also encrypted over the air between the handset and the base station.

In terms of interception on the air interface there is a very low risk for individual users as AML SMS is only triggered when an emergency call is made, which is a random event for individuals in any location.

6.2.4 Limitations

6.2.4.1 Roaming

For international roaming, there are challenges since an SMS is returned to the home country's SMS Centre for routing.

One option that may be used is, for example, to send a message from a phone in the UK with a foreign SIM to the UK AML destination using a "long number": a full length E.164 number including country code, e.g. +44NNNNNNNNN (N representing digits in a normal UK telephone number), which although it looks like a normal mobile phone number is a "virtual mobile number" as it doesn't terminate on a mobile phone, but can be routed by the hosting mobile network to a network termination point, in this case a PSAP. This avoids the issue of the foreign SIM's home SMSC not being able to route the normal 999 code for UK AML messages back to the UK AML destination. However it does mean that the SMS is not automatically zero charged.

NOTE: A number of other options are being considered to allow the AML SMS message to be routed using the visited network's SMSC to the visited country's PSAP. One approach being piloted is that a handset that is roaming uses the MCC of the visited network to alter the normal home SMSC number to which to specifically send the AML SMS, adding the CC (Country Code) to 112 as the SMSC destination for AML: for example the SMSC number used by a roaming device in Belgium would be + 32112. This would then also require the IMSI check by the visited SMSC to be modified, as normally, SMSCs will not process messages from IMSIs for which they are not the home network . However, unless one of these approaches proves practical, the AML functionality should either be used with a long number as described, or should be turned off when roaming.

6.2.4.2 Limited Service State/National Roaming

In case the citizen initiates an emergency call but the handset has no coverage from the home MNO, the call is handled by another mobile network operator with signal coverage in that area. In this limited service state it is currently not possible to send an SMS, as the technical standards only allow emergency voice calls (normally without it being possible to supply an MSISDN), nor would transport using HTTPS always be possible (which requires a data subscription to be verified on home network or a Wi-Fi connection).

6.3 HTTPS

6.3.1 Overview of using HTTPS

When a PSAP selects HTTPS transport (see clause 8.1), HTTPS POST messages shall be used to transfer the emergency location information and associated data described in annex B.

The AML endpoint (AML Reception Server in figure 1) provided by the PSAP (see clause 8.1) shall be capable of receiving HTTPS messages and should generally be able to handle messages with missing/malformed fields. It is recommended that, with exception of those fields with key data described in clause 6.1.1, every other field should be considered optional to ease message handling.

Endpoints shall return 2XX success codes to indicate successful reception of the HTTPS message.

6.3.2 General Format

The web-based AML messages are sent using the HTTPS protocol, which offers encryption and authentication to secure the delivery of location messages. Each message consists of a number of header fields and a body, holding the content for the message. For an AML message it shall use the common format used for web-based forms, sending the media using a MIME type of "application/x-www-form-urlencoded".

6.3.3 Security considerations

There are two possible routes for the message to be sent to the Public Safety Answering Point (PSAP). Either the message is sent directly from the handset, or it could be sent via an intermediate server (i.e. not the AML endpoint server):

a) If direct from the handset, the handset's Operating System (OS) will not be expected to provide any extra header information in the message.

NOTE: The PSAP should make sure their server is robust enough to handle false messages, badly formatted messages and denial of service attacks, since it should be available to any other node on the internet.

b) If the messages are sent via an intermediate server it should include the extra header fields specified in the detailed format description in clause 6.3.4. These will help confirm the sender and categorize the messages. In addition the PSAP server would only need to open its firewall to the intermediate server, so PSAPs would have a more trusted connection.

In either case a signed certificate shall be provided by the PSAP server to assure the handset or intermediate server that the data is being sent to a valid receiver.

6.3.4 Header

The HTTPS header contains a number of standard fields, including content-type, content-language and so on.

As noted above, if an Intermediate Server is being used it is also recommended to include extra header fields to help deal with the messages. A password would increase security slightly, a message type would help the PSAP categorize messages in terms of the source operating system, and a message ID would allow the intermediate server to resend messages in case of failure or to send to multiple PSAP servers to improve resilience. (It is recommended that a PSAP has at least two servers and an intermediate server sends to both for resilience.)

6.3.5 Body

The body of the message shall consist of a number of name-value pairs, just as for any web-based form application. These shall hold the values sent from the handset, including location details and handset identification. This is not a fixed length message and not all name/value pairs are required as detailed in annex B.

6.3.6 Detailed Format

6.3.6.1 Header

The following fields should be added to the HTTPS header by an intermediate server to help the PSAP in dealing with the message.

Table 1

Name	Format	Description
MsgType	String up to 16 chars	Operating System used by originating handset
Password	String up to 16 chars	Simple string agreed between service provider and PSAP as an extra confirmation of the source system
AMLMsgID	String up to 40 chars	Unique ID to identify the message being forwarded. Reused if sending to multiple servers or resending a failed message

6.3.6.2 Body

The data should come through in the body of the POST message as a block of text following the x-www-form-urlencoded format: using the & character as a field separator and the = character to separate field name and value. A portion of the message will look like this:

….location_time=1471528826884&cell_home_mcc=234&device_imsi=234109003946194&cell_home_mnc=10….

If the field values contain any reserved characters (such as & which is used with specific meaning in this MIME type) they should be replaced using the form %XX, where XX is the hexadecimal value for the character in the ASCII character set. Space characters should be replaced with a plus sign, +.

Table B.1 shows the fields to be used in the message. Note that if it has not been possible to determine the location, the location_source is described as Unknown and then the latitude, longitude, radius and accuracy should still be included but the values set to zeroes.

6.3.7 Receipt of HTTPS Message by PSAP

6.3.7.1 Overview of message receipt

To receive HTTPS messages PSAPs shall implement a web server application that receives the HTTPS messages.

6.3.7.2 Example Message Sequence

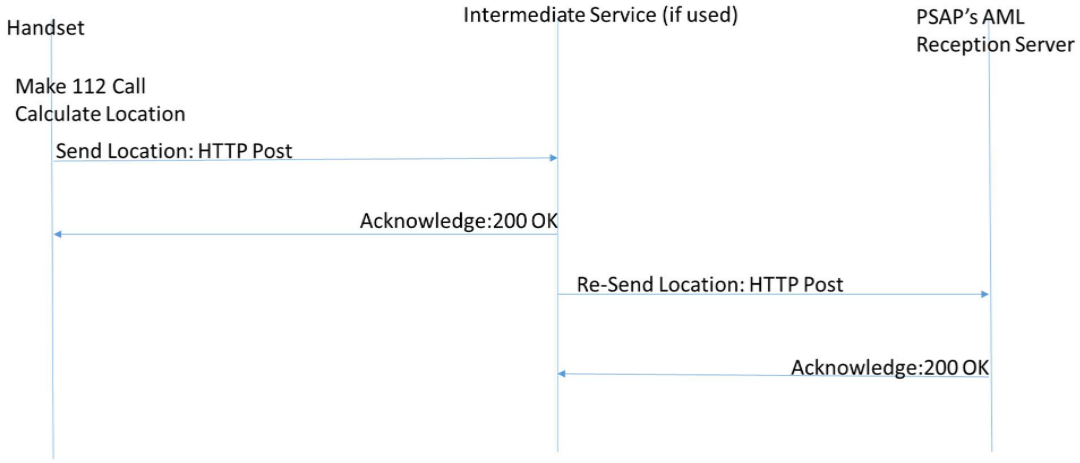

Figure 3

6.3.7.3 Example Message Content

The following text shows an example message body from an HTTPS message, including the optional fields (for example device_model). Note that there are no spaces in the text.

```
v=3&device_number=%2B447477593102&location_latitude=55.85732&location_longitude=-
4.26325&location_time=1476189444435&location_accuracy=10.4&location_source=GPS&location_certainty=83
&location_altitude=0.0&location_floor=5&device_model=ABC+ABC+Detente+530&device_imei=354773072099116
&device_imsi=234159176307582&device_os=AOS&cell_carrier=&cell_home_mcc=234&cell_home_mnc=15&cell_net
work_mcc=234&cell_network_mnc=15&cell_id=0213454321
```

Without the optional fields the message is more compact:

```
v=3&device_number=%2B447477593102&location_latitude=55.85732&location_longitude=-
4.26325&location_time=1476189444435&location_accuracy=10.4&location_source=GPS&location_certainty=83
&device_imei=354773072099116&device_imsi=234159176307582&cell_network_mcc=234&cell_network_mnc=15
```

6.3.7.4 Response Values

The standard HTTP values shall be used for the response message from the PSAP server. In particular the following values shall be used:

- 200 - OK, and other 2XX codes should also be accepted.
- 400 - bad format.
- 401 - authentication failed.
- 500 - internal server error.

The HTTP response code should only be used to signal the success/failure of the HTTP request itself, not delivery of the message content to the PSAP.

6.3.8 Limitations

6.3.8.1 Availability of MSISDN

Emergency services need to be able to match the voice call with the data message, and to do so they can use the MSISDN (Mobile Subscriber ISDN Number). In some instances, the MSISDN can be accessed by the handset's AML functionality (e.g. from the SIM card or information entered by the subscriber) and it shall therefore be included in the HTTPS data. However, in other instances the MSISDN is not accessible and therefore emergency services can't directly match the voice call with the location data string.

One option to allow matching is to receive AML messages using both SMS and HTTPS, then to match them by using the IMSI information received in both, and then match to the emergency voice call using the MSISDN within the SMS message. This can be useful if the PSAP requires the additional fields present in the HTTPS message, but not within the SMS message.

6.3.8.2 Data connectivity

There is required to be a data connection for the HTTPS method to be used, which can be provided by either an authorized connection to the 3GPP network or to a Wi-Fi access point. For the 3GPP connection the user may also need to have credit to support a chargeable transaction, as it is not thought to be readily possible to ensure zero rating for the HTTPS message.

6.4 SIP (network, terminal and PSAP support)

Some terminals (such as some smartphones) used for emergency calling are already able to support SIP calling and conveyance of location using SIP messages, however it is likely to be some years before all terminals are able to do so. Also Communication Provider networks and PSAPs are all likely to move to SIP at different times over several years.

ETSI ES 203 283 [2] expects IETF RFC 6442 [3] to be used to convey location. Although this contains provision for network provided and handset/user provided location as an actual location within the MIME body of a SIP INVITE message, or as a reference to a Location Server (LS):

a) the form of location carried in the SIP body in IETF RFC 6442 [3] (or as extended by IETF RFC 5491 [4]) is less comprehensive in value than required for AML location data;

b) the PSAP may have difficulty to distinguish between more than one location (if network adds a location to a handset/user provided location); and

c) the time delay required to gather location information by the handset would require the best location information (e.g. using GNSS) to be sent after call set-up (i.e. after SIP INVITE), complicating PSAP processes.

In view of a) - c) an external Location Reference would be the simplest way to convey a handset location used in association with a Location Server - see clause 6.5.

Handsets shall continue to support the existing SMS and/or HTTPS methods agreed with PSAPs as described in clauses 6.2 and 6.3 and should also implement the SIP method as described above to allow a gradual evolution of PSAP technology.

6.5 Next Generation 112

If AML is enabled in the access network, a Location Server (LS) that forms part of NG 112 architecture described in ETSI TS 103 479 [5] in any given country may implement the capability to act as an AML end-point, receiving locations from handsets using SMS, "Data SMS" and HTTPS push mechanisms as defined in the present document.

The LS should then be the entity that the reference conveyed by IETF RFC 6442 [3] in ETSI ES 203 283 [2] points towards for the PSAP to extract a location value generated by the handset.

7 Mobile Network capabilities

7.1 Simultaneous SMS/HTTPS and emergency voice

As an important development consideration, AML functionality shall not interfere with the voice emergency call.

The mobile network shall be able to simultaneously support a standard 3GPP emergency voice call, establishment of GNSS/Wi-Fi location and AML transmission to the PSAP by the chosen transport mechanism (at least SMS and HTTPS as described in clauses 6.2 and 6.3).

The mobile network shall fully support all SMS mechanisms following normal SMS standards (ETSI TS 123 040 [1]).

NOTE: End users may not be charged for 112 calls - this regulatory requirement can be met for AML SMSs not incurring a charge when 112 is called, but it is understood that this cannot yet be assured for AML HTTPS messages.

8 Operational Guidance

8.1 PSAP reception of location (location endpoint)

Emergency services are organized differently in each country. In some countries there is only one centralized PSAP receiving all 112 calls from all areas of the country, but in others, there is one PSAP for each region or for each province.

The AML information is sent to a single AML end-point for each country which is very straightforward in the case of having a centralized PSAP. In other cases, other methods may be needed to allow the SMS or HTTPS post (data connection) to be accessed by the same PSAP as where the voice has been received. Methods to be considered are as follows:

- A centralized server (AML end-point) decodes the AML message, reads the location and compares this location with the routing tables for 112 calls. This server takes the decision where to send the AML data and forwards/pushes the data to the appropriate PSAP for the location involved.
- AML messages are received by a centralized server that is accessible by regional PSAPs. For each call it receives, a regional PSAP queries the centralized server to query if an AML location is available for a particular call.

PSAPs providing the AML end-point server(s) for a country shall contact Handset OS providers to indicate when they are ready to receive AML information, to provide emergency numbers for which AML information shall be sent and to confirm which transport method and AML format(s) they can handle - see clauses 6.2 and 6.3.

To assist with compatibility, the PSAP end-point servers shall be able to process the attributes in any order in which they are received. Servers shall also be able to ignore any attributes that are not recognized while still processing the other attributes.

NOTE: Some SMS aggregators - see figure 1 - may not automatically be able to decode the "Data SMS" as they may assume normal encoding, so that if such a provider is used, it may be necessary to draw attention to the use of the specific form of encoding as detailed in clause 6.2.1.

Annex A (normative): SMS Format

Unless explicitly stated in the description data, values should not include white space or zero padded values. Data should be passed using the GSM 7-bit character set as described in clause 6.2.2.

Table A.1

Attribute	Attribute Name	Attribute Size (chars)			Attribute Description
		Name	Value (Max)	Total incl '='	
Header	A"ML	4	3	8	The header shall appear at the beginning of the SMS message as it is used to differentiate AML messages from other emergency SMS messages The header shall be in upper case and have a double quotes character (") in the character 2 position. The attribute value will indicate the interface version number. This is version 1 of the interface. No left padding with zeros is required. The value field is a maximum of three characters allowing iterations of the interface if required. An example of the Header would be **A"ML=1;**lt=…

Table A.2

Attribute	Attribute Name	Attribute Size (chars)			Attribute Description
		Name	Value (Max)	Total incl '='	
Latitude	lt	2	9	12	The WGS84 latitude and longitude of the centre of the location area given in decimal degrees using 5 decimal places giving resolution to 1.1 metres. The format of the attribute value will be <sign><decimal degrees>where: **<sign>** This can either be a + or -. **<degrees>** This is a numeric value representing the latitude or longitude in terms of decimal degrees relative to the equator or meridian. This field consists of numeric and a single decimal point character (.) Latitude values fall in the range of ±90 degrees (2 digits before the decimal point) character, whereas Longitudes fall in the range ±180 degrees (3 digits), therefore Latitude is one character less than Longitude. Examples of the latitude and longitude are given below. Please note that a "." is used for the decimal marker separating the integer part from the fractional part. AML=1**;lt=+55.74317;lg=-4.26881;**rd=… If it is not possible to determine a location the SMS should still be sent with latitude and longitude set to +00.00000(lat), +000.00000 (long) and positioning method set to N.
Longitude	lg	2	10	13	

Table A.3

Attribute	Attribute Name	Attribute Size (chars)			Attribute Description
		Name	Value (Max)	Total incl '='	
Radius	rd	2	5	8	The radius of the location area in metres. This field is all numeric. An example of a radius attribute is given below …576**;rd=50;**top=… If it is not possible to determine a location the SMS should still be sent with a radius set to 'N' and a positioning method set to 'N'.
Time of Positioning (TOP)	top	3	14	18	The date and time that the handset **determined the location area** specified in UTC (Greenwich). This shall be the time that location was determined and no other time. The field format is YYYYMMDDhhmmss Where: **YYYY** is the year. **MM** is the month in the range 01 to 12. **DD** is the day in the range 01 to 31 **hh** is the hour in the range 00 to 23 **mm** is the minute in the range 00 to 59 **ss** is the second in the range 00 to 59. An example of a Time of Position attribute is shown below: ……**;top=20130717175329;**…… When the handset is unable to determine its location the TOP should be the date and time that the location process was deemed to have failed.

Table A.4

Attribute	Attribute Name	Attribute Size (chars)			Attribute Description
		Name	Value (Max)	Total incl '='	
Level of Confidence (LOC)	lc	2	2	5	It is recognized that methods for determining mobile handset location are not infallible. Terrain and weather conditions introduce a margin of error into location calculations. Different methods will have different error factors that need to be communicated to the Emergency Services. The Level of Confidence is a percentage probability that the mobile handset is within the area being communicated, for example a 95 % value tells the Emergency Services that there is a 5 % probability that the caller is not within the location area specified by the lat, long and radius values. It is assumed that it is not possible to achieve 100 % certainty hence the two character field. An example of a Level of Confidence (LOC) message is shown below: ….=50**;lc=95;**pm=…. If it is not possible to determine the location the SMS should still be sent with a level of confidence set to 0 (zero).
Positioning Method	pm	2	1	4	The method used to determine the location area. A single upper case character that can be one of: **G** - GNSS or AGNSS. **W** - Wi-Fi signals **C** - Cell **N** - It has not been possible to determine the location. An example of a Positioning Method attribute is shown below: ….lc=95**;pm=G;**si=…..

Table A.5

Attribute	Attribute Name	Attribute Size (chars)			Attribute Description
		Name	Value (Max)	Total incl '='	
International Mobile Subscriber Identity (IMSI)	si	2	15	18	The SIM card identifier of the handset that has made the emergency call. ….=G**;si=234302543446355;**ei=….
International Mobile Equipment Identity (IMEI)	ei	2	16	19	The identifier of the handset that made the emergency call. …55**;ei=356708041746734;**ml…
MCC	mcc	3	3	7	Mobile Country Code, used to determine the network country that the emergency call was made on. …..34**;mcc=234;**mnc…..
MNC	mnc	3	3	7	Mobile Network Code, used to determine the mobile network used to make the emergency call. In most cases this will be the home network MNC but in some cases will be another network code. **It is important that this field is filled in correctly as it will be used to identify data relating to national roaming calls.** ...234**;mnc=30;**ml=…..
Message Length	ml	2	3	6	The length of the entire SMS message including the header and the length attribute. The message length name shall be in lower case and the value shall be all numeric. An example of the message length message would be ……**;ml=124**

Annex B (normative): HTTPS message format

B.1 HTTPS fields

With the exception of fields for the normative attributes described in clause 6.1.1, every other field should be considered optional and should be omitted if no value is available. The additional space for attributes using HTTPS compared to SMS allows the attributes to be described without abbreviations.

Table B.1

Key	Attribute (Value)	Units	Example(s)
v	Header (Version)	-	2
emergency_number	Emergency number dialled	-	112
source	Source of activation (CALL, SMS)	-	CALL
Handset OS_version	Version number for OS module supporting AML	-	2 800
time	Timestamp of beginning of call (ms since 1 Jan 1970)	ms (unix time)	1438101600123
gt_location_latitude	Ground truth latitude (for testing) (WGS 84)	degrees	37.4217829
gt_location_longitude	Ground truth longitude(for testing) (WGS84)	degrees	-122.0884413
location_latitude	Latitude (WGS 84)	degrees	37.4217845
location_longitude	Longitude (WGS 84)	degrees	-122.0847413
location_time	Time of Positioning - Timestamp of location	ms (unix time)	1438102600123
location_altitude	Altitude (above WGS84 reference ellipsoid)	metres	4.0
location_source	Positioning Method- Location Source (gps, Wi-Fi, cell, unknown) "gps" is used to indicate GNSS or AGNSS, and "unknown" if it has not been possible to determine the location	-	gps
location_accuracy	Accuracy (Radius of circle describing location centred on Lat, Long)	metres	20.0
location_vertical_accuracy	Vertical accuracy (Indicates the vertical variance, plus or minus, from given altitude)	metres	2.5
location_confidence	Level of Confidence in location accuracy	Percentage divided by 100 (0-1)	.6827
location_bearing	Bearing (horizontal)	degrees	156.7
location_speed	Speed (horizontal)	metres/second	1.2
device_number	Device phone number (MSISDN as reported by handset)	-	+1438101600
device_model	Device model	-	device model
device_imsi	IMSI	-	310260579377451
device_imei	IMEI	-	355458061005220
device_iccid	ICCID	-	89148000001466 362977
cell_home_mcc	Home MCC (from the device's IMSI)	-	310
cell_home_mnc	Home MNC (from the device's IMSI)	-	260

Key	Attribute (Value)	Units	Example(s)
cell_network_mcc	Network MCC	-	310
cell_network_mnc	Network MNC	-	260
NOTE: A "." is used for the decimal marker separating the integer part from the fractional part.			

Annex C (informative): Management of location best practice by PSAPs

Handset locations obtained through the AML functionality should be displayed on call-taker positions as location circles of specific radius and with a level of confidence that a caller is within the circle provided.

If possible locations displayed should also identify if AML message was the source and whether the location is based mainly on GNSS, on WiFi or on mobile network cell information.

PSAPs should ensure the call takers/call handlers understand that the handset locations are the same as they see on their own smartphones when using mapping applications.

PSAPs should train the call takers/handlers how to most effectively use the handset location - still using verbal confirmation with the caller wherever possible, and taking into account the location provided by mobile networks (often simply using basic cell coverage information). This comparison between handset and network location may be done visually - so PSAP call takers see both location circles - which provides additional validation of any handset location information provided (as it will normally be consistent with the network location).

Rules for how to resolve conflict, e.g. if handset and network circles are completely separate, will need to be provided, as neither is guaranteed to be 100 % accurate and will depend, for example, on quality of information provided by networks or on whether AML location is mainly derived from GNSS information. Typically GNSS location estimates obtained by handsets in open-sky environments are expected to be more precise, accurate and reliable than other technologies. However, in some situations, such as dense urban or indoor scenarios, this may not always be the case and handset location providers indicate this by using a larger radius (with their normal levels of confidence - see note).

So PSAP call takers should particularly note both the radius of location circles and the level of confidence that a caller is within that circle, as well as (if provided to call takers) whether the location circle is predominantly based on GNSS, WiFi or Cell information.

PSAPs should ensure that call handling systems allow call takers to match the coordinates provided as part of the handset locations:

a) directly to nearby civic locations used within PSAP databases; or

b) with a free text description added if more appropriate, e.g. '100 metres west of {Nearest Property, or Road Junction, as matched by local address database}.

This assists if locations need to be relayed verbally to responding resources.

NOTE: Handset/OS providers should use a high-enough level of confidence so as to meaningfully focus the location circle estimated to contain the caller, while reducing the chances of a PSAP call taker mis-estimating the user's true location, which may be outside the circle (even if just outside).

History

Document history		
V1.1.1	December 2019	Publication