European Commission

Pilot project on the design, implementation and execution of the transfer of GNSS data during an E112 call to the PSAP

Contract No 440/PP/GRO/PPA/15/8308

Deliverable D3.4

-

Analysis of the gaps with existing standards

Ismail Embaby

July – 2017

Contract No 440/PP/GRO/PPA/15/8308

Deliverable D3.4
Analysis of the gaps with existing standards

Pilot project on the design, implementation and execution of the transfer of GNSS data during an E112 call to the PSAP

	Responsibility-Office-Company	Date	Signature
Prepared by			
Ismail Embaby	Project Manager – Creativity Software	01/02/2017	
Verified by			
Approved by			

ENREGISTREMENT DES EVOLUTIONS / *CHANGE RECORDS*

ISSUE	DATE	§ : DESCRIPTION DES EVOLUTIONS § : CHANGE RECORD	REDACTEUR AUTHOR
1.0	05/02/2016	Deliverable outline as discussed during the KOM	I.Embaby
1.1	05/12/2016	First Draft	I.Embaby N.Stamps
1.2	07/12/2016	Comments and change suggestions Change suggestion Implement the change suggestions and add content.	L.Bellon J.Medland I.Embaby
1.3	02/01/2017	Add to all the standards used in the architecture (3GPP, OMA,…) and to links to their descriptions, in addition to the Android versions where AEL is already enabled.	I.Embaby
1.4	11/01/2017	Respond to the queries and requests made by both DG GROW and GSA	I.Embaby
1.5	01/02/2017	Respond to additional queries and requests made by both DG GROW and GSA	I.Embaby

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

3GPP - 3rd Generation Partnership Project

A-GNSS - Assisted Global Navigation Satellite System

A2C - Authorities to Citizens communication

ACE - Accredited Center of Excellence

AEL - Android Emergency Location

AML - Advanced Mobile Location

API - Application Program Interface

BSC - Base Station Controller (2G)

BSSAP-LE - LCS Extension for Lb, Lp and Ls interfaces

BSSMAP-LE - BSSMAP LCS Extension

BSSLAP - BSS LCS Assistance Protocol

C&C - Command & Control

C2A - Citizens to Authorities communication

CAD - Computer-aided dispatch

CAPEX - Capital expenditures

CEN - European Committee for Standardisation

CERN - European Organisation for Nuclear Research

CNES - French Space Agency

CS - Creativity Software

EC - European Commission

E-CID – Enhanced Cell ID

ECAS - Emergency Call Answering Service

ECC - Electronic Communications Committee

EE - British mobile phone operator, formerly Everything Everywhere

EGNOS - European Geostationary Navigation Overlay Service

E-GNSS – European Global Navigation System

EISEC - Enhanced Information System for Emergency Calls

ESA - European Space Agency

ESSN - Emergency Services Staff Network

ETC - Electronic Toll Collection

ETSI - European Telecommunications Standards Institute

EU - European Union

FP7 - Framework Programme 7

GIS - Geographical Information System

GMLC - Gateway Mobile Location Center

GNSS - Global Navigation Satellite System

GPS - Global Positioning System

GSM - Global System for Mobile Communications

HSS - Home Subscriber Server

HTTPS - Hypertext Transfer Protocol Secure

ICE - In Case of Emergency

IETF - Internet Engineering Task Force

IP - Internet Protocol

IPR - Intellectual Property Right

IRSN - French Nuclear Safety Institute

Iupc - Interface between RNC and SAS (RNC interface)

IVE - in-vehicle equipment

IVS - in-vehicle systems

KPI - Key Performance Indicator

LAC - Location Area Code

LBS - Location based Services

LCS - LoCation Services

LCS-AP - LCS Application Protocol

LPP - LTE Positioning Protocol

LTE - Long-Term Evolution

LPP - LTE Positioning Protocol

MAC - Media Access Control

MEP - Member of the European Parliament

MLC - Mobile Location Centre

MME - Mobility Management Entity (4G)

MNO - Mobile Network Operator

MSD - Minimum Set of Data

MSG - Mobile Standard Group

MT-LR - Mobile Terminating Location Request

NG - Next Generation

NG112 - Next Generation 112

OMA – Open Mobile Alliance

OMA MLP – Open Mobile Alliance Mobile Location Protocol

OPEX - Operating Expenditures

OS – Operating System

OTDOA - Observed Time Difference Of Arrival

PCAP - Positioning Calculation Application Part

PCO - Project Control Office

PEMEA - Pan-European Mobile Emergency Application

PSAP - Public Service Answering Point

R&D - Research & Development

RMR – Radio Measurement Report

RNC - Radio Network Controller (3G)

Rx - Received Signal level

RRLP - Radio Resource Location services Protocol

RTT – Round Trip Time

SAS - Standalone SMLC

SET - SUPL enabled terminal

SIM - Subscriber Identity Module

SIP - Session Initiation Protocol

SL - SUPL Location

SLA - Service Level Agreement

SLC - SUPL Location Center

SLP - SUPL location platform

SMLC - Serving Mobile Location Center

SMS - Short Message Service

SMSC – Short Message Service Center

SMPP – Short Message Peer to Peer

SSID - Service Set IDentifier

SUPL - Secure User Plane

TDOA - Time Difference of Arrival

TA - Timing Advance (between an MS and its serving BTS)

TL - Task Leaders

TLRR - Trigger Location Reporting Request

TM - Technical Manager

TOA - Time of Arrival

TPZF - Telespazio France

TTFT - Time To First Fix

WP - Work Package

WPL - Work Package Leader

UE - User Equipment (mobile)

UMTS - Universal Mobile Telecommunication System

URI - Uniform Resource Identifier

URN – Uniform Resource Name

WGS84 - World Geodetic System Datum 84

VoLTE - Voice over LTE

1. INTRODUCTION

1.1 PLACE OF THIS DOCUMENT AND OBJECTIVES

This document is the "Analysis of the gaps with existing standards (eCall)", identified as D3.4 in the list of project deliverables. It is generated as part of the contract 440/PP/GRO/PPA/15/8308.

The objectives of the document are to:

- Analyse the interfaces for each sub-system in the chosen solution;
- Identify the differences and similarities with the eCall implementation. Especially in the way of transmitting data to PSAPs with the inband modem technology;
- Determine the key interfaces that need to be standardised;
- Identify potential changes to be made to existing standards (3 Gpp, eCall, ECC report 225).

1.2 FOREWORD

Emergency caller location is the most important piece of information for both PSAPs and first responders. Ensuring that it is accurate, reliable and timely will save lives and significant emergency services resources. Not having it will mean negative outcomes for our citizens.

In the absence of a detailed and prescriptive regulatory framework, emergency mobile caller location information in Europe has typically relied on Cell-ID. Often, Cell-ID is inadequate because the cell radius is too large, notably in rural areas.

Developments in location technologies and the proliferation of GNSS enabled smartphones are leading to improved location information being available in the handset. Making such handset derived positioning information available to PSAPs during emergency communications, in a secure and reliable manner, is highly desirable.

This consortium, known as the HELP112 consortium, is tasked to demonstrate that accurate and reliable caller location information is highly effective and highly efficient. The consortium will also demonstrate that this service can be made available across Europe in a cost-effective manner, securing better outcomes for our citizens; while simultaneously ensuring that no additional burden is placed on the emergency services, mobile network providers or public authorities.

1.3 APPLICABLE DOCUMENTS

AD	Title of the document & reference
AD 1	Contract 440/PP/GRO/PPA/15/8308
AD2	Help112 Consortium Agreement

Table 1 – Applicable documents

1.4 REFERENCE DOCUMENTS

RD	Title of the document & reference
RD 1	Help112 Technical, Management & Financial Proposal TPZF/SSA-T2015-PP-0451 is1.0 31/07/2015
RD 2	D1.2: State of the Art Analysis document.
RD 3	D3.1: Description of the Scenarios Document
RD 4	D3.3: Recommendation for the Pilot
RD 5	D4.1 – D4.2: Tests technical design and specification

Table 2 – Reference documents

2. CANDIDATE ARCHITECTURE SELECTION

2.1 CANDIDATE ARCHITECTURE – PROPOSALS

During the Help112 project, the consortium identified several candidate architectures for the new E112 architecture. A total of six candidate architectures were identified in D3.2 (section 6) as follows:

- **Architecture 1:** Handset hybrid positioning method + E-GNSS SUPL server and client + SMS transmission.
- **Architecture 2:** Handset hybrid positioning method + SMS transmission with international roaming enabled.
- **Architecture 3:** Handset hybrid positioning method + SMS transmission + Network Based Location (NBL) Location Calculator based on Radio Measurement Report (RMR).
- **Architecture 4:** Handset hybrid positioning method + Data channel transmission.
- **Architecture 5:** Handset hybrid positioning method + IMS SIP transmission.
- **Architecture 6:** Handset hybrid positioning method + In-band modem transmission (Personal eCall).

It is important to highlight that the **core component** of the first four candidate architectures is the **Advanced Mobile Location (AML) solution**, operational by BT in the UK since July 2014. For more on the AML deployment in the UK, please refer to Appendix 9.1.

2.2 CANDIDATE ARCHITECTURE - SELECTION PROCESS

Referring to Deliverable D3.3, further analyses were made on each of the candidate architectures to check their respective compliance with the following three main criteria:

- The first criteria which was considered was the compliance with **user requirements** (Requirements that apply to all HELP112 stakeholders: Caller, MNOs, PSAP, OS provider, Handset manufacturers …) defined in HELP112 deliverables D1.1 and D3.1.
- The second criteria was the output of the **costs and benefits analysis** (Work Package 2); which aimed at defining the most effective architecture to be deployed in the pilots for the short term, with regards to the associated implementation and maintenance costs for each stakeholder (MNOs, PSAP, Public Authority, OS provider, Handset manufacturers, …) and with regards to the benefits in terms of human lives saved as well as material savings delivered by each architecture.
- The third and final criteria was the **capacity of each pilot to implement** the necessary infrastructure for each candidate architecture in the timeframe of HELP112 project. Based on the feedback from each pilot site as reported in HELP112 deliverable D3.2, each architecture was ranked depending on its implementation roadmap in the pilot sites.

2.3 SELECTED ARCHITECTURE: HANDSET BASED HYBRID POSITIONING METHOD USING SUPL SERVER + AUTOMATED ACTIVATION + SMS TRANSMISSION (ROAMING-ENABLED)

Referring to the conclusion of D3.3 document, the new proposal for the E112 architecture is a **combination of architecture 1 and 2A** as follows:

- **Architecture 1 element**: Cell-Id, E-GNSS (including Galileo) and WiFi. The tests of the potential value added by using E-GNSS in the location estimate process have been conducted by BT in the UK, 112ERC in Lithuania and TPZF in France.
- **Architecture 2 element**: SMS transmission method that handles international roaming, which is an enhancement compared to today's AML deployment in the UK. The test of the SMS transmission method that handles international roaming has been conducted by BT in the UK.

The activation process corresponds to the HELP112 automated activation process and the transmission process corresponds to the HELP112 transmission process by sending the location MSD (Minimum Set of Data) using SMS, as described in HELP112 deliverable D3.1 (Description of the scenarios). These methods of activation and transmission derive from the Advance Mobile Location process standardised by ETSI in *ETSI TR 103 393*[1].

The chart below shows the components involved in **the proposed E112 architecture** as well as the interfaces between them:

1 ETSI TR 103 393, Advanced Mobile Location for emergency calls, latest version

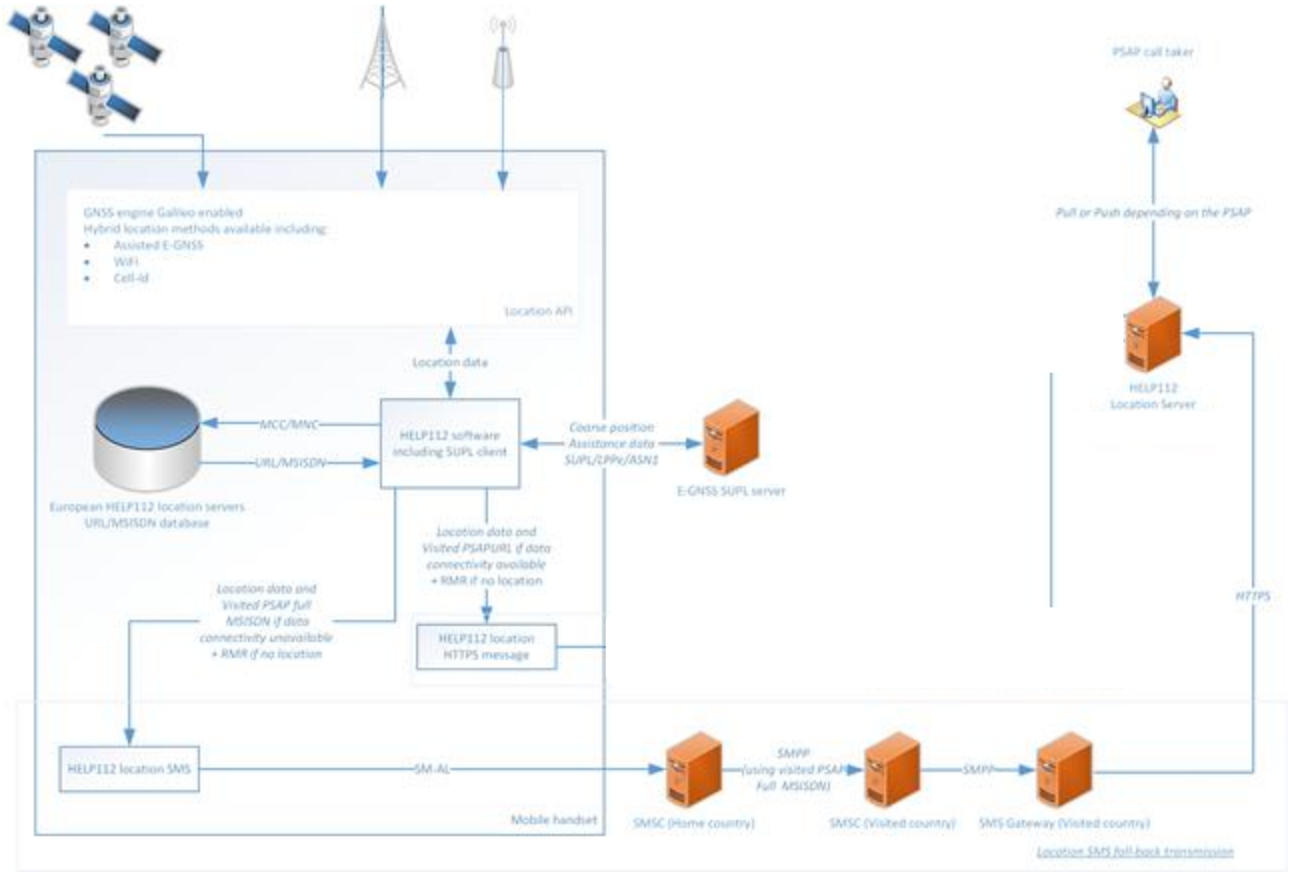

Figure 1 – Selected Architecture: Handset based hybrid positioning method using SUPL server + Automated activation + SMS transmission (Roaming-Enabled)

Please note that the SMS gateway is a logical gateway and could be either:

- Centralized,
- Per MNO,
- Or, incorporated to the Help112 server.

In 2016, Google released its own implementation of AML, Thunderbird, to all Android phones in the world back to Gingerbread (above 90% of Android devices on the market[2]): Google has already built their Android Emergency Location (AEL) Service into the Play Services application which has been downloaded to Android phones during the software update to the latest version after v9 was released. Therefore, the location estimation part in this architecture is available today for up to 90% of all Android mobile phones that have location capabilities. The Roaming-enabled SMS transmission is yet to be implemented in Google AEL. The location methods used will therefore rely on the capabilities of the handset, the user's settings, and the environment of the caller.

It is worth noting that Google is currently providing support for the activation and configuration of Thunderbird at Country/MNO level.

[2]Vision Mobile, Global Trends in Android Use 2015, https://www.visionmobile.com/reports/global-trends-Android, December 2015

In this proposed new E112 architecture, the handset checks a series of locally present rules to get the full MSISDN of the location server in the visited country based on the MCC and MNC. This full MSISDN is used by the home country's SMSC to route the HELP112 location SMS to the appropriate HELP112 location server in the visited country. All mobile networks involved should agree to a zero-rate for such emergency location SMSs for end users.

3. CANDIDATE ARCHITECTURE – INTERFACES ANALYSIS

The following subsections present the interfaces for each sub-system in the selected architecture.

3.1 SUPL INTERFACE

As described in Deliverable D3.2, the interface between the SUPL server and the handset's SUPL client is using SUPL (Secured User Plane Protocol) with LPP (LTE Positioning Protocol) data format. SUPL and LPP are standards for location services defined by the Open Mobile Alliance (OMA), and 3GPP. For more details, please refer to http://www.openmobilealliance.org/release/SUPL/V2_0_3-20160524-A/

It is worth mentioning that the assistance data received by the client is LPP ASN1 encoded. ASN1 (Abstract Syntax Notation One) is a joint standard of the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and International Telecommunication Union Telecommunication Standardization Sector ITU-T, that describes rules and structures for representing, encoding, transmitting, and decoding data in telecommunications and computer networking.

The SUPL client requests for assistance data to the SUPL server, in order to compute a more accurate location and speed up the TTFF. The assistance data is of several types as described in Deliverable D3.1 section 4.2.3 including Real Time assistance data (the data downlinked at that time by the satellites from the different GNSS constellations) and long duration assistance data (the Extended Ephemeris, also called the seeds. One seed contains, for each satellite of a GNSS constellation, the compacted information on the precise satellite trajectory over 14 days. This information is transported as such, compacted, to the GNSS chipset in the user terminal where it will be decompacted and process.)

Requests to the SUPL server are possible on any network (2G, 3G, 4G) as long as the data connectivity is available on the handset.

For more details, please refer to section 4.2.3 in Deliverable D3.1

3.2 SMPP INTERFACE

It is the interface between:

- The SMSC and SMS Gateway
- The Visiting SMSC and Home SMSC, in the case of roaming

This interface requires no modification as it supports all current and future SMS requirements. In this solution, SMPP3.4 is proposed. For more details, please refer to
http://www.3gpp.org/ftp/tsg_t/tsg_t/tsgt_04/docs/pdfs/TP-99128.pdf

In the UK, the SMS gateway is provided by an SMS aggregator which takes SMPP (Short Message Peer to Peer) output from the SMSCs of all mobile networks and sends an HTTPS message containing the SMS content to the HELP112 location server.

Each country will provide a server to receive the HELP112 location SMS message from SMSCs or make use of any potentially existing server for emergency SMS service for deaf/hard of hearing users.

Please refer to the Deliverables D4.3, D4.4, D4.5 and D4.6 pilots reports for the detailed customized deployment on each pilot site.

3.3 HTTPS INTERFACE

This is the interface between the SMS Gateway and the Help112 Server; and is a new interface.

Below are a few recommendations:

- This interface should be adopted as the de facto standard for Help112 services to ensure a harmonized architecture throughout EU and smoother interoperability and communication between the diferent entities.
- Serving Cell-Id and LAC (Location Area Code) could be supplied to allow routing to regional/distributed Help112 servers.

Please note that a Help112 Location server with an integrated SMS Gateway does not need to implement this interface.

3.4 OMA MLP INTERFACE

This is the interface between the Help112 Location server and the PSAP (MLP emergency interfaces). No extensions to these interfaces are necessary.

In this solution, OMA MLP 3.2 or above (the Emergency Interface) is proposed. For more details, please refer to http://www.openmobilealliance.org/release/MLP/OMA-LIF-MLP-V3_1-20040316-C.pdf

ELIS (Emergency Immediate Service)

- This service is used for querying the location of a mobile subscriber that has made an emergency call to an emergency call centre or similar and the centre requests the mobile location. The response to this service is required immediately (within a set time - default 10 seconds).
- Where ELIR stands for Emergency Location Immediate Request and ELIA stands for Emergency Location Immediate Answer.
- It does support both Pull and Push.

3.5 SUMMARY

The table here below summarizes the different interfaces included in the new E112 architecture and whether any changes or extensions are needed.

Interface name	Description	Comments
SUPL	The interface between the SUPL server and the handset's SUPL client	No need to extend it.
SMPP	It is the interface between: • The SMSC and SMS Gateway • The Visiting SMSC and Home SMSC, in the case of roaming	No need to extend it.
OMA MLP	This is the interface between the Help112 Location server and the PSAP (MLP emergency interfaces).	No need to extend it.
HTTPS	This is the interface between the SMS Gateway and the Help112 Server	Please note that a Help112 Location server with an integrated SMS Gateway does not need to implement this interface. Please refer to both sections 3.3 and 7.2

Table 3 – Summary of required interfaces for new E112 architecture

4. EXISTING SOLUTION - ECALL

eCall[3] aims to bring rapid assistance to motorists involved in a collision anywhere in the European Union. A vehicle equipped with eCall will establish a 112 voice call to the nearest PSAP in case of a traffic incident. eCall can be triggered manually by vehicle passengers or automatically via activation of in-vehicle sensors when a serious road accident occurs. The manual activation of eCall is useful to alert emergency services about traffic incidents that do not meet the threshold of the automated notification, or about a vehicle occupant with a medical emergency.

A voice channel is established during the call between the vehicle passengers and the emergency service receiving the eCall. Even if no passenger is able to speak, a 'Minimum Set of Data' (MSD) is sent to the PSAP, including the location information and other related data such as the triggering mode (automatic or manual), the vehicle identification number, a timestamp, as well as current and previous positions[4].

4.1 POSITIONING METHOD

eCall uses non-assisted and non-augmented GNSS as a positioning method in the in-vehicle equipment (IVE). The current implementation of eCall calculates the position estimate by GPS. Future eCall implementations, equipped with the appropriate chips, will also use GLONASS, Galileo and EGNOS.

4.2 TRANSMISSION METHOD

eCall uses a data and voice link over the same channel to send data and to establish the voice call between the passengers of the vehicle and emergency services. The data link is realised by an in-band modem, which has been specifically designed and standardised for eCall. This approach guarantees an EU-wide availability of free eCall data transmission through established 112 voice call mechanisms. In the case where the data is not sent or received for any reason, the eCall continues as a normal 112 emergency call. The priority given to normal 112 calls in the mobile network also applies to the eCall data transmission. This maximises the coverage and availability of the eCall service.

A Minimum Set of Data (MSD) has been defined and it is standardised by the European Committee for Standardisation (CEN), document number EN 15722[5].

The EENA operations document[6] on eCall states that the MSD includes the parameters listed in the table overleaf:

3 EENA Operations Document, "eCall", 13 August 2014

4 EENA, "eCall Fact Sheet: Everything that you wanted to ask, but did not know how", 2015

5 CEN, EN 15722, "Intelligent transport systems - eSafety - eCall Minimum set of data", 1 April 2015

6 EENA Operations Document, "eCall", 13 August 2014, section 6, p. 9

Field	Description
Message identifier	MSD format version (later versions to be backwards compatible with existing versions)
Activation	whether the eCall has been manually or automatically generated
Call type	whether the eCall is real emergency or test call
Vehicle type	passenger Vehicle, buses and coaches, light commercial vehicles, heavy duty vehicles, motorcycles
Vehicle identification number	Vehicle identification number (VIN)
Vehicle propulsion storage type	This is important particularly relating to fire risk and electrical power source issues (e.g. Gasoline tank, Diesel tank, Compressed natural gas (CNG), etc.)
Time stamp	Timestamp of incident event
Vehicle location	determined by the on-board system at the time of message generation. It is the last known vehicle's position (latitude and longitude)
Confidence in position	this bit is to be set to "Low confidence in position" if the position is not within the limits of +/-150m with 95% confidence
Direction	helpful to determine the carriageway that vehicle was using at the moment of the incident
Recent vehicle location (Option-	vehicle's position in (n-1) and (n-2)
Number of passengers (Option-	number of fastened seatbelts
Optional additional data (Optional)	in some cases, optional data may be available in the MSD (at the vehicle manufacturer discretion). This data incorporate a tag for the identification in the beginning of the optional data (type and structure identification). This data will be registered and maintained. PSAP will have free access such registry data

Table 4 – eCall MSD structure

4.3 NG eCALL

The PSAP operator may at any time request that a new MSD is sent (e.g. data appears corrupted or inconsistent, or the PSAP operator believes that the data may have changed).

The Next Generation (NG) eCall is already being discussed[7]. NG eCall focuses on the transmission of data and voice to the PSAP, by taking into account the new technical capabilities that are being introduced by the evolution of mobile networks. However, the shift from circuit switched technologies to LTE networks will be evolutionary. Until its full deployment, large parts of the existing network infrastructure will be reused and since eCall is based on a CS emergency call, it will be supported in mobile networks for a quite some time.

4.4 PERSONAL ECALL

Current EU legislation only covers eCall for vehicles. Personal eCall[8] has been discussed in CEN TC 278 and in ETSI TC MSG but no standardisation has yet been done.

Personal eCall is essentially eCall initiated by a user from a mobile phone rather than (e.g. automatically) from a vehicle. It is expected that the newly selected architecture AML-based solution is already superseding the Personal eCall solution.

4.5 WHY ECALL ISN'T SELECTED FOR THE NEW E112 ARCHITECTURE?

Although the main advantage of eCall is its wide deployment currently in the EU member states - due to the support of the legislation, the following identified characteristics have been instrumental in not selecting eCall as the new E112 architecture:

1. Use of the voice channel as a transmission method imposes the major disadvantages of eCall:
   - Takes longer than other methods to transmit the data.
   - The voice call is interrupted to transmit the data.
2. Low position estimation accuracy due to lack of A-GNSS or augmented GNSS.
3. Plenty of filtering of fake calls of false emergency calls (primarily for manual eCalls) would have to be done directly at the PSAP.
4. Based on a technology which is now deemed an old one.

7 This section is based on the following two documents

EENA Operations Document, "eCall", 13 August 2014, section 11, p. 31

EENA Technical Committee Document, "Next Generation eCall", 11 December 2015

8 This section is used from the document:

EENA NG112 Technical Committee Document, "Handset Derived Location for Emergency Calls", 19 November 2014, Annex C.2, p. 12

5. BENCHMARKING BETWEEN ECALL AND SELECTED NEW 112 ARCHITECTURE

The following table was extracted from Deliverable D1.2 then updated here with more details. It does provide an overview of the differences and similarities (if any) between existing eCall and the selected new E112 architecture:

	New E112 Architecture:	eCall
Positioning Method	E-GNSS (A-GNSS including Galileo and EGNOS) enabled, WiFi and Cell-Id	GPS (GLONASS, Galileo, A-GNSS and EGNOS to be supported)
Transmission method	SMS	Voice Channel
Does it require a data connection?	Yes for Assistance data and for Wifi resolution	No
What handsets are supported?	Handset enabled with AML software	Built into the vehicles
Involvement of MNOs	1. Transmit the 112 SMS free of charge and allow it to be transmitted during the 112 voice call 2. Provide the MSISDN to where the 112 SMS is delivered. 3. Sign-up to Google AEL services.	1. Implement the eCall flag 2. Treat eCalls as 112 emergency calls (free of charge, priority, national roaming, etc.) 3. Provide the right routing based on eCall flag following the instructions of the National Authorities 4. Providing SIM cards for the IVE if necessary
Involvement of network vendors	Ensure that the SMS can be sent during the emergency call (a network configuration parameter)	None

	New E112 Architecture:	eCall
Involvement of handset manufacturers / OS Providers	1. Implement the AML functionality 2. AML SMS message should be sent only in AML ready countries based on MCC/MNC to a short or long SMS number determined by MCC. Already done for up to 99% of Android phones by Google.	Not applicable
Involvement of application providers	None	None
Involvement of emergency services	Be able to receive/retrieve the AML location and display it on their CAD systems	1. Infrastructure set-up (e.g. integrate eCall into the PSAP systems) 2. Verify that eCall information is correctly received 3. Staff training 4. Establishment of operational protocols
Advantages	1. Simple to develop – rapid to launch 2. Easy to deploy in countries where there is already a text message service to 112 services 3. Transmission of location is automatically triggered without the need for manual user intervention	1. Supported by legislation and standardisation 2. A pan-European approach and works for roaming users 3. Same prioritisation as a 112 call 4. Minor changes required in the mobile networks (eCall flag and PSAP routing tables)

	New E112 Architecture:	eCall
Disadvantages	1. Android devices are the only ones supported as of today. It means that around 25% of the devices (from other OS providers) in Europe still have to be supported 2. Accurate location requires data connection for assistance data and for WiFi. 3. Roaming users might need data connection to get their location accurately calculated, seeking feed for the AGNSS and/or for the WiFi connection.	1. Takes longer than other methods to transmit the data 2. The voice call is interrupted to transmit the data 3. A lot of fake calls 4. Based on old technology

Table 5 – Benchmarking between existing eCall and selected new E112 architecture

6. ADDITIONAL POTENTIAL METHODS

It is worth noting that additional tests have been made for the following methods:

- **Enhanced NBL User Plane** - Positioning method: As a main component of **Architecture 3**. An offline test of the added value brought about by a Network Based Location method was made by Creativity Software in both UK (EE network, Kingston Upon Thames area) and Lithuania (Tele2 network, Vilnius area). Please refer to the deliverables of Work Package 4 for more details about the tests and the reported results.

  To benefit from the advantages and capabilities of the Network-Based Location solution (please refer to Deliverable D1.2) and overcome the lack of GNSS or WiFi based location which reported up to 20% to 25% of AML messages as per the figures shared by the AML deployment at BT in UK and the Help112 pilots sites, an architecture that uses the NBL as User Plane solution could be considered in the future by integrating a Location Calculator to the PSAP architecture while introducing required modifications to the handset OS.

- **HTTPS** - Transmission method: Since European PSAPs are moving toward IP transmission and since HTTPS transmission (data channel) can carry additional information (medical information about the caller, exact civic address...etc.), when data connectivity is available; testing of **Architecture 4,** which uses the data channel to transmit the location information, has been conducted by BT in the UK, 144 Notruf in Austria and AREU in Italy.

  The primary results from the testing in the pilot sites revealed that the phone number wasn't always reported as a part of the HTTPS message. Phone number reporting is requested in order to correlate the location data message with the ongoing E112 voice call. With some further investigation we found that some SIMs store the telephone number, while others do not and the number is only known by the home network.

  As proposed by BT, PSAPs could continue to use the SMS for its robustness and wider geographic availability for the foreseeable future, but HTTPS could be useful as follows:

  - Supplementary information.
  - Non-GSM devices – emergency calls can be made from other devices that don't use the mobile networks, and hence cannot send SMS messages. For instance, a voice-over-IP (VOIP) device.
  - Other PSAPs – this interface could also be used to send messages between PSAPs, for instance where two countries border each other and a caller in country A roams to a mobile network in the neighbouring country B, the voice call could be passed on by PSAP B to the correct country A and the location could also be passed on using the HTTPS interface.

  More details about the above two additional potential methods are listed in following subsections:

6.1 Positioning Method – User Plane Network Based Location (NBL)

As explained in D3.1, Architecture 3 refers to a Handset-based hybrid location method + SMS transmission method + NBL Location Calculator (acting as a Safety Net) which is based on Radio Measurement Report (RMR).

The handset's HELP112 software is automatically triggered by a 112 call to determine the location of the caller which is transmitted to the PSAP using an SMS. After the HELP112 configured timeout, it might be possible that no location has been calculated and the HELP112 location SMS is then sent with a "No location" message.

In this case, when a HELP112 location SMS is received at the HELP112 location server with no location in it, it should be possible to provide another location estimate based on the Network capabilities as accurately as possible.

The Network Based Location solution (Deliverable D3.1) is a good candidate to fill this gap, acting as a **Safety Net**. It can be implemented at the HELP112 location server level in such a way that there will be no involvement from either mobile operators or network vendors, by adding the measurement report information to the location data within the HELP112 location SMS that is sent to the HELP112 location server.

Note that this measurement report is already sent automatically by the handset to the network in dedicated mode (when a voice call is ongoing) every 480ms for the purposes of managing the allocated radio resources by the network. This measurement Report contains the Timing Advance value from the Serving Cell (2G and LTE networks) in addition to the Received Signal Strengths from both the Serving Cell and up to six best neighbouring cells for a 2G network (details vary on 3G and LTE).

Follow-up activities are recommended after the closure of Help112 project in January 2017: work with Help112 partners and Google should be undertaken to find a way to add the network measurement report to the location SMS (data SMS) information.

The location methods that the Location Calculator software will be able to perform will depend on the content of the measurement report, and the type of network used by the caller (2G, 3G, and 4G). These types of locations methods are described in more details in section 10.

To compute the location based on the network Radio Measurement Report, the Location Calculator software needs to access a database containing the mapping of the cell sites of the mobile network. This is the only point in this solution that involves MNOs, who would need to provide periodic updates to this database, each related to their own network. Please refer to section 7.1.3 for more details on required info. The provision of this info from the MNOs is essential for the (User Plane) NBL solution to be used. Without this info provide, NBL solutions can't calculate the location of the mobile handset as the exact location of surrounding cell sites are used as reference points in the calculation process.

The chart below shows Architecture 3:

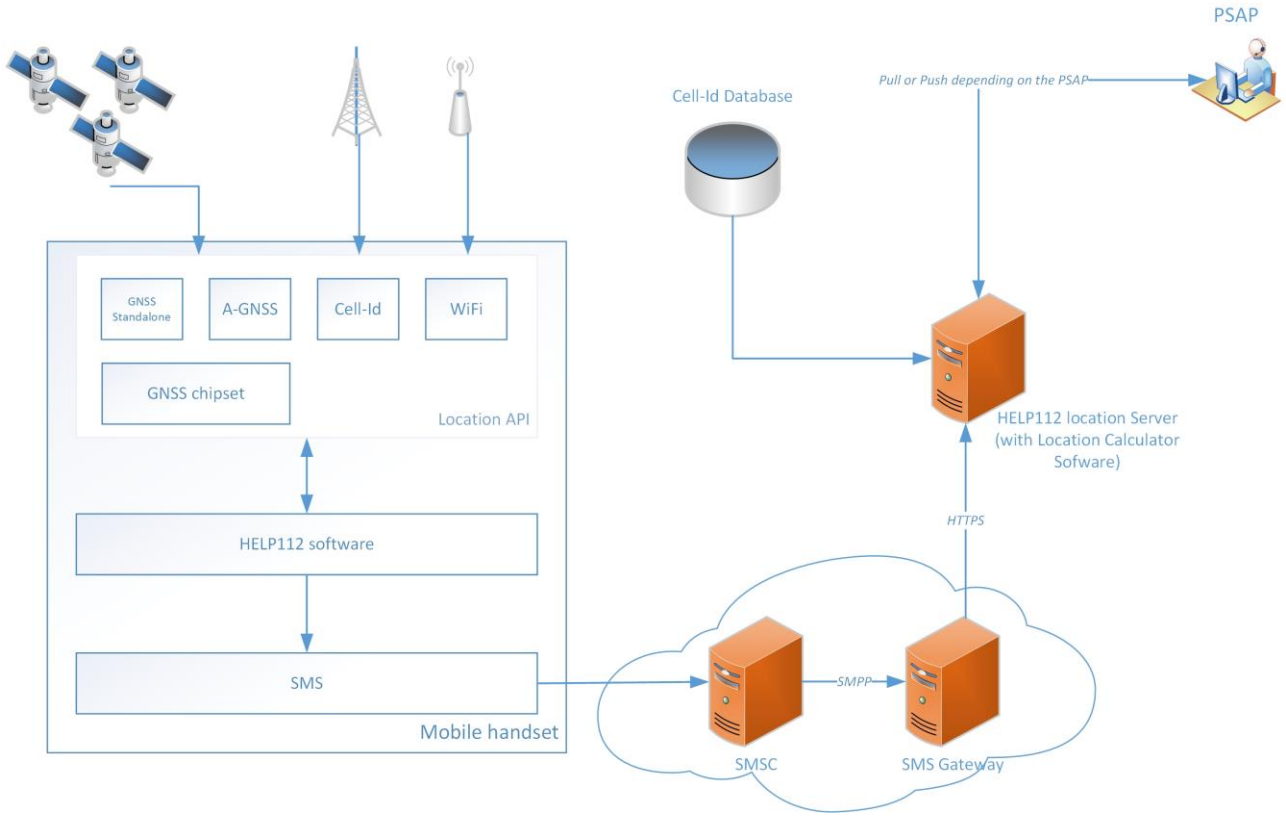

Figure 2 - Architecture 3: Handset based hybrid positioning method + Automated activation + SMS transmission + Location Calculator as safety net

In Architecture 3, the HELP112 location MSD (Minimum Set of Data) is formatted with additional data containing the network Radio Measurement Report. This report would be added as part of the HELP112 software into the handset should either the handset manufactures or OS developers agree to implement this change.

The **interfaces** up to the HELP112 location server are the same as in a classic SMS transmission solution:

- SMPP between the SMSC and the SMS Gateway – please refer to section 3.3
- HTTPS between the SMS Gateway and the HELP112 Location server – please refer to section 3.2

Each country will anyhow provide a server to receive the HELP112 location SMS message from SMSCs or make use of an existing server for emergency SMS services for deaf/hard of hearing users.

In this architecture, the required data parameters (Radio Measurement Report) would be included in the existing HELP112 location SMS process if no location was made available. The HELP112 software would extract the network Radio Measurement Report as an input for the Location Calculator solution.

7.1.1 Radio Resource Measurement Report - RMR

This subsection presents the structure and content of the RMR, which would be directly sent from mobile handset to the Help112 server either via Data SMS or via HTTPS message.

7.1.2 AML SMS Interface

It is recommended to:

- Use the AML SMS interface - as defined by the Google AEL documentation (please refer to the annex 10 for more details.
- Introduce an extension of the AML specification to provide network measurements in a location failure scenario.

A single SMS is composed of 153 characters in binary format.

To create a space for network measurements to be sent in a smallest possible size, the following attributes can be considered redundant and not transmitted:

- lat
- lon
- radius
- confidence level

We propose to drop the fields listed above to create space to add the measurement reports which will be sent to the server. This removal will free-up 42 characters. Optionally, the explicit MCC and MNC fields could be also removed as they will be transmitted as part of the measurement report. This will free an additional 13 characters.

The current serving network measurement will be provided first; where additional networks are detected, the measurements from up to three other networks can also be transmitted. This would introduce a maximum of an extra 109 characters including field delimiter and field indicator.

So, for a current message size of 127 characters:

- Remove unnecessary fields = 55 characters' reduction – as explained above
- Include primary network measurements = 181 characters.

This is too large for a single SMS message (153 characters in binary format), however if the number of readings were reduced to the serving cell and the best four neighbour cells, this will fit in a single SMS message and reduce the transmitted information. If concatenation of SMS messages is considered a barrier to the adoption of the fallback (i.e. safety net) solution, a reduced dataset could be considered.

If we wish to have the RMR from more than one mobile network, we can provide the measurements as follows:

- The Serving network and one more network within two concatenated SMS messages by having the best four neighbours only.

- Or, the Serving network plus two others if only the best four neighbours for each network are communicated.

This opens the opportunity for multi network multi-lateration to be used to provide a location.

The table below presents the proposed content of the RMR within the AML SMS for each technology:

Field	Example	Length	Description
Field indicator	mr=	3	Measurement report field indicator
Number of networks	1	1	An indicator of how many networks are provided.
Network type	3	1	2,3 or 4G indicator
Serving Cell Identifier	234300051130005	15	Cell identifer as Cgi (2 and 3G) or eCgi (4G)
Serving cell Power	068	3	Serving cell RX Full level in decibels. No negative symbol is required – it is considered implicit.
Serving cell TA	01	2	Serving cell timing advance band

The adjacent cell information format will vary depending upon the network (2G,3G,4G)

2G Adjacency format

Field	Example	Length	Description
Neighbour 1 bcch	12	2	bcch
Neighbour 1 bsic	23	2	Bsic in bit shifted format as specified by 3GPP. 3 Bits representing Network Colour code and 3 Bits representing Base station Colour Code. 3GPP TS 03.03 Numbering, Addressing and Identification http://www.3gpp.org/ftp/Specs/html-info/03-series.htm
Neighbour 1 rxLevel	110	3	RX Full level in decibels

Pattern is now repeated for neighbour cells 2-6. Where measurements are not available zero

padding will be used.

3G Adjacency format

Field	Example	Length	Description
Neighbour 1 Primary scramble code	511	3	The primary scramble code (PSC)
Neighbour 1 Channel	00000001	8	Channel number (UARFCN)
Neighbour 1 Power level	110	3	Received Signal core power reading in decibels

The pattern is now repeated for Neighbours 2-6. Where measurements are not present zero padding will be used.

4G Adjacency format

Field	Example	Length	Description
Neigbour 1 EARFCN		5	EARFCN
Neighbour 1 PCI		2	
Neighbour 1 Power Level		3	Received power reading in decibels

The pattern is now repeated for Neighbours 2-6. Where measurements are not present zero padding will be used.

Table 6 – Proposed AML SMS RMR's content

7.1.3 Cell Tower Database

It will be required for the MNOs to provide a data file periodically to the Help112 Location Server that contains information on the individual cells in their networks.

This information would include the coordinates and technical details of the antennas such as azimuth, beam angle, height above ground and other technical information that network-based location technologies make use of to calculate a location estimate.

6.2 TRANSMISSION METHOD – HTTPS

As was explained through Architecture 4 in D3.1, in the case where the handset's data connection is available and sufficiently reliable (on a 3G or 4G network or Wifi) to be used at the time of the emergency call, a data push across the data channel could be used to transmit the location data to the PSAP. The location data is pushed to a location server using an HTTPS message, using the same data elements as in the SMS message, probably using XML, JSON, or attribute pairs within the HTTPS message.

Two different approaches to implement the solution were described in D3.1. This document presents the regional/distributed approach due to its closer relevance to the selected new architecture.

In the regional/distributed approach, PSAPs operate at the regional level and the location data should be maintained in the regional jurisdiction. Once the data has been pushed to the national location server, the solution could be to establish a hierarchy of proxy-servers that reside inside each PSAP region, and then the national location server should be able to identify the correct regional proxy server to push the data to. The regional PSAP could then pull the location data from the proxy server, for instance using the caller's handset MSISDN as a key.

The chart below shows the architecture of this solution with a Regional approach:

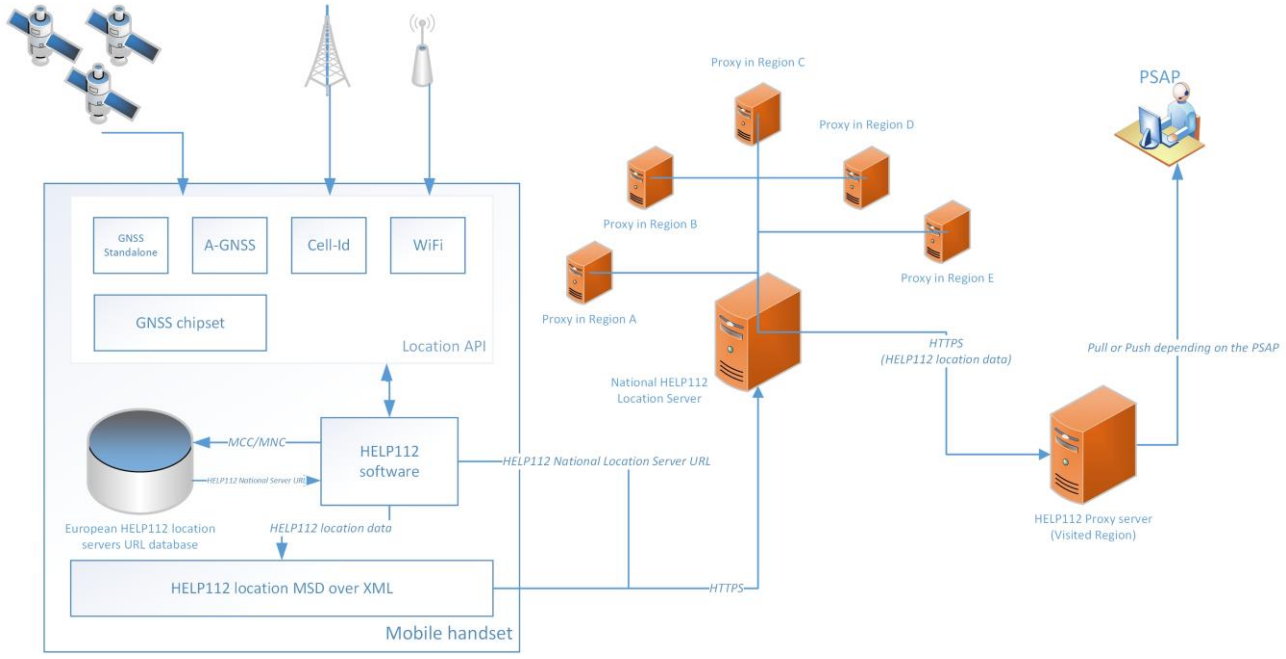

Figure 3 - Architecture 4: Handset based hybrid positioning method + Automated activation + Data channel transmission (Regional approach)

Access to the HELP112 location data from the PSAP depends on how the PSAP obtains location in the concerned country. In a regional/distributed approach, the regional PSAP that has handled the emergency call could make a request to pull location data from the related HELP112 Regional proxy (using the originating device's telephone number/MSISDN as a key).

7.2.1 Format of HTTPS Message

In their Thunderbird Partner Endpoint Overview document, Google describes the fields which will be sent in the HTTP post message. These should come through as normal CGI (Common Gateway Interface) name-value pairs in the HTTP post.

Possible names are:

location_latitude	device_number	cell_carrier	place_name
location_longitude	device_model	cell_home_mcc	place_id
location_time	device_imsi	cell_home_mnc	place_likelihood
location_altitude	device_imei	cell_network_mcc	place_address
location_floor		cell_network_mnc	place_latitude
location_accuracy			place_longitude
location_source			place_number
			place_website

Table 7 – Google description of fields in the HTTP post message

As suggested by BT in their pilot report document (Deliverable D4.3):

- To receive this sort of message, the PSAP would have to implement a web application that will receive the HTTPS messages, reformat them to match the interface for AML SMS messages and then forward them onto the existing AML reception system.
- The diagram in the following page shows the message flow for an SMS AML message, using the phone Home mobile network SMS service to send the message to the SMS Aggregator, which then forwards it to the SMS Gateway. This extracts the message to check if it's an AML message and forwards those to the AML Reception process on the PSAP's external-facing server. This then forwards the message to our AML Server process, which sits in the PSAP's internal network.
- The path for an HTTPS message would be simpler. The phone would connect to the PSAP's external-facing server directly, sending an HTTP POST to the AML HTTP process. This could connect directly to the AML Server, but it is more convenient to make it forward the reformatted message to the AML Reception process first. This provides a single point of contact on an externally facing server that can report on all AML messages of both types.
- The AML HTTP process searches for some of the fields in the POST message and translates them to fields in the output AML message. Some of these fields need to be reformatted and some need to be generated, since they aren't present in the Google HTTPS message.

The figure here below presents the message flow for both the SMS and HTTPS message

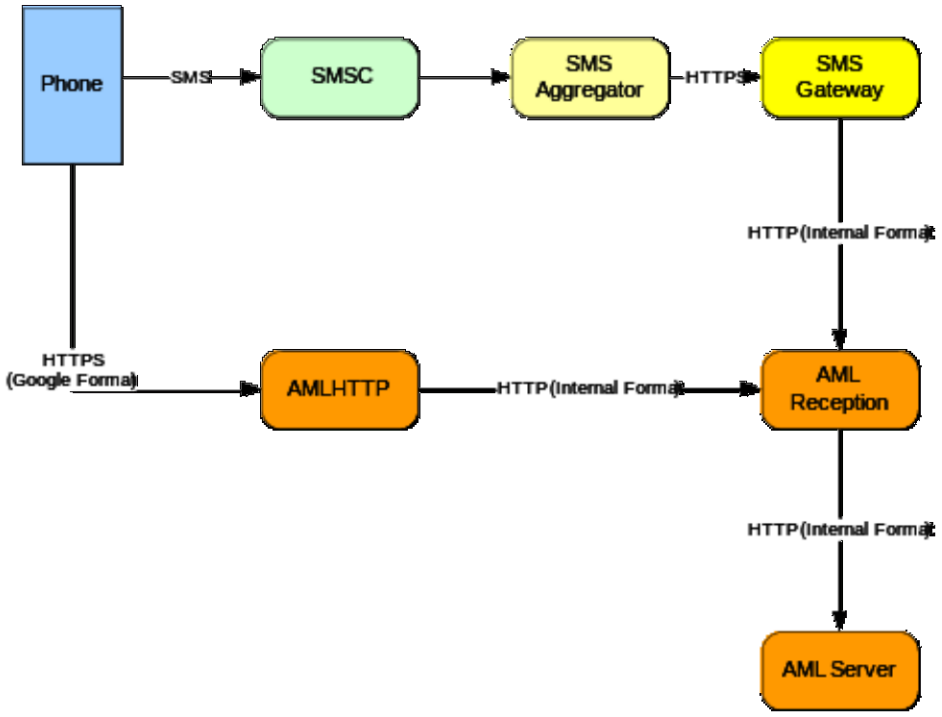

Figure 4 – SMS and HTTPS Message flows between the handset and the AML Server

Note that the output message will consist of two parameters, one of which (SRC-MSN) is the telephone number (the MSISDN) of the sending device and the other (MSG) contains the contents of the SMS message. Please refer to the table overleaf.

Security is an additional factor to consider when using the HTTPS method for sending locations from the handset. With SMS, the PSAP location server simply has to open up its firewalls for a connection from the SMS gateway. But with HTTPS, the location server needs to be able to receive messages from any client on the internet. This means that extra precautions must be taken to protect against denial of service attacks. The handset also needs to be sure to send its location to a valid PSAP server.

Use of HTTPS is important, and in a live environment server-side signed certificates would be used to prevent misdirection of messages.

The table below presents both the SMS and HTTPS fields:

HTTPS Field	SMS Parameter and Field	Conversion
device_number	SRC-MSN	exact copy
location_latitude	MSG – lt	restrict to 5 decimal places
location_longitude	MSG – lg	restrict to 5 decimal places
location_accuracy	MSG – rd	convert to integer
location_source	MSG – pm	convert to W/G/C/N
device_imsi	MSG – si	exact copy
device_imei	MSG – ei	exact copy
cell_network_mcc	MSG – mcc	exact copy
cell_network_mnc	MSG – mnc	exact copy
location_time	MSG – top	convert from Unix milliseconds to YYYYMMDDhhmmss
	MSG – lc	insert static level of confidence 67
	MSG – ml	count message length

Table 8 – AML (SMS and HTTPS) Reception Output message

7. CONCLUSION

The Help112 Consortium has selected a new E112 architecture which complies best with the selection criteria presented in section 2.2.

The selected new E112 architecture is mostly based on available standard interfaces, i.e. SUPL, SMPP, OMA-MLP. As highlighted below, none of these standard interfaces would require any extensions.

Only one interface would have to be standardized, which is the HTTPS interface between the SMS Gateway and the Help112 Server.

It is recommended to use the Minimum Set of Data (MSD) presented in section 7.2.1 to be used as the standard by any other OS provider or handset manufacturer should they implement the required Help112 software to their OS or software respectively.

Based on the test results, it is recommended to further consider the following methods for near future upgrades of the selected new E112 architecture:

- User Plane Network Based Location (NBL), which is a component of the Architecture 3, has been tested in both Lithuania and the UK.
    - Based on the test-bed results in Lithuania, the NBL solution proved to be an excellent fall-back solution (**Safety Net**) when GNSS or Wifi return no location information. For more details about the test-bed results in Lithuania, please refer to Deliverable D4.4 for NBL test in Lithuania. Please note that the preparation of a report on the results of the UK test-bed of the NBL solution is still ongoing as the furnished cell tower databases for some cells require filed visits to ensure its correctness and accurateness.
    - The SMPP interface is already standardized and require no further extensions.
    - Similar to the selected architecture, the HTTPS interface between the SMS Gateway and the Help112 Server would have to be standardized. Please refer to section 3.3 for more details.
    - Accordingly, the new format of the AML SMS containing the Radio Measurement Report (RMR) would be as listed earlier on this document in section 7.1.2.
    - This NBLimprovement needs nevertheless to be trade off with the drawback due to the necessary involvement of MNOs for providing the cell database, involvement that would seriously impede the deployment of E112.
- HTTPS transmission has been tested in the UK, Austria and Italy. HTTPS Transmission could serve as a supplementary transmission method to the robust SMS which enjoys a wider geographic coverage.
    - HTTPS transmission could carry additional information info.
    - The format of the HTTPS message has been listed in section 7.2.1, adopting the recommended definition presented by BT in Deliverable D4.3.

8. APPENDIX 1: ADVANCED MOBILE LOCATION – AML

The objective of the AML is to produce a simple, cost effective solution to the mobile location estimation challenge. This solution makes use of the **built-in location capabilities** of modern handsets. Once the mobile handset knows its location, it is sent to the PSAPs using a simple, already available, Short Message Service (SMS) based protocol, which gives up to 160 characters of data. An ETSI Technical Report[9] published in March 2016 provides a reference on AML for administrations, mobile networks and handset manufacturers.

In June 2016, Google communicated that 99% of Android phones in the market were now upgraded to support AML functionality. The Android Software Upgrade is called Android Emergency Location (AEL).

8.1 POSITIONING METHOD – GNSS + WIFI + CELL-ID

AML uses GNSS and Wi-Fi positioning to compensate the lack of accuracy by the existing implementation of caller location estimated by Cell ID. As soon as the emergency call is initiated the handset switches on GNSS and Wi-Fi, if not already activated. This activation is subject to a configurable battery check.

With AML, the handset immediately attempts to determine the location via all methods, so as to ensure that the transmission of the location data is done within a specific time interval, defined as the T1 timeout. The T1 timeout is the maximum time between the emergency call being initiated and the location SMS being sent. The AML specification suggests that T1 should be configurable with an "over the air" update. The T1 timeout in the UK has a value of 20 seconds.

8.2 TRANSMISSION METHOD – SMS

When the location is determined, the AML SMS is generated. The location SMS is routed to the home network SMSC of the caller. This SMSC has to be programmed to send emergency location SMS to a location server that handles emergency location SMS.

To be routed to the corresponding location server, the SMS is identified by an SMS number such as 112, or a dedicated full length MSISDN.

The call taker CAD has access to the location server and then is able to retrieve and display the location of the caller.

The use of an SMS to transmit the location data to the location server gives a maximum 160 characters of data to transmit all the needed location information.

The AML specification suggests that two types of SMS may be used to provide the AML location information: "regular SMS" and "data SMS". "Data SMS" is a particular subset of the SMS standard and it is important to note that this is not an SMS message sent through a data connection. It is 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. Which type of SMS message is used may depend on the op-

9 ETSI Technical Report, "Advanced Mobile Location for emergency calls", ETSI TR 103 393 V1.1.1 (2016-03)

tions open to OS providers to suppress a record of sent AML location messages on the handset. It is worth noting that data SMS is also called Class-zero SMS, which is invisible to the handset user.

9. APPENDIX 2: NETWORK BASED POSITIONING ALGORITHMS

This section describes the different positioning methods available through a mobile network.

9.1 CELL ID

Cell ID positioning simply returns the geographic position of the area covered by the device's serving cell. This area is dependent on the angle of coverage and cell radius. The latter can vary from 550 meters to several kilometers. Important note: the serving cell is not necessarily the closest cell tower from the caller.

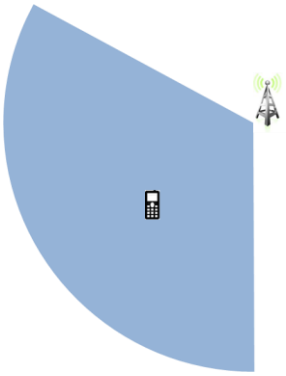

Figure 5: Cell ID precision level

9.2 2G - CITA

CITA is an abbreviation for Cell ID and Timing Advance. With the addition of timing advance, the device may be located within a 550m band within the serving cell.

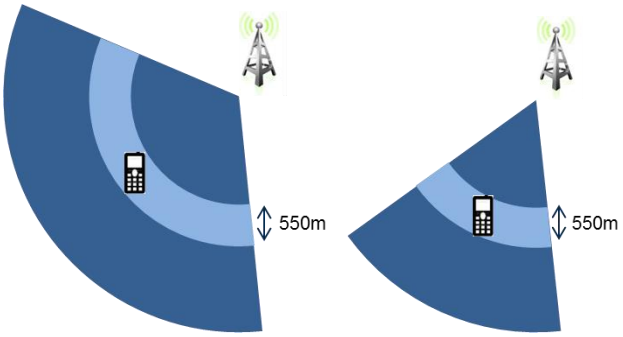

Figure 6: CITA precision level

9.3 2G - CITARx

CITARx is an abbreviation of Cell ID, Timing Advance and Received Signal levels. With the addition of received signal strengths from the co-sited cells, the position of the device may be calculated and a more precise position calculated along the given TA band.

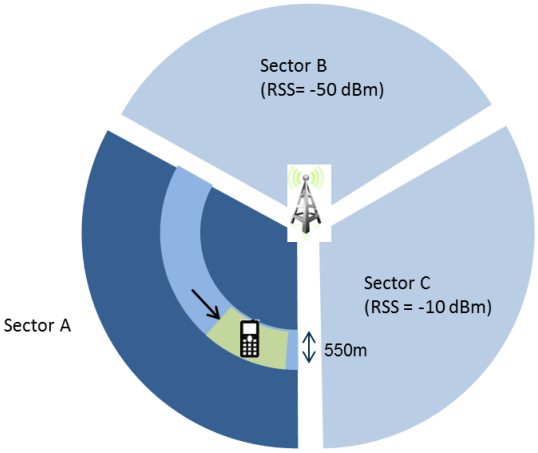

Figure 7: CITARx precision level

9.4 2G – RF Pattern Matching (RFPM)

The RF Pattern Matching positioning method is based on radio link measurements collected from the network and/or the mobile terminal. The method relies on predictions or models of the radio environment against which it performs an algorithmic comparison of the measurements to determine a best match estimation of the mobile terminal location. RFPM may utilise measurements other than the path loss measurements noted above, e.g. RTT or TA.

CS solution is commercially known as Accuracy+.

Figure 8: RFPM precision level

9.5 3G - CIRTT

CIRTT is an abbreviation of Cell ID and Round Trip Time. In UMTS (3G) networks a Round Trip Time parameter is returned. With 3GPP Release 9 the timing measurement has been enhanced, so that there are now Type 1 and Type 2 measurement.

This parameter allows the calculation of ~75-78m bands (Type 1) or ~35 m bands (Type-2) within the serving cell as shown. For 3G, neighbouring cells also return the RTT parameter. Note that the equivalent parameter, TA, is not returned for neighbouring cells in 2G networks. This additional information allows for a multilateration calculation and hence a much greater precision. For multilateration algorithms data is required from multiple cells from the Active, Monitored or Detected sets as described in 3GPP 25.453.

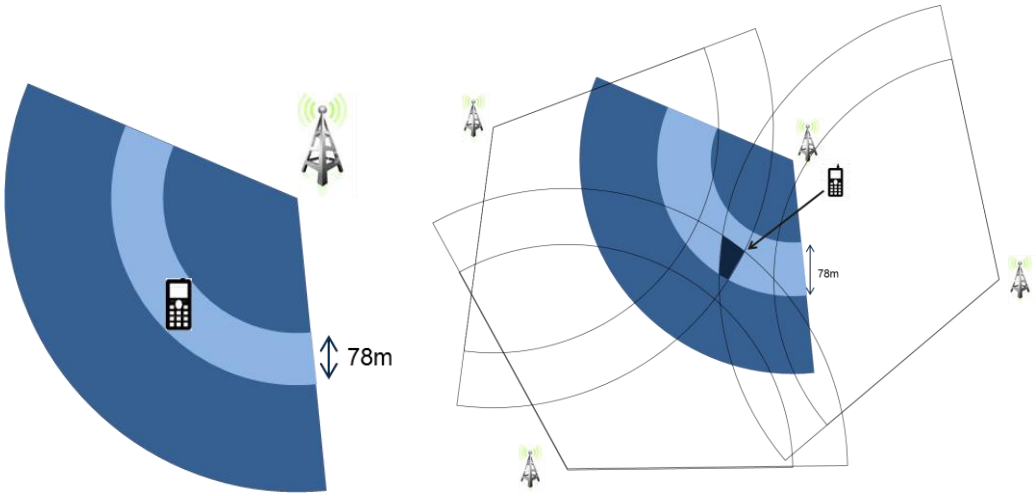

Figure 9: CIRTT precision level

9.6 4G - CITA

CITA is an abbreviation of Cell ID and Timing Advance. In LTE (4G), one of the position estimation methods is E-CID. This method can be executed in the following ways:

- E-CID - estimating distance from one base station

  Either RTT, Reference Signal Received Power or TA measurement value from Cell of origin is used in this method to estimate the distance of UE.

- E-CID - estimating the distance from multiple base stations

  In this method, the measurement values from multiple base stations are computed to perform Multilateration.

9.7 4G - OTDOA

Observed Time Difference Of Arrival (OTDOA) parameters are also availabale from LTE networks. The measurement of this parameter is more accurate than that for ECID and therefore once the multilateration calculations are computed, the returned accuracy is correspondingly greater.

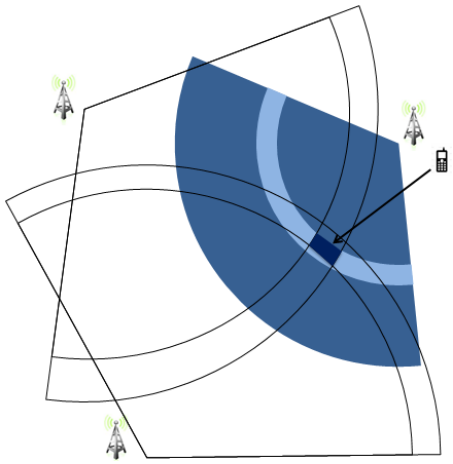

Figure 10: OTDOA precision level

10. APPENDIX 3: DATA SMS STRUCTURE

As described in the Android Emergency Location Data SMS Specification document, for sending a SMS from the handset to the carrier, a subset of the SMS standard - generally called a "data SMS" - is selected. It is important to note, this is NOT an SMS message sent through a data connection, this is simply a normal SMS which contains binary data 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 common as the normal SMS everyone is familiar with, but are still in use in specialized circumstances. The reason for choosing this type of SMS is that the Android OS will not automatically serialize a data SMS into the user's "sent messages" section, allowing for greater user privacy (and less confusion than seeing an unreadable text message).

For the purposes of Google's usage of SMS for the Emergency Location, we are only concerned with SMS from the handset to the mobile service center (SMSC), ie, SMSSUBMIT type messages.
SMSC's should be able to receive these messages without problems as they are part of the normal SMS standard. In the following, we consider an SMSSUBMIT message from the handset to the SMSC, which follows normal SMS standards (GSM 3.40).

We define a "data SMS" as a subset of normal SMS that:

1. Has the UserDataHeaderIndicator flag set in the SMS header (6th bit of the first octet of a GSM 03.40 or 3GPP 23.040 message)
2. Contains a UserDataHeader within the UserData of the SMS
3. The UserDataHeader contains an application port address InformationElementIdentifier (IEI)

It is necessary to send an SMS in this fashion rather than a regular SMS to ensure that it does not appear in the handset's list of sent messages. The above is that we consider necessary for an outgoing emergency location SMS, but we also present an example of a potential SMS user data segment below.

Note that we do not specify any particular DataCodingScheme (DCS) here. The DCS is used to identify the encoding within the UserData segment.

There are three options currently for the DCS:

- GSM 7 bit default alphabet (which includes national language shift tables)
- UCS2
- 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. For the purposes of emergency location, if the 8 bit data flag is set, the encoding used will be the GSM 7 bit alphabet, with each 7 bit encoded element occupying only 7 bits, not 8 bits. Thus the first element occupies bits 17, the second element 814, the third 1521, and so forth. For now it is a safe assumption that the DCS will always be set to 8 bit

data for emergency location data SMS, as this allows us to pack the maximum amount of information into the SMS.
Given that the UserData segment has a maximum of 140 bytes, and that the minimum size of a UserDataHeader that includes port information is 7 bytes, this leaves a maximum of 133 bytes (152 7 bit encoded elements) to encode the actual emergency message.

As an overview, the handset will send an SMS in this format, with the emergency location information contained in a binary format in the UserData segment of the SMS. Most SMSC's should be able to parse and return this type of text message without any problems as this is already part of the SMS standard.

Once the SMSC has received and parsed the message however, it is up to the carrier or receiving entity to decode the payload found in the UserData segment, as the SMSC has no special knowledge of how to parse this. If the DCS is set to 8bit data (currently always), then the binary data should be parsed into text as if it were a GSM 7 bit encoding, as mentioned above.

END OF DOCUMENT