EENA Operations Document

112 Smartphones Apps

Title:	112 Smartphones Apps		
Version:	1.0		
Revision Date:	25-02-2014		
Code:	2.2.3		
Status of the document:	Draft	For comments	**Approved**

EENA asbl
info@eena.org - www.eena.org

Contributors to this document

This document was written by members of the EENA:

Members	Country / Organisation
Alexander Bousema	Consultant / Vice-chair EENA Operations Committee
Bertrand Casse	Deveryware
Christof Constantin Chwojka	Notruf Niederosterreich, AU
Cristina Lumbreras	EENA
Daniel Hadot	Minister of the Economy, Finances and Industry, FR
David Ruiz	Catalonia 112
Fidel Liberal	University of the Basque Country (UPV/EHU)
Francisco Puertas	Geoceler
Mark Fletcher	Avaya
James Winterbottom	EENA
Joke Bonte	Federal Ministry of the Interior – Civil security, BE
John Medland	BT
José Oscar Fajardo	University of the Basque Country (UPV/EHU)
José Luis Solar	Telefónica
Lambros Lambrinos	Cyprus University of Technology
Luka Mulej	XLAB d.o.o.
Marko Nieminen	Emergency Response Centre Administration (ERCA), FI
Minna Ronkko	Cassidian
Peter Gerber	ASTRID
Peter Woodford	VoIPs911
Sandro Locati	Beta 80 Group
Wolfgang Kampichler	Frequentis AG
Wolfgang Weinem	Federal Criminal Police Office of Germany

Legal Disclaimer

This document is authored by EENA staff members with contributions from individual members of EENA and represents the views of EENA. This document does not represent the views of individual members of EENA, or any other parties.

This document is published for information purposes only and it does not declare to be a statement or interpretation of EU law or the national law of EU Member States. This document is entirely without prejudice to the views of relevant national statutory authorities and their legal functions and powers, whether under EU law or the national law of their Member State. Accordingly, under no circumstances may reliance be placed upon this document by any parties in compliance or otherwise with any applicable laws. Neither may reliance be placed upon this document in relation to the suitability or functionality of any technical specifications, or any other matters discussed in it. Legal advice, technical advice and other advice as relevant, may be sought as necessary.

Table of contents

EENA asbl
info@eena.org - www.eena.org

1 Introduction

All over the world, citizens expect to be able to contact emergency services with technologies they use to communicate every day[1]. Thus, European citizens have clear expectations about the availability of 112 emergency services with the enhanced capabilities of technology being used in every day life. The use of applications for smartphones (Apps) is increasing in Europe (see chapter 3).

In the last year a large number of "SOS" and "help" Apps have been created. Almost all European emergency services have been contacted by developers who wanted to send data and establish a voice connection directly to 112.

It is worth mentioning that some emergency services and some national public authorities together with EENA (European Emergency Number Association) have tried to drive pan-European initiatives to create a harmonised 112 application for smartphones that could be used by all citizens in the European Union. Unfortunately, all these initiatives have never been accepted. This may explain why some public authorities have already developed their own official Apps (see chapter 8) that can only be used by citizens living in a certain geographic area and may not work in the same way if they are used outside the boundaries of a certain Public Safety Answering Point (PSAP).

EENA strongly believes that all Apps connecting citizens with the emergency services have to work in a standardised way all over the European Union. Additionally, we also believe that a common pan-European App should be developed to ensure the availability of at least one App solution for accessing emergency services all over the European Union. Therefore, the scope of this document is to describe the functional requirements, recommend a common architecture and establish a minimum set of data to be sent by 112 smartphones applications to the most appropriate PSAP in case of emergency in a pre-NG112 (pre-Next generation 112) architecture. It is worth mentioning that this document is a high level description and further technical implementation documents will be needed. Furthermore, this document outlines some of the already available Apps for emergency services in Europe. The description of functional requirements and practices was obtained through information sent by EENA members.

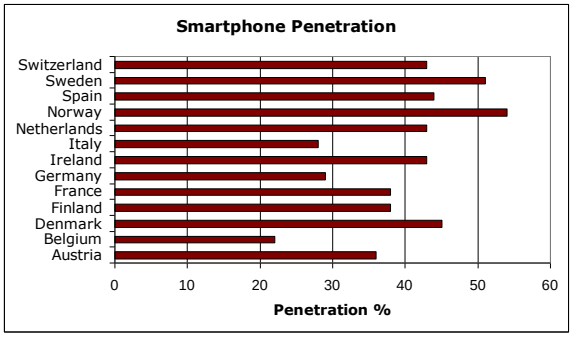
2 Abbreviations and Glossary

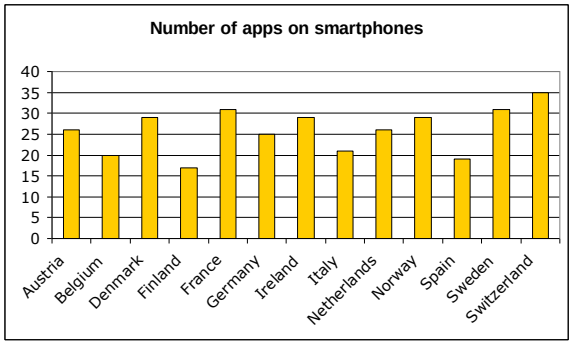
All definitions of terms and acronyms related to 112 are available in the 112 Terminology EENA Operations Document.[2]

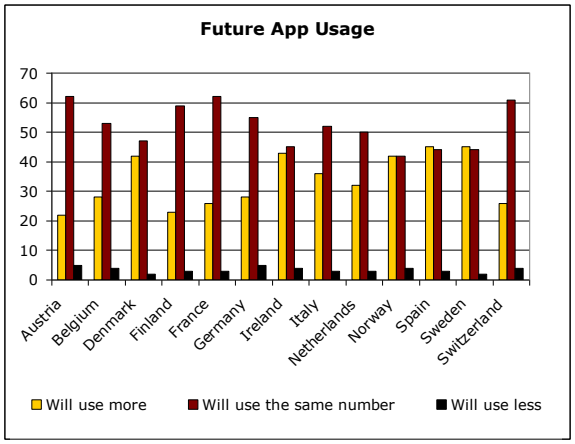
[1] www.redcross.org/www-files/Documents/pdf/other/SocialMediaSlideDeck.pdf
[2] www.eena.org/view/en/Committees/112operations/index/generalframework.html

3 Use of applications for smartphones in Europe[3]

The use of smartphones is increasing in Europe. Nowadays in some countries, the number of smartphones is higher than the number of mobile phones[4]. Europeans install in average more than 20 Apps and most of them will use, at least, the same number of applications in the future.







Europeans are using smartphones applications daily and, therefore, we can conclude that Apps for communicating with the emergency services are needed and they should work in the same way as 112, i.e. they should be available all over the European Union. This is the main reason why all the developed applications shall be compliant with a pan-European standard.

[3] www.thinkwithgoogle.com/mobileplanet/en/
[4] Smartphone penetration: percentage of mobile phone users who have a smartphone

EENA asbl
info@eena.org - www.eena.org

4 Why is a standard for 112 Apps for smartphones needed?

Technological development of the past years has changed the way citizens look at communication. Consequently, emergency services should make themselves accessible even if this has an impact on their technology. The main benefits of a pan-European standard approach are the following:

- Creating a pan-European standardised way to access 112 through Apps would put PSAPs more in control and not having to rely on propriety technology.
- Call-taker training would also be harmonised as a result.
- Handset-based additional data can be made available to emergency services; more accurate location being the most important one.
- With one European 112 Apps standard, the European emergency number 112 can be promoted. This way, citizens will better know how to get help in an emergency and misuse of this number will decrease.
- With one standard to connect to 112 with an application, people can use the application in their own language while being abroad and connecting to the local PSAP in that country.

Furthermore, all European citizens should have the possibility to download an App for contacting the emergency services. This is the reason why we recommend that a pan-European App, which will co-exist with other Apps that are compliant with the standard, should be developed.

5 Operating requirements

In this chapter the intended features that 112 Apps and PSAPs have to be compliant with are captured. There are three categories of requirements: namely "mandatory", "desirable" and "nice to have".

Mandatory:

- The call and data shall be routed to the most appropriate PSAP.
- The voice call to 112 shall be set up with no delays.
- The call shall be treated as an emergency call, i.e. prioritisation in the network, caller line identification and caller location shall be available
- Call-back to the citizen has to be available.
- Handset-based accurate caller's location information shall be sent to emergency services when available and at the same time of the voice call. Nevertheless, the voice call shall never be disrupted.
- The user shall confirm his/her willing to establish a 112 call in order to avoid false emergency calls.
- The App shall deliver a minimum set of data to the emergency services and shall facilitate the entering and delivering of this minimum standard dataset in their application.
- The functioning of the application that is built conform this standard should be guaranteed by all countries and regions of the European Union for at least the basic functions mentioned here.
- People with specific communication needs shall be able to use the App as a starting point of setting up communication with the most appropriate emergency service.
- Information and telecommunication technology security risks, i.e. authentication and privacy protection, have to be taken into account. The authentication of the phone has to be done during the installation process.
- The emergency App must be a native developed App and should be developed for the more used operative systems.

EENA asbl
info@eena.org - www.eena.org

Desirable:

- To send and receive extra information (photo and video) from people in or witnessing an emergency should be possible.
- Optional additional data should be available in a format that can be shared with the emergency service

Nice to have:

- The App should also facilitate the communication from emergency services towards citizen.
- The application should be country/regional aware and be able to inform the user of other local relevant Apps for official services.
- The App should work with the more used operating systems.

EENA asbl
info@eena.org - www.eena.org

6 112 Apps MSD data structure

6.1 112 Apps MSD based on eCall MSD data structure (1)

An eCall is an emergency call generated either automatically via activation of in-vehicle sensors or manually by the vehicle occupants; when activated, to provide notification and relevant location information to the most appropriate PSAP, by means of mobile wireless communications networks and carries a defined standardised minimum set of data (MSD), notifying that there has been an incident that requires response from the emergency services and establishes an audio channel between the occupants of the vehicle and the most appropriate PSAP.

All member states in the European Union will have to upgrade their 112 systems to be able to receive and handle eCalls. The technology used to establish the connection between the vehicle in distress and the most appropriate PSAP is based on in-band modem technology. This technology cannot be used directly in smartphones however but it would make sense that data sent by the App follows the same structure as eCall messages.
The data that is sent by the vehicle in case of an accident is the eCall MSD[5]. In this context, we can speak about App MSD as the standardised format of the message that is sent by the App to the PSAP.

The idea is to make eCall MSD and App MSD compatible with each other. This is the reason why some of the blocks have been intentionally left blank. The following table shows the information in a simple way:

Block N	Name	Mandatory/ Optional	Description
01	ID	M	The purpose of this data concept is to: discriminate from later MSD formats.
02	Message Identifier	M	The purpose of this data concept is: so that if any of the information in the MSD has been updated, it can be discriminated from the original MSD.
03	Control	M	The purpose of this data concept is to: Advise the emergency services of - whether the position information can be trusted - whether the call is a real emergency or known to be a test call. This is considered useful information for the PSAP/emergency services. For example: If the position cannot be trusted the emergency services may take extra steps to help confirm the location. This flag should only be cleared to "position can be trusted" if a 2D or 3D position fix from current GNSS reception is available
04	IMEI (mobile phone identification)	M	*(Vehicle identification in eCall MSD)* The purpose of this data concept is to give a unique identifier of the handset to emergency services. It can be useful to combat false emergency calls.
05	Caller line identifier		*(Vehicle propulsion storage type in eCall MSD)* Emergency services can use this field for call-back.
06	Time stamp	M	The purpose of this data concept is to: Identify the accurate time of the incident. This is important in issues to do with how long the injured persons have been affected. It is important also for emergency services performance management.
07	Caller Location		Advise the emergency services of the exact location of the caller so that emergency services can locate it as quickly as possible.
08	*Blank*		*(Vehicle direction in eCall MSD)*
09	*Blank*		*(Recent Vehicle Location n-1 in eCall MSD)*
10	*Blank*		*(Recent Vehicle Location n-2 in eCall MSD)*
11	*Blank*		*(No. of passengers in eCall MSD)*
12	Optional additional data	O	Voluntary optional data fields are not required, but may be able to provide the emergency services with useful relevant additional information. The additional data field may include an address or the language of the caller where other relevant related data or functions are available.

[5] Intelligent transport systems - eSafety - eCall minimum set of data (MSD) – European Standard EN 15722

6.2 112 Apps MSD based on PIDF-LO data structure (2)

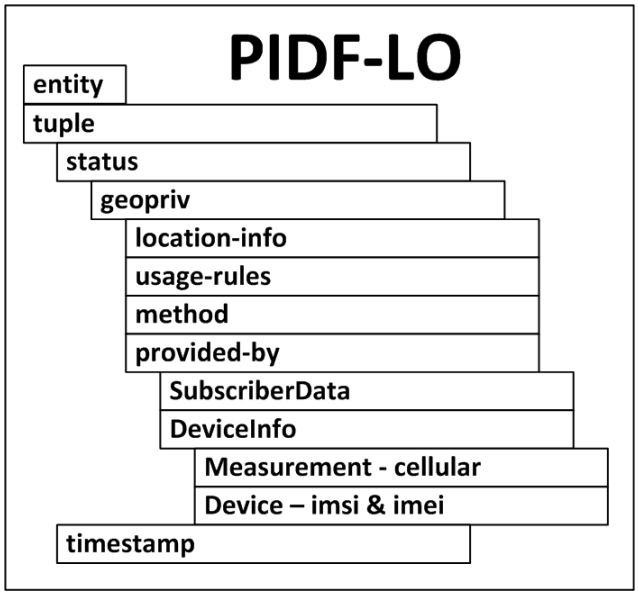
NG112 provides for a plethora of supplementary information to be sent about a caller, the various access and service providers as well as the device on which the call is being made. These data use XML (Extensible Markup Language) structures defined in the IETF[6] (The Internet Engineering Task Force) and used in a range of protocols used in other organisations such as 3GPP[7], ETSI[8] (European Telecommunications Standards Institute) and NENA[9] (National Emergency Number Association). Using these data structures in smartphone emergency calling applications provides compatibility with NG112[10] (Next Generation 112) and a clear migration path to NG112.

Information about an emergency call can be considered a form of presence information; indeed this is how the IETF treats location information in general. For an emergency call, it has to be considered who the caller is, when the call is made, where the caller is located, and information about the calling device. The all encompassing data structure for location-based presence information in the Presence Information Data Format Location Object (PIDF-LO) and is specified in RFC4119[11].

Rules about how to format a PIDF-LO and what kinds of geodetic information should be supported are defined in the PIDF-LO profile specification RFC5491[12]. A smartphone emergency calling application must support all of the two dimensional (2D) shapes defined in this document to be compatible with NG112.

Other information about the subscriber (name, home address, email address) and the device, such as IMEI (Mobile Equipment Identity), IMSI (International mobile subscriber identity) and serving cell can be sent in the additional structures defined in draft-ietf-ecrit-additional-data[13].

The overall flow of the data structure for use by emergency applications is shown below. Detailed description of the data structure can be founded in annex B.



[6] www.ietf.org
[7] www.3gpp.org
[8] www.etsi.org
[9] www.nena.org
[10] www.eena.org/view/en/Committees/NG112.html
[11] tools.ietf.org/html/rfc4119
[12] tools.ietf.org/html/rfc5491
[13] tools.ietf.org/html/draft-ietf-ecrit-additional-data

7 High level technical architecture overview

The long term scenario should be compliant with the NG112 specification; in the meantime the 112 applications will implement transition solutions. In this chapter an overview of the possible technologies that can be use to send the App MSD to the PSAP is described.

7.1 MSD data on the screen (1)

The application is a speed dial button to 112. It shows the MSD data on the screen and the user is able to read it to the 112 call-taker.
This simple solution could be useful and not complicated to implement. Nevertheless, mandatory operating requirements such as *"People with specific communication needs shall be able to use the App as a starting point of setting up communication with the most appropriate emergency service"*, are not covered.

7.2 MSD read by a synthetic voice (2)

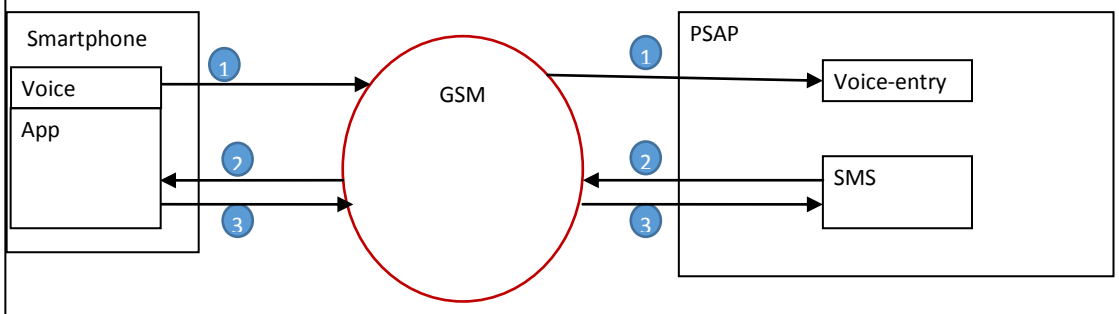
Another option is to integrate a synthetic voice that reads the data in the MSD to the call-taker. Once the communication between the citizen and the PSAP has been established, the synthetic voice delivers a message in the language of the country and reads the content of the MSD.
On one hand, this option could be useful for locating people with communication disabilities. On the other hand, sending automatic messages to 112 may be restricted in some European countries and also be not viable because of the existence of automatic welcome messages.

7.3 MSD data sent by SMS (3)

In this solution, the information is delivered to the PSAP by legacy method (SMS – Short Message Service). The application will build the MSD without optional data and send it to the PSAP using SMS.

The main problem in the SMS based solution is to know the most appropriate PSAP's number to send the MSD. One approach to solve this problem could be that the PSAP, after having received the 112 call sends an SMS to the caller with an e.164 number where the App can send the MSD. The MSD will be then sent to the PSAP.

Schematic representation of Smartphone application using SMS



1 = 112 call (voice) with caller line identification (CLI)
2 = SMS sent from the PSAP to the caller with e.164 number
3 = Apps sends SMS with MSD to the PSAP's e.164 number

It is worth mentioning that some European countries have already implemented e-SMS to contact to emergency services. As already mentioned, the strongest point of this solution is the already available SMS reception and dispatch technology in some PSAPs. The weaker sides are the delays that SMS can suffer and the restrictions of numbers of characters to be sent by SMS.

EENA asbl
info@eena.org - www.eena.org

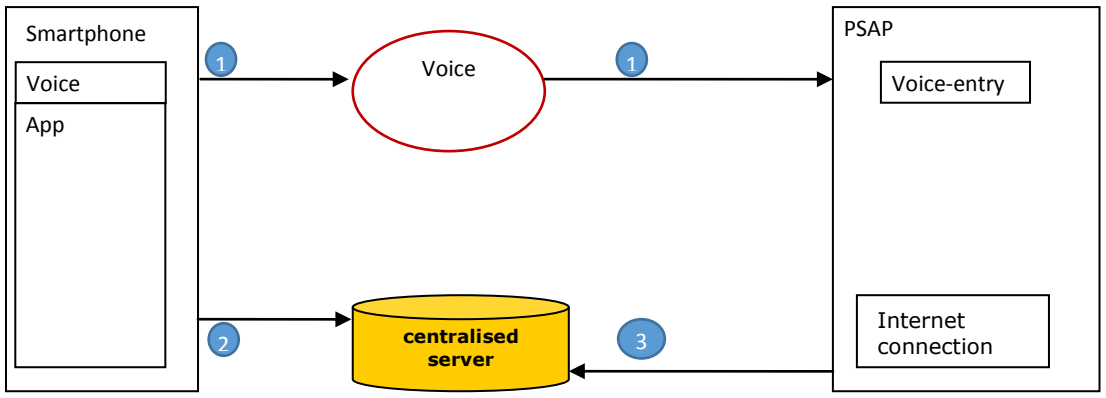
7.4 MSD delivered through mobile data services

In this section, the MSD is delivered through mobile data services. Two models are described: in the first one MSD is pulled by the PSAP from a central server and in the second one the MSD is pushed to the most appropriate PSAP.

7.4.1 Centralised server (pull option) (4)

The Apps MSD should be sent using the data connection of the mobile phone and received by a server. PSAPs will connect to the central server and pull the MSD using, for instance, the caller line identification number of the caller.

Schematic representation of Smartphone application using a centralised server (pull option)



1 = 112 call (voice)
2 = The App sends the MSD to a centralised server (all apps will use the same)
3 = the PSAP pulls the data from the centralised server

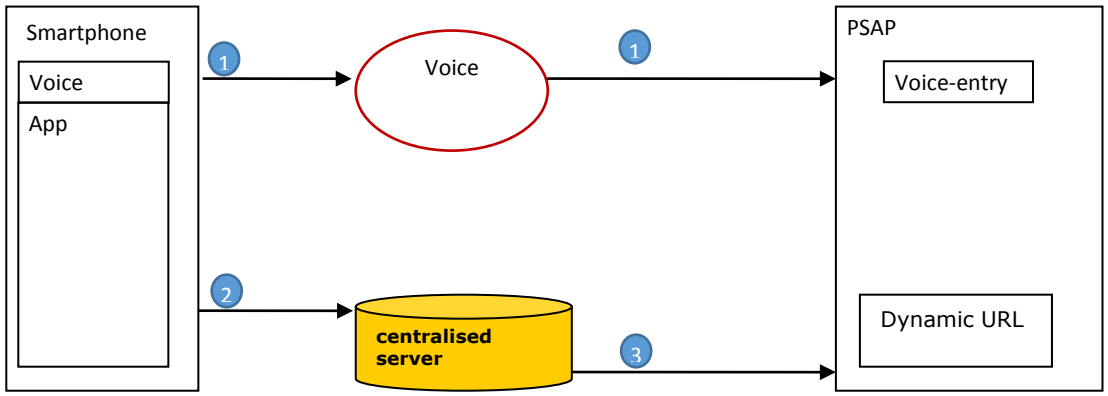
The main problems of this architecture are the not currently existing legal framework for sharing the data with the PSAPs and how to secure the transfer and (temporary) storage of the shared data. The positives sides of this architecture are the small update efforts to be made by the PSAPs and the flexibility of using the mobile data network to send the MSD (for instance format and number of characters restrictions).

EENA asbl
info@eena.org - www.eena.org

7.4.2 Centralised server (push option) (5)

The Apps MSD should be sent using the data connection of the mobile phone and received by a server that could then route data to the most appropriate PSAP.

Schematic representation of Smartphone application using a centralised server



1 = 112 call (voice)
2 = The App sends the MSD to a centralised server
3 = the centralised server pushes the MSD to the most appropriate PSAP (databases with boundaries and PSAPs' addresses)

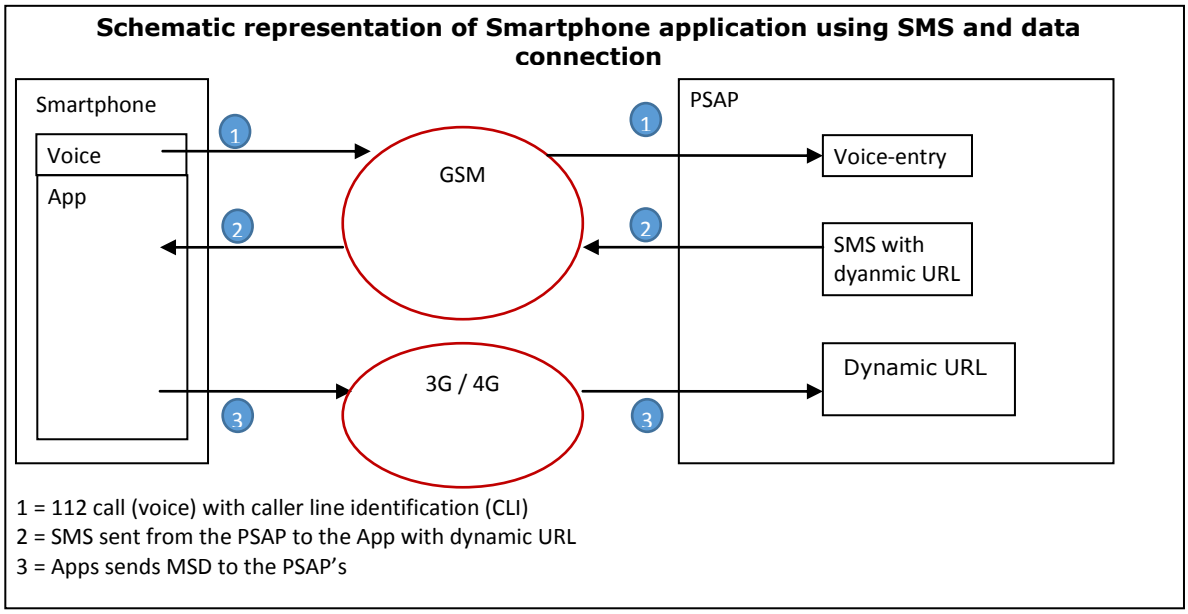
This solution is compatible with future evolutions of technology. The PSAP receives the data with no delays in comparison with other architectures.

One of the challenges of this solution is to manage the database containing the dynamic URLs (uniform resource locator) of the PSAPs and their boundaries. These data are currently not available. Subsequently, the database should be maintained.

As for the previous solution, the main problems of this architecture are the not currently existing legal framework for sharing the data with the PSAPs and how to secure the transfer and (temporary) storage of the shared data.

7.4.3 Combination of mobile data services and SMS approach (6)

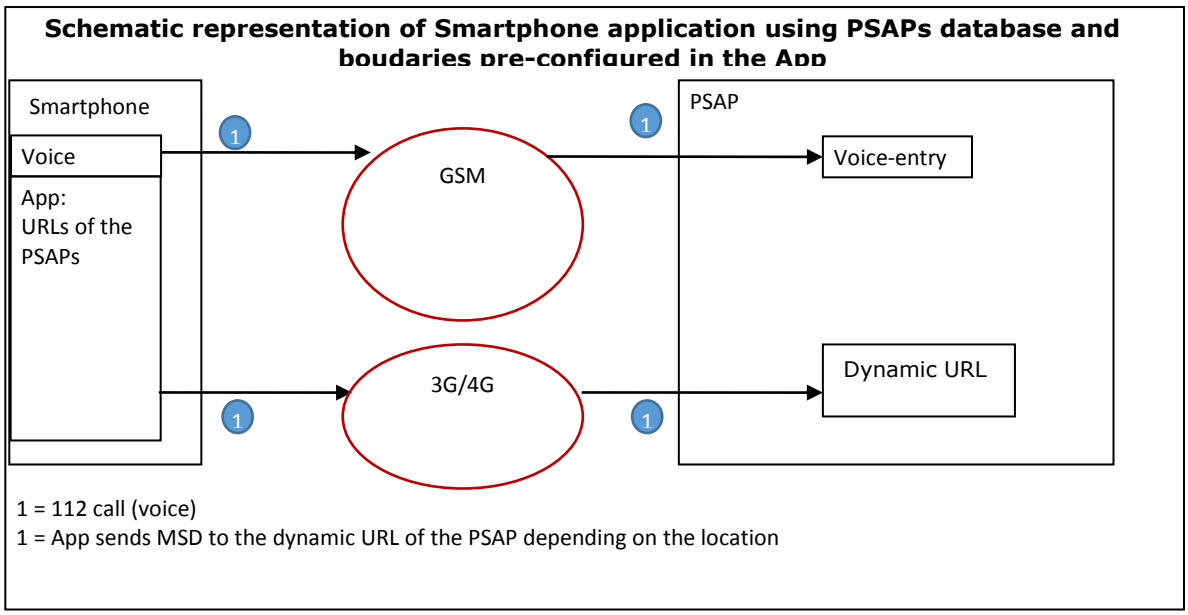
Callers make a 112 call to the PSAP. Consequently, the call is routed to the most appropriate PSAP. Caller location identifier and cell identifier (depending on the country) are available with the call.
Once the call is received by the PSAP, the PSAP sends an SMS to the phone including its dynamic URL. The App can then send the MSD to this dynamic URL and it is received by the PSAP.



In this architecture there is no centralised server, consequently problems described in the previous sections would not apply. Nevertheless, weakness of SMS has been already explained.

7.4.4 PSAPs database and boundaries pre-configured in the App (7)

The 112 application is preconfigured to send location data to a dynamic PSAP's URL.



This solution is the easiest way to start with. One of the challenges of this solution is to manage the database. The first step would be to create a database with all dynamic PSAPs' URL. These data are currently not available. Subsequently, the database should be maintained.

7.5 MSD delivered through mobile network (8)

Following 3GPP and ETSI specifications[14], the handset location data are transmitted to the mobile network operator's GMLC (Gateway Mobile Location Centre), and then the GMLC push these data to the designated PSAP (3GPP/ETSI) using the same mechanism and geographical data base as currently used for the regular 112 voice call and caller location routing.

This standard architecture is a reliable and robust solution by reusing existing deployed implementations across Europe. In addition, it is a future proof approach that supports the 3GPP/ETSI interfaces between handset and network and network-PSAP. Data transmission security and handset tracking functions are supported by standard specifications.

7.6 MSD delivered through the smartphone's softmodem (9)

Using the eCall capabilities that will be established, the caller location information is communicated through mobile networks. In eCall, the in-vehicle system takes the geographical position from the satellite positioning system module and converts it into an MSD, subsequently the in-vehicle system's modem on-board sends the MSD in-band with the voice call to 112. Finally, the PSAP receives the MSD.

In smartphones their in-built softmodem can be used to send the location to the PSAP. The phone's operating system has to be modified that when dialing 112 it would first pick the satellite positioning system position, create a "mobile phone MSD" and send this using the modem; the PSAP would receive an eCall from a non-vehicle-based device and could decode the location in its system.

[14] www.etsi.org/deliver/etsi_ts/123200_123299/123271/10.04.00_60/ts_123271v100400p.pdf

8 General challenges

- Managing of different sources of location by the PSAPs:
An additional challenge for the PSAP would be to manage the two sources of caller location: the current compulsory access network data and the new handset data. Both locations' data could be related using the caller line identification number.

- Configuration of mobile networks
Another problem to be solved is the fact that some network operators do not allowed to send data (through SMS or mobile data connection) at the same time an emergency call is done. Changes in the mobile network parameters may be necessary.

- Responsibility in case of malfunctioning:
One of the major concerns of emergency services is who is responsible in case of malfunctioning of the App. This question is answered the same way as who is responsible if a call is made to 112 and because of technical failures it does not reach the PSAP (for instance the handset, the network or the PSAP may be not responding).

- Accreditation process:
Certification that the App is fully compliant with the pan-European standard has to be organised. European standardisation bodies may have to be involved.

- Cost for call taker:
Placing an emergency call is free of charge all over Europe, even when you have a pre-paid SIM without credit or if you are on a roamed network.
On the other hand, data connection is always charged. Due to this, if you may expect that the user has signed a flat-rate while under his/her home network, most users will disable data roaming in foreign countries (preventing unexpected costs and increasing battery life).
To really address a pan-European infrastructure, emergency data connection should be free of charge and granted even when roaming is disabled.

- Link between data and voice call:
Up to now, even if defined by the spec and available as OS API, the SIM does not provide the caller-ID. Thus the voice-data association is not as trivial as it may appear. Up to now the user needs to register himself on a centralised service (pairing manually provided caller-ID with either an App instance ID or a device ID), but granting the right identity, supporting single identity on multiple devices, and avoiding identity switching is a real tough issue.

9 Recommended architecture

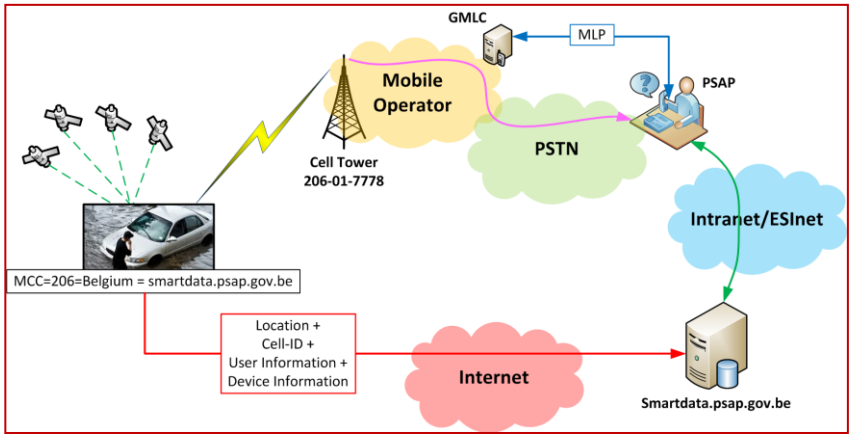
The recommended architecture takes into account a large number of factors, including political, regulatory and evolutionary aspects. A single application needs to be able to work in the same way in any of the euro-state countries while still acknowledging each country's autonomy. It is for this reason that a single pan-European smartphone application data server was deemed impractical. Countries requiring emergency information to be resident in regional PSAPs before it can be accessed need to direct data arriving at the centralised server to correct regional servers. Requiring a smartphone application to maintain regional PSAP boundaries for all member states is deemed impractical as it would lead to the application needing to maintain hundreds of routing boundaries that are subject to change and keeping application data up to date becoming a real challenge.

For these reasons, the chosen architecture places a smartphone application data server in each member state. This has the advantage of addressing the two stated issues and is easy to solve in a smartphone application because the mobile country code (MCC) is readily discernable from the current serving cell information. The net result is that a smartphone application need only maintain 28 entries, mapping MCC to a country server address.

EENA asbl
info@eena.org - www.eena.org

Smartphone applications of this nature provide a forerunner to NG112. The smartphones are expected to convey highly-accurate location information as well as information about the calling device and caller. As a consequence of this using the data formats specified for use in NG112 provides the best forward migration path for PSAPs to NG112 and avoids the introduction or prolonging of intermediary and legacy data formats. This allows all data to be conveyed in an IETF PIDF-LO presence document. The contents of this document will be the telephone number of the calling device, the location of the device, information about the calling subscriber and information about the calling device. Additional information can be provided if desired. If required, the nationally-centralised server is able to convert the data coming from the NG112 smartphone App format to a national format (for example the eCall MSD) for consumption by the PSAP.

The general flow is described in the following figure:



Data is pushed from the smartphone application to the specific country's centralised server using secure HTTP It is recommended that applications be certified from a common root certificate authority so as to reduce the likelihood of spam and denial of service attacks on the servers. The nature of this certification architecture and operational structure are for further study. The smartphone application may periodically push information updates to the centralized server. To keep client and server implementations more simple, updates contain all the additional information and the server replaces any previous record with the new record rather than trying to determine which specific content has changed.

Location veracity can be checked a certain degree at the PSAP. The cell-id provided by the device in the additional-data push not only identifies the cell but also the operator network to which the cell belongs, the mobile network code (MNC). This can be used by the PSAP to cross-reference against the operator network from which the call originated. In addition to this, the PSAP may have been provided the cell-id by the operator or the coverage area of the cell and this can be compared to the information provided by the device.

Once the location and additional data has been stored at the national central server it may be pushed to the PSAP or pulled from the PSAP depending on country policies and preferences. Each record has a time stamp applied to it when it arrives at the server and records are deleted after they exceed a certain age determined by the specific country.

10 EENA recommendations

Stakeholders	Actions
Application developers	• Implement the standard
European Authorities	• Mandate the creation of a standard for emergency smartphones applications data communication to PSAPs • Make the use of this standard mandatory • Ensure the necessary legislation is in place and implemented correctly by the Member States • Dissemination of the use of 112 Apps
European/National Standardisation bodies	• Creation of a standard for emergency smartphones applications • Certify that the Apps are compliant with the mandatory set of functionality • Enforce the standard and prohibit the non-compliant Apps
Telecommunication operators	• Implement necessary changes within the networks as necessary • Dissemination of the use of 112 Apps
Competent Regulatory Authorities	• Ensure that the telecommunication operators and all other relevant organisations comply with the legislation
National / Regional Authorities	• Set up the required solution for receiving data from Apps for their PSAPs • Dissemination of the use of 112 Apps
Emergency services / PSAP Management	• Upgrade the 112 systems to be compliant with the standard • A procedure for handling emergency Apps for smart phone data available • Dissemination of the use of 112 Apps

EENA asbl
info@eena.org - www.eena.org

ANNEX A: Examples - smartphones application for accessing emergency services

As it was already mentioned in previous chapters of this document, in some countries public authorities have developed 112 Apps that are already available for citizen.

Denmark:

- 112 Denmark: http://www.112app.dk/

With Denmark's official 112 App citizens can initiate a call to the PSAP and satellite positioning system coordinates will be sent simultaneously.

Iceland:

- 112 Iceland: (Link)

It is the official App for Iceland's emergency service 112. The App sends an SMS to the Icelandic emergency service 112, with the phones satellite positioning system location, before calling 112

Italy:

- Lombardy's emergency services 112 - AREU

WHERE ARE U	WhereAREU is the official App for Lombardy's emergency service 112. The App places the emergency call and, in the background, it sends info about the location and the profile (including a list of ICE-contacts) of the caller. To increase user's confidence with and faith in the App, a DEMO function is available. Technical details: ○ The App architecture implements the "centralised server (pull option)" scenario as described in the document ○ The App is developed as native-App and will be available for Android, iOS, WindowsPhone8. It is in testing phase and will be available on the stores in spring. ○ The App uses data connection as primary channel, but is aware of its unavailability and is able to use GSM-SMS texting as fallback channel. ○ The communication channel is secured by a server certificate, and each request is protected against Denial of Service and fake request attacks by a custom App/service handshaking protocol. ○ The App has a DEMO function, which places a real call to the PSAP and really sends data. Of course the call is routed to a dedicated number with an automatic response (fixed or text-to-speech may be used). In our analysis we found that people are usually scared of using an App they are not confident with. This feeling is, obviously, increased in emergency situations. To let people become confident with the App, we added this feature. ○ The App is widely based on our e-call backend infrastructure. ○ The App is able to send profile data of the expected caller. The dataset is currently under study. Up to now we include the owner's static data and allow him/her to setup a list of ICE-numbers which will be shared to the PSAP. Other info (i.e. allergies, intolerances, known disease, ...) may be added. ○ The App allows the caller to check on a map the current position, without the need to switch App.

Spain:

- Canary Island: http://www.112canarias.com/info/

- ○ exact location sent to the PSAP
- ○ communication establishment by voice, text (instant messaging) and images
- ○ profile details such as blood group or chronic illnesses information sent to the PSAP

- Catalonia:

  - citizen can receive information about emergency situations (Link)

  - The 112 Emergency Service along with Telefónica and the Catalan Deaf People Federation (FESOCA) is currently developing a new App for cell phones. It will display three pictures representing Fire Department, Police Department and Health Services. Depending on the button that is pressed, different pictures will show up, each of them reflecting different situations that might be happening, as well as advices about how to act and instructions communicated via sign language. This way this App will be easy for low hearing capability people because every possible situation will be based on inphography, text messages and sign lenguage videos. Besides, this App will allow locating the call geographically and transmitting all the data to the Catalonian PSAP.

- DGT (Directorate-General for Traffic): (Link)

  - fast dial to 112
  - citizen can receive information coming from public authorities

The Netherlands:

- Politie Netherlands:

  - Send picture or videos to the police

Other 112 Apps are claiming to have a 112 functionality. Some examples are listed below:

Echo 112 (Switzerland)
http://www.echo112.com/

Help! (Vodafone foundation)
http://enviu.org/our-work/help-App/

PAP town counsel (Singapore)
http://www.youtube.com/watch?v=MOEIk4Bg2qU

112 Alarm (NL)
http://www.112-alarmapp.com/

Rescue phone (NL)
http://www.rescuephone.nl/home

ANNEX B: Detailed description of the data structure

The entity is a URI that specifies who/what the presence information pertains to. This will be a tel URI using the MSISDN of the calling device.

Tuple, status and geopriv are all common element types that contain the specific presence information elements that we wish to convey.

The location-info element contains the actual location information to convey. This is usually a shape defining an area in which in the calling device can be found. The shapes that must be supported are the 2D set defined in RFC5491[15]. For devices using one of the various global navigation satellite system (GNSS) technologies, location is generally provided as a circle, ellipse or ellipsoid. And example of how to encode this in a PIDF-LO is shown below:

```
<gp:location-info>
               <gs:Ellipse srsName="urn:ogc:def:crs:EPSG::4326">
                 <gml:pos>42.5463 -73.2512</gml:pos>
                 <gs:semiMajorAxis uom="urn:ogc:def:uom:EPSG::9001">
                   1275
                 </gs:semiMajorAxis>
                 <gs:semiMinorAxis uom="urn:ogc:def:uom:EPSG::9001">
                   670
                 </gs:semiMinorAxis>
                 <gs:orientation uom="urn:ogc:def:uom:EPSG::9102">
                   43.2
                 </gs:orientation>
               </gs:Ellipse>
</gp:location-info>
```

The usage-rules define how the information may be used, this is most often just left empty.

The method element defines how the location was determined. The allowed values for the method element are defined in a IETF register, http://www.iana.org/assignments/method-tokens/method-tokens.xhtml - method-tokens-1. In general for smartphone applications this will be some kind of satellite positioning system value. If the method is known then the element should be omitted.

The provided-by element is used as a container to provide additional information about the subscriber and the device. This is shown below:

```
<provided-by
   xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:emergencyCallData"
   xmlns:sub="urn:ietf:params:xml:ns:emergencycalldata:SubscriberInfo"
   xmlns:dev="urn:ietf:params:xml:ns:emergencycalldata:DeviceInfo"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <emergencyCallDataValue
          purpose="emergencyCallData.SubscriberInfo">
      <sub:emergencyCallData.SubscriberInfo>
            ...
      </sub:emergencyCallData.SubscriberInfo>
   </emergencyCallDataValue>
   <emergencyCallDataValue
          purpose="emergencyCallData.DeviceInfo">
      <dev:emergencyCallData.DeviceInfo>
            ...
      </dev:emergencyCallData.DeviceInfo>
   </emergencyCallDataValue>
</provided-by>
```

[15] tools.ietf.org/html/rfc5491

The SubscriberData container is defined in the IETF additional-data specification. It consists of a privacy indicator and an xCard element that provides and name and contact information for the subscriber. Table 1 provides the fields and suggested values:

Table 1 SubscriberData description

Field	Description	Recommended Value
id	Common identifier linking all blocks provided by the same entity.	This should be the same as the value used in the id element of the DeviceInfo block.
privacyRequested	Caller is requesting that their personal data be kept as private as the local jurisdiction allows for emergency calls	false
SubscriberData	Details about the caller. This is a complex structure with recommended data described in Table YYY	Table YYY

The subscriber data can cover quite a few areas. The recommend information types are covered in Table 2. Each of the information blocks are further broken up into their own tables with each field described in detail.

Table 2 Caller information

Caller information	Description
Name of caller	The full name of the caller including things like salutations. See Table 3.
Home address	The home address of the caller. This can provide things like nationality that may be of importance. See Table 4.
Age and gender	This is information optional. See Table 5.
Languages spoken	Provides a list of the languages that the caller speaks. This is covered by using the <*lang*> element, a new element is required for each language spoken. See Table 6.
Other contact information	Provides other ways to contact the caller. This may include a home telephone number, an instant message account name or an email address. See Table 7.
Emergency contact information	It is often useful for a person to provide information about whom to contact in the event that the person becomes involved in a critical situation.

Table 3 Caller name information

Caller Info.	Desc.	xCard field	Example
Full name	Full name of the caller	<vcards><vcard><fn><text>	<fn><text> John Smith</text></fn>
Surname	Family name of the caller	<vcards><vcard><n><surname>	<n><surname>Smith</surname>/n>
Given name	First name of the caller	<vcards><vcard><n><given>	<n><given>John</given></n>
Additional name	Any additional names the caller may have. One element is required per additional name	<vcards><vcard><n><additional>	<n><additional>Cedric</additional></n>
prefix	Prefix salutation, for example Mr., Dr., Sir.	<vcards><vcard><n><prefix>	<n><prefix>Sir</prefix></n>
suffix	Any honorific suffix, such as MD or Jr. If there is more than suffix then the values should be included in multiple suffix elements	<vcards><vcard><n><suffix>	<n><suffix>MD</suffix></n> <n><suffix>Sr</suffix></n>

Table 4 Caller home address information

Address description	ADR field	Example
Indicator of the type of address, e.g. home or work	<adr><parameters><type><text>	<type><text>home</text/</type>
Optional full address label	<adr><parameters><label><text>	<label><text>John Smith 222 Ragoon street Oonagallabi Ozone Oz 5555</text></label>
Post office box :- Not recommmended	pobox	
Extended address elements. Used where required only.	<adr><ext>	
The street and house number information	<adr><street>	<street>222 Ragoon Street</street>
The city or town name	<adr><locality>	<locality>Oonagallabi</locality>
State, county or region information	<adr><region>	<region>Ozone</region>
Postal code	<adr><code>	<code>5555</code>
Country	<adr><country>	<country>Oz</country>

Table 5 Caller age and gender information

Caller Information	xCard field	Example
Age	<bday><date>	<bday><date>15/08/1983</date></bday>
Gender	<gender><sex> Valid values are: M,F,O,N,U	<gender><sex>M</sex></gender>

Table 6 Caller language information

Caller Info	xCard field	Example
The order of preference of a particular language, since a caller may speak more than one language.	<lang><parameters><pref><integer>	<parameters><pref><integer>1</integer></pref></parameters>
The language spoken	<lang><language-tag>	<language-tag>en></language-tag>

Table 7 Caller alternative contacts

Caller Info	xCard Field	Example
An alternative telephone number	<tel>	<tel> <parameters><type> <text>**home**</text> <text>voice</text> </type></parameters> <uri> tel:+61 55 55555555 /uri> </tel>
An email address	<email>	<email> <parameters> <type><text> work </text></type> </parameters> <text>jw@eena.org</text> </email>

Table 8 Caller emergency contact information

Caller Info	xCard field	Example
Emergency contact information	<related>	<related> <parameters><type><text> emergency </text></type></parameters> <uri> tel:+61-2-42266004 </uri> </related>

SubscriberData example:

```
<sub:emergencyCallData.SubscriberInfo
        xmlns:sub="urn:ietf:params:xml:ns:emergencycalldata:SubscriberInfo"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   privacyRequested="false">
       <sub:id>12345</sub:id>
       <sub:SubscriberData xmlns="urn:ietf:params:xml:ns:vcard-4.0">
           <vcards>
               <vcard>
                   <fn><text>James Winterbottom</text></fn>
                   <n>
                       <surname>Winterbottom</surname>
                       <given>Anthony</given>
                       <additional>James</additional>
                       <prefix>Mr</prefix>
                       <suffix/>
                   </n>
                   <bday><date>25/08/1956</date></bday>
                   <gender><sex>M</sex></gender>
                   <lang>
                       <parameters><pref><integer>1</integer></pref>
                       </parameters>
                       <language-tag>en</language-tag>
                   </lang>
                   <adr>
                       <parameters>
                           <type><text>home</text></type>
                           <label><text>James Winterbottom
                               123 Main street
                               Gwynneville, QNSW, Australia
                               2500</text></label>
                       </parameters>
                       <pobox/>
                       <ext/>
                       <street>123 Main street</street>
                       <locality>Gwynneville</locality>
                       <region>NSW</region>
                       <code>2500</code>
                       <country>Australia</country>
                   </adr>
                   <tel>
                       <parameters>
                           <type>
                               <text>home</text>
                               <text>voice</text>
                           </type>
                       </parameters>
                       <uri>tel:+61-123-456-7890</uri>
                   </tel>
                   <email>
                       <parameters>
                          <type><text>work</text></type>
                       </parameters>
                       <text>jw@eena.org</text>
                   </email>
                   <related>
                      <parameters>
                                 <type><text>emergency</text></type>
                        </parameters>
```

```
                        <uri>tel:+61-2-42-263755</uri>
                    </related>
                </vcard>
            </vcards>
        </sub:SubscriberData>
    </sub:emergencyCallData.SubscriberInfo>
```

The DeviceInfo container is defined in the IETF additional-data specification. This container is extended with cellular measurement element from the IETF geopriv measurement specification RFC7105, and the IMSI and IMEI elements from the IETF geopriv identity extensions draft RFC6155. Table 9 provides the fields and suggested values:

Table 9 Device Information

Field	Desc.	Recommended Value
id	Common identifier linking all blocks provided by the same entity.	This should be the same as the value used in the id element of the SubscriberData block.
DeviceClassification	The type of device making the call. This is a smart phone.	smrtPhn
DeviceMfgr	Device Manufactuer. Should be provided if available, may be omitted if not available	Apple
DeviceModelNr	Device Model Number. Should be provided if available, may be omitted if not available	iPhone4s
<cellular xlmns="urn:ietf:params:xml:ns:geopriv:lm:cell"> <servingCell>	Defines the serving cell to which the smartphone is attached. This must be provided.	<mcc>???</mcc><mnc>***</mnc><cid>$$$$$$$$$$$$</cid>
<imsi xmlns:ietf:params:xml:geopriv:held:id">	The IMSI of the calling device. This must be provided.	01234598421
<imei xmlns:ietf:params:xml:geopriv:held:id">	The IMEI of the calling device. This must be provided.	5976832175

DeviceInfo example:

```
<dev:emergencyCallData.DeviceInfo
        xmlns:dev="urn:ietf:params:xml:ns:emergencycalldata:DeviceInfo"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <dev:id>12345</dev:id>
   <dev:DeviceClassification>SmrtPhn</dev:DeviceClassification>
   <dev:DeviceMfgr>Nokia</dev:DeviceMfgr>
   <dev:DeviceModelNr>Lumia 1520</dev:DeviceModelNr>
      <cellular xlmns="urn:ietf:params:xml:ns:geopriv:lm:cell">
         <servingCell>
            <mcc>206</mcc><mnc>20</mnc><cid>55555</cid>
         </servingCell>
      </cellular>
      <device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
         <imsi>11235550123</imsi>
         <imei>77723390012356</imei>
      </device>
</dev:emergencyCallData.DeviceInfo>
```