Paper number ITS-XXXX

Requirements for Next generation 112 eCall

Harold Linke[1*], Kate Yeadon[2], Uberto Delprato[3], Christina Lumbreras[4], Bob Williams[5]

1. HITEC Luxembourg S.A., 5, rue de l'Eglise, L-1458 Luxembourg, Luxembourg, harold.linke@hitec.lu
2. Post Luxembourg, Luxembourg
3. IES Solutions, Italy
4. EENA, Belgium
5. CSI, UK

Abstract

The European Standard eCall that will be mandatory in 2018 is designed to use standard GSM voice channels. This approach provides a very good coverage over Europe but limits the information that can be provided to the 112 centre. Future networks e.g. LTE and 5G onwards are based on IP technology only and no circuit switched emergency calls will be available anymore. Next Generation 112 centres (NG112) leveraging the new technologies are under discussion and new features will be integrated into the new Next Generation 112 centres. In any event, a migration strategy is needed to move from current circuit switched networks to packet switched networks at some point in time.

This paper describes the background and the requirements for a European eCall that supports Next Generation 112 centres using IP technology.

Keywords: eCall, NG112

What is Next Generation 112 (NG112)?

In their paper "Next Generation 112 Long Term Definition" EENA defines Next generation 112.

It is estimated that 320 million emergency calls are made every year in the European Union, enabling emergency services to assist citizens in all sorts of difficult situations. For the time being however, most European emergency services can only be reached through the public switched telephony or mobile networks.

Voice over Internet Protocol (VoIP) based devices and applications have become commonplace. Citizens use them to conveniently communicate, send and receive information. Text messaging is an ever more common communication means, replacing the traditional two-way voice telephone call. Pictures and videos from phones and PDAs are shared instantly with friends and colleagues around the world, and social networks have become a media by themselves. Video and text based communications are replacing traditional systems such as teletypes for the deaf and hard of hearing. Cars are being fitted with telematics systems that automatically initiate a voice call and provide valuable data when a car is involved in an accident (eCall). Geographical location based services are increasingly used to submit or lookup close points of interest or friend's current position. Modern mobile phones from which an emergency call might be placed have the potential to transmit lifesaving location information with the call. Enterprise workers expect to be able to place an emergency call from a campus or remote building complex environment and have a first line response dispatched to the specific location, be that a building within a campus or a floor in a building or an office on a floor.

All over the world, citizens expect to be able to contact emergency services with technologies they use to communicate every day. Thus, European citizens have clear expectations about the availability of 112 emergency services with enhanced capabilities of technologies being used in daily life.

However, the existing, legacy emergency services infrastructure (circuit switched telephony for 112 telephone calls, not data) is not designed in a way that enables interaction with enhanced services, or that current and future communications and operational requirements will be met. Simply put, the emergency services infrastructure has not kept up with technology, thus, is not able to provide the level of service that citizens may expect.

Hence, a new technology with a new architecture is needed to resolve these issues – the "Next Generation 112 architecture (NG112)". NG112 will enable citizens to contact emergency services in different ways, using modern digital technology. It also makes possible that 112 PSAPs could receive more and better information about emergencies of all magnitudes and improves interoperability between emergency services. Consequently, response time and operation cost will be reduced, while effective response will increase significantly.

NG112 addresses three major objectives:

1. Communication between citizens and emergency services: NG112 is designed to enable citizens to reach an authority (public service answering point [PSAP]) by calls using digital, packet-switched, technology, thus enabling VoIP, text messaging, real-time text, pictures and video. Where allowed by, and within, regulations, it could also provide emergency services

with more data, such as videophone, provision of scene of crash video to the PSAP, etc. and where permitted by regulations, health data such as Bluetooth connection to smartwatches in or close to the vehicle, personal health condition data etc. NG112 will enable the delivery of calls, messages and data to the appropriate PSAP, and enable easier routing of information from the first level responder to the responding emergency service personnel supporting the on-site response, and adds significant value to the call handling process.

2. Interoperability between emergency services: NG112 enables several Public Safety Answering Points (PSAPs) to be part of a common emergency services IP network, providing them with redundancy and interoperability features. This network should support data and communications needs for coordinated incident management between PSAPs, and provide a reliable and secure environment for emergency communications.
3. Open Standards approach: NG112 is based on Internet Protocol (IP)-network based standard interfaces between all forms of communications components. For instance ECRIT and Geopriv working groups in the IETF NG112 have already defined standards applicable to Next Generation 112. Hence, existing off-the-shelf hardware and software can be deployed, which increases the technical commonalities between EU member states, drives TCO and fosters the European public safety eco-system. Existing experience from other regions, namely NENA in the US, with its significant work on the NG911 architecture definition and couple with pilot and certification experience, is carefully examined in the NG112 approach and where necessary, adapted to European needs.

What is Pan European - eCall

Pan European eCall is an initiative with the purpose to bring rapid assistance to motorists involved in a collision anywhere in the European Union.

Emergency (112) calls are routed by the mobile network operator to the most appropriate PSAP - which is dependent on the origin of the emergency call, and nature of the call. This origin is a geographical area which is identified by the official municipal identifier for emergency calls.

In case of a crash, an eCall-equipped car automatically calls the network service provider who routes the call to the most appropriate public service answering point. Even if no passenger is able to speak, e.g. due to injuries, a 'Minimum Set of Data' (MSD) is sent, which includes the exact location of the crash site, direction of travel, vehicle description etc.. Shortly after the accident, emergency services therefore know that there has been an accident, and where exactly. This significantly cuts emergency services response time.

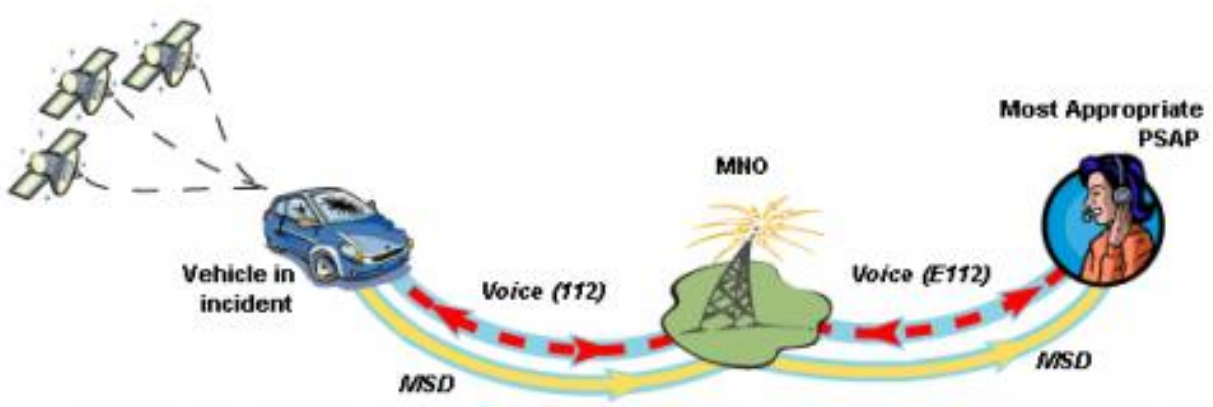

Figure 1 –European eCall Architecture

An eCall can also be manually activated by pushing a button inside the car. In normal working mode the eCall system 'sleeps': as such it does not facilitate any form of vehicle tracking and tracing.
The objective is to have this system seamlessly functioning throughout Europe by 2018, with the coordination of Member States, car manufacturers, telecom operators and emergency centres. EU legislation enforces eCall being fully functional across Europe in 2018 for all new models of personal cars (categories M1 and N1). An active aftermarket for existing vehicles is also expected.

NG112 eCall

The Pan European eCall's technology is based on circuit switched emergency call and an in-band modem which was developed for GSM (2G) and UMTS (3G) networks (because these are already deployed and pervasive across Europe). Future mobile networks e.g. LTE and 5G onwards are based on packet-switched IP technology only and, at some time in the future, it can be expected that circuit switched emergency calls will cease to be available. ISDN is not supported for new connections in many European countries anymore, and here operators are already obliged to provide emergency services in IP networks. In many countries, this is already regulated by the government or it is on the way to be regulated. The new data transmission methods require revising specifications in many ways and many levels of network communication. This affects signaling, voice and data transmission. This change will affect eCall.
Vehicles have a lifespan of more than 15 years, and even if circuit switch emergency calls may be supported in mobile networks for a long time, due to legacy handsets and regulatory needs, a next generation technology for eCall needs to be considered.
ETSI published a Technical report "TR 103 140 V1.1.1" with the conclusions of the investigation made by the specialist task force STF 456 about the migration of eCall transport over IP Multimedia Subsystem (IMS). The IP Multimedia Subsystem (IMS) architecture specified by the 3GPP (release 6) is the platform of choice for operators to offer unified communication for both fixed and mobile networks.

The transfer will also influence the work flow within the PSAP. Today, the data transmission takes place as an inband communication prior to the voice communication between call taker and occupants in the vehicle. When based on VoIP, the transfer of data will happen in parallel to the ongoing voice communication and with potential to provide more detailed information than is possible today (because it will not have the length limitations of the current MSD which is sent as data in a voice channel).
NG112 eCall is expected to offer to carry more data (e.g., an enhanced Minimum Set of Data MSD or an MSD plus additional sets of data), to handle video and text, and to provide the ability for the PSAP to access vehicle components (e.g., an on-board camera (such as rear facing or blind-spot cameras) for a visual assessment of the crash site situation) and to request the vehicle to take actions (e.g., sound the horn, disable the ignition, lock/unlock doors).

Requirements for NG112 eCall

General requirements

Overall eCall requirements are specified by CEN in [EN_16072/EN_16062] and by 3GPP in [TS22.101] clauses 10.7 and A.27. Requirements specific to vehicle data are contained in EN 15722 [msd].

eCall in general has following requirements:

- The call needs to be recognized as an eCall (which is inherently an emergency call)
- The call setup indicates if the call was manually or automatically triggered
- A voice channel between the vehicle and the PSAP is setup
- The minimum set of data (MSD) is intrinsically transferred with the call (the MSD needs to be available to the same call-taker as the voice).
- The PSAP needs to have the ability to acknowledge receipt of the MSD
- The PSAP needs to have the ability to request that the vehicle generates and transmits a new MSD
- The PSAP needs to have the ability to re-contact the occupants of vehicle after the initial eCall is concluded
- The ability is needed to perform a test call (which can be routed to a PSAP but is not treated as an emergency call and not handled by a call taker)

As explained above NG-eCall offers many potential enhancements, although these are not required by current EU regulations. These enhancements can be:

- Faster and more reliable MSD transfer, no loss of speech path, significantly more than the current 140 bytes would be possible (e.g. later) in the MSD (e.g., an enhanced MSD or an MSD plus additional sets of data)

- Additional media could be used (e.g. video from dashboard cameras, text from speech or hearing impaired users).
- The ability for the PSAP to access vehicle components (e.g., an onboard camera (such as rear facing or blind-spot cameras) for a visual assessment of the crash site situation)
- The ability for the PSAP to request the vehicle to take actions (e.g., sound the horn, disable the ignition, lock/unlock doors)
- No audio muting of the voice channel is necessary anymore when the PSAP accesses the MSD – faster voice connection to the people in the vehicle

Emergency Services IP Network - *ESInet*

For the handling of NG112 emergency calls a concept called Emergency Services IP Network (ESInet) is proposed by ESTI and EENA.

An Emergency Services IP Network (ESInet) is a network operated by emergency services authorities. It handles emergency call routing and processing before delivery to a PSAP. In the NG112 architecture adopted by EENA, each PSAP is connected to one or more ESInets. Each originating network is also connected to one or more ESInets. The ESInets maintain policy-based routing rules which control the routing and processing of emergency calls. The centralization of such rules within ESInets provides for a cleaner separation between the responsibilities of the originating network and that of the emergency services network, and provides greater flexibility and control over processing of emergency calls by the emergency services authorities. This makes it easier to react quickly to unusual situations that require changes in how emergency calls are routed or handled (e.g., a natural disaster closes a PSAP), as well as ease in making long-term changes that affect such routing (e.g., cooperative agreements to specially handle calls requiring translation or relay services). ESInets might support the ability to interwork NG-eCall to legacy eCall to handle eCall-capable PSAPs that are not IP PSAPs (similarly to the ability to interwork IP emergency calls to legacy non-IP PSAPs).

Migration requirements

The EENA document "Next Generation eCall" defines the Migration requirements:

Cars last typically 15 or more years, compared to 2-3 years for mobile phones. Cars being deployed with in-band modem eCall, based on circuit-switched 112, will need circuit switched 112 support from the network until the 2030s. This may be longer than the mobile operators desire.

As IMS emergency call capability will be extensively deployed well before the 2030s, in-band modem eCall and IMS eCall will have to co-exist. ETSI TR 103 140 considered this co-existence and how migration from eCall to IMS eCall can be managed.

- Introduction of IMS eCall into IVSs can occur when standards are available. Such IVSs will also have to be capable of in-band modem eCall for many years.

- From a certain date PSAPs shall support IMS eCall but shall be able to receive and process in-band modem eCalls as well.

- An IVS capable of IMS eCall shall only use IMS eCall if informed (by a system information indicator) that IMS eCall is supported in the network.

- The mobile operator will only switch on the system information indicator when there is IMS eCall coverage and at least one routable PSAP capable of receiving IMS eCalls.

Security Considerations

In addition to any network-provided location that is inherently permitted for IMS emergency calls (which might be determined solely by the network, or in cooperation with or possibly entirely by the originating device), an eCall carries an IVS-supplied location within the MSD. This is likely to be useful to the PSAP, especially when the two locations are independently determined. Even in situations where the network-supplied location is limited to the cell site, this can be useful as a sanity check on the device-supplied location contained in the MSD.

Security considerations specific to the mechanism by which the PSAP sends acknowledgments and requests to the vehicle are discussed in the "Security Considerations" block of Section 14.3. In addition to that discussion, it's important to note that vehicles MAY decline to carry out any requested action, e.g., if the vehicle is unable to verify the certificate used to sign the request. The vehicle MAY use any value in the reason registry in Section 14.8.3 to indicate why it did not take an action (e.g., the generic "unable" or the more specific "security-failure").

Data received from external sources inherently carries implementation risks including buffer overflows, which in many platforms can introduce remote code execution vulnerabilities; null characters can corrupt strings, numeric values used for internal calculations can result in underflow/overflow errors; malformed XML objects can expose parsing bugs, etc. Implementations need to be cognizant of the potential risks, observe best practices (e.g., good quality static code analysis, fuzz testing, component isolation, avoiding use of unsafe coding techniques, third-party attack tests, signed software, over-the-air updates, etc.), and have multiple levels of protection. Implementers need to be aware that, potentially, the data objects described here and elsewhere might be malformed, might contain unexpected characters, excessively long attribute values, elements, etc. (This applies across the board, not just to the 'text' attribute of a <request> element.)

Privacy Considerations

Since this document builds on [I-D.ietf-ecrit-additional-data], the data structures specified there, and the corresponding privacy considerations discussed there, apply here as well. The MSD carries some additional identifying and personal information (mostly about the vehicle and less about the owner), as well as location information, and so needs to be protected against unauthorized disclosure. Local regulations may impose additional privacy protection requirements. The additional functionality enabled by this document, such as access to vehicle camera streams, carries a burden of protection and so implementations need to be careful that access is only provided within the context of an emergency call and to an emergency services provider, for example, by verifying that the request for camera access is signed by a certificate issued by an emergency services registrar.

The data structure containing vehicle information is designed to carry vehicle and incident-related data during an emergency call. This data contains information including vehicle VIN, location, direction, etc. Appropriate precautions need to be taken to limit unauthorized access, inappropriate disclosure to third parties, and eavesdropping of this information. In general, it is permissible for the data to be unprotected while briefly in transit within the Mobile Network Operator (MNO); the MNO is trusted to not permit the data to be accessed by third parties.

Privacy considerations specific to the mechanism by which the PSAP sends acknowledgments and requests to the vehicle are discussed in the "Security Considerations" block of Section 14.3.

This content type carries metadata and control information and requests, primarily from a Public Safety Answering Point (PSAP) to an In-Vehicle System (IVS) during an emergency call, and also capabilities from the IVS to the PSAP.

Metadata (such as an acknowledgment that data sent by the IVS to the PSAP was successfully received) has limited privacy and security implications. Control information (such as requests from the PSAP that the vehicle perform an action) has some privacy and important security implications. The privacy concern arises from the ability to request the vehicle to retransmit the MSD, which contains vehicle specific and location information. The security concern is the ability to request the vehicle to perform an action. It is important that control information originate only from a PSAP or other emergency services provider, and not be modified en-route. The level of integrity of the cellular network over which the emergency call is placed is important: when the IVS initiates an eCall over a cellular network, it relies on the MNO to route the call to a PSAP. (Calls placed using other means, such as Wi-Fi or over-the-top services, generally incur higher levels of risk than calls placed over cellular networks.) A call-back from a PSAP incurs additional risk, since the current mechanisms are not ideal for verifying that such a call is indeed a call-back from a PSAP in response to an emergency call placed by the IVS. One safeguard, applicable regardless of which end initiated the call and the means of the call, is for the PSAP or emergency service provider to sign the body part using a certificate issued by a known emergency services certificate authority and for which the IVS

can verify the root certificate.

Next steps for definition of NG112 ecall

The NG112 eCall activity of the EU project I-HeERO is working together with EENA, CEN and ETSI representatives to define NG112 eCall. The activity focuses on the migration of eCall to NG112 (Next Generation 112). A relevant strategy for the migration of the PSAP will allow effective management thus ensuring that eCall remains effective. I_HeERO possess the necessary MS involvement and of course PSAP and MNO infrastructure to trial any future developments. In addittion the CEN 278 WG15 (in charge of eCall) will be available to work directly with the entire project to ensure that any amendments that are identified are processed in the most effective way.

References

1. ETSI TR 103 140 V1.1.1 (2014-04), eCall for VoIP
   http://www.etsi.org/deliver/etsi_tr/103100_103199/103140/01.01.01_60/tr_103140v010101p.pdf
2. IETF Next-Generation Pan-European eCall
   https://tools.ietf.org/html/draft-ietf-ecrit-ecall-03
3. CEN EN 15722 eCall Minimum Set of Data
   http://shop.bsigroup.com/ProductDetail/?pid=000000000030301210
4. CEN EN 16062 eCall High Level Application Protocol
   http://shop.bsigroup.com/ProductDetail/?pid=000000000030301213
5. CEN EN 16072 eCall Pan European Operating Requirements
   http://shop.bsigroup.com/ProductDetail/?pid=000000000030301207
6. Williams D., Lumbreras C. (2015) *Next generation eCall*, EENA Technical Committee Document
7. Grososiu A., Lumbreras C., et al. (2012), *Next Generation 112 - Long Term Definition*, EENA Technical Committee Document