ECRIT
Internet-Draft
Intended status: Informational
Expires: September 8, 2015

R. Gellens
Qualcomm Technologies, Inc
B. Rosen
NeuStar, Inc.
H. Tschofenig
(no affiliation)
March 7, 2015

Next-Generation Vehicle-Initiated Emergency Calls
draft-ietf-ecrit-car-crash-02.txt

Abstract

This document describes how to use IP-based emergency services mechanisms to support the next generation of emergency calls placed by vehicles (automatically in the event of a crash or serious incident, or manually invoked by a vehicle occupant) and conveying vehicle, sensor, and location data related to the crash or incident. Such calls are often referred to as "Automatic Crash Notification" (ACN), or "Advanced Automatic Crash Notification" (AACN), even in the case of manual trigger. The "Advanced" qualifier refers to the ability to carry a richer set of data.

This document also registers a MIME Content Type and an Emergency Call Additional Data Block for the vehicle, sensor, and location data (often referred to as "crash data" even though there is not necessarily a crash). An external specification for the data format, contents, and structure are referenced in this document.

Profiling and simplifications of the general emergency call mechanism, as described in [RFC6443] and [RFC6881], are possible due to the nature of the functionality that is provided in vehicles such as the usage of Global Satellite Navigation System (GNSS).

This document reuses the technical aspects of next-generation pan-European eCall (a mandated and standardized system for emergency calls by in-vehicle systems within Europe and other regions), as described in [I-D.ietf-ecrit-ecall]. However, this document specifies a different set of vehicle (crash) data, specifically, the Vehicle Emergency Data Set (VEDS) rather than the eCall Minimum Set of Data (MSD).

Status of This Memo

Copyright Notice

Table of Contents

1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

This document re-uses terminology defined in Section 3 of [RFC5012].

Additionally, we use the following abbreviations:

Term	Expansion
3GPP	3rd Generation Partnership Project
AACN	Advanced Automatic Crash Notification
ACN	Automatic Crash Notification
APCO	Association of Public-Safety Communications Officials
EENA	European Emergency Number Association
ESInet	Emergency Services IP network
GNSS	Global Satellite Navigation System (which includes the various such systems including the Global Positioning System or GPS)
IVS	In-Vehicle System
MNO	Mobile Network Operator
NENA	National Emergency Number Association
TSP	Telematics Service Provider
VEDS	Vehicle Emergency Data Set

2. Introduction

Emergency calls made by in-vehicle systems (e.g., in the event of a crash) assist in significantly reducing road deaths and injuries by allowing emergency services to respond quickly and often with better location.

Drivers often have a poor location awareness, especially outside of major cities, at night and when away from home (especially abroad).

In the most crucial cases, the victim(s) may not be able to call because they have been injured or trapped.

For more than a decade, some vehicles have been equipped with telematics systems that, among other features, place an emergency call automatically in the event of a crash or manually in response to an emergency call button. Such systems generally have on-board location determination systems that make use of satellite-based positioning technology, inertial sensors, gyroscopes, etc., to provide a fairly accurate position for the vehicle. Such built-in systems can take advantage of the benefits of being integrated into a vehicle, such as more reliable power, ability to have larger or specialized antenna, ability to be engineered to avoid or minimise degradation by vehicle glass coatings, interference from other vehicle systems, etc. Thus, the PSAP can be provided with a good estimate of where the vehicle is during an emergency. Vehicle manufacturers are increasingly adopting such systems, both for the safety benefits and for the additional features and services they enable (e.g., remote engine diagnostics, remote door unlock, stolen vehicle tracking and disabling, etc.).

The general term for such systems is Automatic Crash Notification (ACN) or "Advanced Automatic Crash Notification" (AACN). "ACN" is used in this document as a general term. ACN systems transmit some amount of data specific to the incident, referred to generally as "crash data" (the term is commonly used even though there might not have been a crash). While different systems transmit different amounts of crash data, standardized formats, structures, and mechanisms are needed to provide interoperability among systems and PSAPs.

Currently deployed in-vehicle telematics systems are circuit-switched and lack a standards-based ability to convey crash data directly to the PSAP (generally relying on either a human call taker or an automated system to provide the PSAP call taker with some crash data orally, or possibly a proprietary mechanism). The PSAP call taker needs to first realize that the call is related to a vehicle incident, and in most cases must then listen to the data and transcribe it.

The transition to next-generation calling in general, and emergency calling in particular, provides an opportunity to vastly improve the scope, breadth, reliability and usefulness of crash data during an emergency by allowing it to be presented alongside the call, and to be automatically processed by the PSAP and made available to the call taker in an integrated, automated way. In addition, vehicle manufacturers are provided an opportunity to take advantage of the same standardized mechanisms for data transmission for internal use

if they wish (such as telemetry between the vehicle and a service center for both emergency and non-emergency uses, including location-based services, multi-media entertainment systems, and road-side assistance applications).

Next-generation ACN provides an opportunity for such calls to be recognized and processed as such during call set-up, and optionally routed to an upgraded PSAP where the vehicle data is available to assist the call taker in assessing and responding to the situation.

An ACN call may be either occupant-initiated or automatically triggered. (The "A" in "ACN" does stand for "Automatic," but the term is often used to refer to the class of calls that are placed by an in-vehicle system (IVS) and that carry incident-related data as well as voice.) Automatically triggered calls indicate a car crash or some other serious incident (e.g., a fire) and carry a greater presumption of risk of injury. Manually triggered calls are often reports of serious hazards (such as drunk drivers) and may require different responses depending on the situation. Manually triggered calls are also more likely to be false (e.g., accidental) calls and may thus be subject to different handling by the PSAP.

This document describes how the IETF mechanisms for IP-based emergency calls, including [RFC6443] and [I-D.ietf-ecrit-additional-data], are used to provide the realization of next-generation ACN.

The Association of Public-Safety Communications Officials (APCO) and the National Emergency Number Association (NENA) have jointly developed a standardized set of incident-related vehicle data for ACN use, called the Vehicle Emergency Data Set (VEDS) [VEDS]. Such data is often referred to as crash data although it is applicable in incidents other than crashes.

VEDS provides a standard data set for the transmission, exchange, and interpretation of vehicle-related data. A standard data format allows the data to be generated by an IVS, and interpreted by PSAPs, emergency responders, and medical facilities (including those capable of providing trauma level patient care). It includes incident-related information such as airbag deployment, location of the vehicle, if the vehicle was involved in a rollover, various sensor data that can indicate the potential severity of the crash and the likelihood of severe injuries to the vehicle occupants, etc. This data better informs the PSAP and emergency responders as to the type of response that may be needed. This information was recently included in the federal guidelines for field triage of injured patients. These guidelines are designed to help responders at the accident scene identify the potential existence of severe internal

injuries and to make critical decisions about how and where a patient needs to be transported.

This document registers the 'application/EmergencyCallData.VEDS+xml' MIME content-type, and registers the 'VEDS' entry in the Emergency Call Additional Data registry.

VEDS is an XML structure (see [VEDS]). The 'application/ EmergencyCallData.VEDS+xml' MIME content-type is used to identify it. The 'VEDS' entry in the Emergency Call Additional Data registry is used to construct a 'purpose' parameter value for conveying VEDS data in a Call-Info header (as described in [I-D.ietf-ecrit-additional-data]).

VEDS is a versatile structure that can accomodate varied needs. However, if additional sets of data are determined to be needed (e.g., in the future or in different regions), the steps to enable each data block are very briefly summarized below:

- o A standardized format and encoding (such as XML) is defined and published by a Standards Development Organization (SDO).

- o A MIME Content-Type is registered for it (typically under the 'Application' media type and with a sub-type starting with 'EmergencyCallData.').

- o An entry for the block is added to the Emergency Call Additional Data Blocks sub-registry (established by [I-D.ietf-ecrit-additional-data]); the registry entry is the root of the MIME sub-type (not including the 'EmergencyCallData' prefix and any suffix such as '+xml').

A next-generation In-Vehicle System (IVS) transmits crash data by encoding it in a standardized and registered format (such as VEDS) and attaching it to an INVITE as a MIME body part. The body part is identified by its MIME content-type (such as 'application/ EmergencyCallData.VEDS+xml') in the Content-Type header field of the body part. The body part is assigned a unique identifier which is listed in a Content-ID header field in the body part. The INVITE is marked as containing the crash data by adding a Call-Info header field at the top level of the INVITE. This Call-Info header field contains a CID URL referencing the body part's unique identifier, and a 'purpose' parameter identifying the data as the crash data per the registry entry; the 'purpose' parameter's value is 'EmergencyCallData.' and the root of the MIME type (not including the 'EmergencyCallData' prefix and any suffix such as '+xml' (e.g., 'purpose=EmergencyCallData.VEDS').

The mechanisms described here are thus used to place emergency calls that are identifiable as ACN calls and that carry one or more standardized crash data objects in an interoperable way.

3. Overview of Current Deployment Models

Current (circuit-switched or legacy) systems for placing emergency calls by in-vehicle systems, including automatic crash notification systems, generally have a limited ability to convey at least location and in some cases telematics data to the PSAP. Most such systems use one of three architectural models, which are described here as: "Telematics Service Provider" (TSP), "direct", and "paired handset". These three models are illustrated below.

In the TSP model, both emergency and non-emergency calls are placed to a Telematics Service Provider (TSP); a proprietary technique is used for data transfer (such as proprietary in-band modems) to the TSP.

In an emergency, the TSP call taker bridges in the PSAP and communicates location, crash data (such as impact severity and trauma prediction), and other data (such as the vehicle description) to the PSAP call taker verbally. Typically, a three-way voice call is established between the vehicle, the TSP, and the PSAP, allowing communication between the PSAP call taker, the TSP call taker, and the vehicle occupants (who might be unconscious).

```
   ///----\\\  proprietary  +------+    911 trunk      +------+
  ||| IVS |||-------------->+ TSP  +------------------>+ PSAP |
   \\\----///  crash data   +------+                   +------+
```

Figure 1: Legacy TSP Model.

In the paired model, the IVS uses a Bluetooth link with a previously-paired handset to establish an emergency call with the PSAP (by dialing a standard emergency number such as 9-1-1), and then communicates location data to the PSAP via text-to-speech; crash data is not conveyed. Some such systems use an automated voice prompt menu (e.g., "this is an automatic emergency call from a vehicle; press 1 to open a voice path to the vehicle; press 2 to hear the location read out") to allow the call taker to request location data via text-to-speech.

```
                  +---+
     ///----\\\   | H |   911/etc voice call via handset   +------+
    ||| IVS |||-->| S +------------------------------------>+ PSAP |
     \\\----///   +---+   location via text-to-speech      +------+
```

Figure 2: Legacy Paired Model

In the direct model, the IVS directly places an emergency call with the PSAP by dialing a standard emergency number such as 9-1-1. Such systems might communicate location data to the PSAP via text-to-speech; crash data might not be conveyed.

```
     ///----\\\      911/etc voice call via IVS          +------+
    ||| IVS  |||---------------------------------------->+ PSAP |
     \\\----///     location via text-to-speech          +------+
```

Figure 3: Legacy Direct Model

4. Document Scope

This document is focused on the interface to the PSAP, that is, how an ACN emergency call is setup and incident-related data (including vehicle, sensor, and location data) is transmitted to the PSAP using IETF specifications. (The goal is to re-use specifications rather than to invent new.) For the direct model, this is the end-to-end description (between the vehicle and the PSAP). For the TSP model, this describes the right-hand side (between the TSP and the PSAP), leaving the left-hand side (between the vehicle and the TSP) up to the entities involved (i.e., IVS and TSP vendors) who are then free to use the same mechanism as for the right-hand side (or not).

Note that while ACN systems in the U.S. and other regions are not currently mandated, Europe has a mandated and standardized system for emergency calls by in-vehicle systems. This pan-European system is known as "eCall" and is the subject of a separate document, [I-D.ietf-ecrit-ecall]. Vehicles designed to operate in multiple regions may need to support eCall as well as the ACN described here. If other regions devise their own specifications or data formats, a multi-region vehicle may need to support those as well. This document adopts the call set-up and other technical aspects of [I-D.ietf-ecrit-ecall], which uses [I-D.ietf-ecrit-additional-data], which makes it easy to substitute a different data set while keeping other technical aspects unchanges. Hence, both NG-eCall and the ACN mechanism described here are fully compatible, differing only in the specific data block that is sent (the eCall MSD in the case of NG-eCall, and the APCO/NENA VEDS used in this document). If other

regions adopt their own data set, this can be similarly accomodated without changing other technical aspects.

5. Migration to Next-Generation

Migration of emergency calls placed by in-vehicle systems to next-generation (all-IP) technology provides a standardized mechanism to identify such calls and to present crash data with the call. This allows ACN calls and crash data to be automatically processed by the PSAP and made available to the call taker in an integrated, automated way. Because the crash data is carried in the initial SIP INVITE (per [I-D.ietf-ecrit-additional-data]) the PSAP can present it to the call taker simultaneously with the appearance of the call.

Vehicle manufacturers using the TSP model may choose to take advantage of the same mechanism to carry telematics data between the vehicle and the TSP for both emergency and non-emergency calls.

A next-generation IVS establishes an emergency call using the emergency call solution as described in [RFC6443] and [RFC6881], with the difference that the Request-URI indicates an ACN type of emergency call and a Call-Info header field indicates that vehicle crash data is attached. When an ESInet is deployed the MNO only needs to recognize the call as an emergency call and route it to an ESInet. The ESInet may recognize the call as an ACN with vehicle data and may route the call to an NG-ACN capable PSAP. Such a PSAP would interpet the vehicle data sent with the call and make it available to the call taker.

Because of the need to identify and specially process Next-Generation ACN calls (as discussed above), [I-D.ietf-ecrit-ecall] registers new service URN children within the "sos" subservice. These URNs provide a mechanism by which an NG-ACN call is identified, and differentiate between manually and automatically triggered NG-ACN calls, which can be subject to different treatment, depending on policy. (The two service URNs registered in [I-D.ietf-ecrit-ecall] are: urn:service:sos.ecall.automatic and urn:service:sos.ecall.manual.)

Note that in North America, routing queries performed by clients outside of an ESInet are likely to treat all sub-services of "sos" identically to "sos" with no sub-service. However, the Request-URI header field retains the full sub-service; route and handling decisions within an ESInet or PSAP may take the sub-service into account. For example, in a region with multiple cooperating PSAPs, an NG-ACN call might be routed to a PSAP that is NG-ACN capable, or one that specializes in vehicle-related incidents.

Migration of the three architectural models to next-generation (all-IP) is described below.

In the TSP model, the IVS transmits crash and location data to the TSP using either a protocol that is based on a proprietary design or one that re-uses IETF specifications. In an emergency, the TSP call taker bridges in the PSAP and the TSP transmits crash and other data to the PSAP using IETF specifications. There is a three-way call between the vehicle, the TSP, and the PSAP, allowing communication between the PSAP call taker, the TSP call taker, and the vehicle occupants (who might be unconscious).

```
                proprietary
   ///----\\\  or standard       +------+     standard       +------+
  ||| IVS ||| -------------------->+ TSP +-------------------->+ PSAP |
   \\\----/// crash + other data +------+ crash + other data +------+
```

Figure 4: Next-Generation TSP Model

The vehicle manufacturer and the TSP may choose to use the same IETF specifications to transmit crash and location data from the vehicle to the TSP as is described here to transmit such data from the TSP to the PSAP.

In the paired model, the IVS uses a Bluetooth link to a previously-paired handset to establish an emergency call with the PSAP; it is not clear what facilities are or will be available for transmitting crash data through the Bluetooth link to the handset for inclusion in an NG emergency call.

```
                                +---+
   ///----\\\     (unclear)     | H |      (unclear)     +------+
  ||| IVS |||------------------>| S +-------------------->+ PSAP |
   \\\----///     (unclear)     +---+      (unclear)     +------+
```

Figure 5: Next-Generation Paired Model

In the direct model, the IVS communicates crash data to the PSAP directly using IETF specifications.

```
  ///----\\\           NG emergency call              +------+
 ||| IVS |||----------------------------------------->+ PSAP |
  \\\----///          crash + other data              +------+
```

Figure 6: Next-Generation Model

If the call is routed to a PSAP that is not capable of processing the vehicle data, the PSAP ignores (or does not receive) the vehicle

data. This is detectable by the IVS or TSP when it receives a 200 OK to the INVITE that lacks an eCall control structure acknowledging receipt of the data [I-D.ietf-ecrit-ecall]. The IVS or TSP then proceeds as it would for a non-NG ACN call (e.g., verbal conveyance of data)

6. Profile

In the context of emergncy calls placed by an in-vehicle system it is assumed that the car is equipped with a built-in GNSS receiver. For this reason only geodetic location information will be sent within an emergency call. The following location shapes MUST be implemented: 2d and 3d Point (see Section 5.2.1 of [RFC5491]), Circle (see Section 5.2.3 of [RFC5491]), and Ellipsoid (see Section 5.2.7 of [RFC5491]). The coordinate reference systems (CRS) specified in [RFC5491] are also mandatory for this document. The <direction> element, as defined in [RFC5962] which indicates the direction of travel of the vehicle, is important for dispatch and hence it MUST be included in the PIDF-LO [RFC4119]. The <heading> element specified in [RFC5962] MUST be implemented and MAY be included.

Calls by in-vehicle systems are placed via cellular networks, which may ignore location sent by an originating device in an emergency call INVITE, instead attaching their own location (often determined in cooperation with the originating device). Standardized crash data structures often include location as determined by the IVS. A benefit of this is that it allows the PSAP to see both the location as determined by the cellular network (often in cooperation with the originating device) and the location as determined by the IVS.

This specification inherits the ability to utilize test call functionality from Section 15 of [RFC6881].

7. Call Setup

It is important that ACN calls be easily identifiable as such at all stages of call handling, and that automatic versus manual triggering be known. ACN calls differ from general emergency calls in several aspects, including the presence of standardized crash data, the fact that the call is known to be placed by an in-vehicle system (which has implications for PSAP operational processes), and, especially for automatic calls, information that may indicate a likelihood of severe injury and hence need for trauma services. Knowledge that a call is an ACN and further that it was automatically or manually invoked carries a range of implications about the call, the circumstances, and the vehicle occupants. Calls by in-vehicle systems may be considered a specific sub-class of general emergency calls and are optimally handled by a PSAP with the technical and operational

capabilities to serve such calls. (This is especially so in environments such as the U.S. where there are many PSAPs and where individual PSAPs have a range of capabilities.) Technical capabilities include the ability to recognize and process standardized crash data. Operational capabilities include training and processes for assessing severe injury likelihood and responding appropriately (e.g., dispatching trauma-capable medical responders or those trained and equipped to extract occupants from crashed vehicles and handle gasoline or other hazardous materials, transporting victims to a trauma center, alerting the receiving facility, etc.).

Because ACN calls differ in significant ways from general emergency calls, and because such calls should be handled by specialized PSAPs (equipped technically to interpet and make use of crash data, and operationally to handle emergency calls placed by in-vehicle systems), [I-D.ietf-ecrit-ecall] registers SOS sub-services. Using a sub-service makes it readily obvious that the call is an ACN; a further child element distinguishes calls automatically placed due to a crash or other serious incident (such as a fire) from those manually invoked by a vehicle occupant (specifically, "SOS.ecall.automatic" and "SOS.ecall.manual"). The distinction between automatic and manual invocation is also significant; automatically triggered calls indicate a car crash or some other serious incident (e.g., a fire) and carry a greater presumption of risk of injury and hence need for specific responders (such as trauma or fire). Manually triggered calls are often reports of serious hazards (such as drunk drivers) and may require different responses depending on the situation. Manually triggered calls are also more likely to be false (e.g., accidental) calls and may thus be subject to different handling by the PSAP.

A next-generation In-Vehicle System (IVS) transmits crash data by encoding it in a standardized and registered format and attaching it to an INVITE as an additional data block as specified in Section 4.1 of [I-D.ietf-ecrit-additional-data]. As described in that document, the block is identified by its MIME content-type, and pointed to by a CID URL in a Call-Info header with a ’purpose’ parameter value corresponding to the block.

Specifically, the steps required during standardization are:

- o A set of crash data is standardized by an SDO or appropriate organization

- o A MIME Content-Type for the crash data set is registered with IANA

  * If the data is specifically for use in emergency calling, the MIME type is normally under the 'application' type with a subtype starting with 'EmergencyCallData.'

  * If the data format is XML, then by convention the name has a suffix of '+xml'

- o The item is registered in the Emergency Call Additional Data registry, as defined in Section 9.1.7 of [I-D.ietf-ecrit-additional-data]

  * For emergency-call-specific formats, the registered name is the root of the MIME Content-Type (not including the 'EmergencyCallData' prefix and any suffix such as '+xml') as described in Section 4.1 of [I-D.ietf-ecrit-additional-data]

When placing an emergency call:

- o The crash data set is created and encoded per its specification

- o The crash data set is attached to the emergency call INVITE as specified in Section 4.1 of [I-D.ietf-ecrit-additional-data], that is, as a MIME body part identified by its MIME Content-Type in the body part's Content-Type header field

- o The body part is assigned a unique identifier label in a Content-ID header field of the body part

- o A Call-Info header field at the top level of the INVITE is added that references the crash data and identifies it by its MIME root (as registered in the Emergency Call Additional Data registry)

  * The crash data is referenced in the Call-Info header field by a CID URL that contains the unique Content ID assigned to the crash data body part

  * The crash data is identified in the Call-Info header field by a 'purpose' parameter whose value is 'EmergencyCallData.' concatenated with the specific crash data entry in the Emergency Call Additional Data registry

  * The Call-Info header field MAY be either solely to reference the crash data (and hence have only the one URL) or may also contain other URLs referencing other data

- o Additional crash data sets MAY be included by following the same steps

The Vehicle Emergency Data Set (VEDS) is an XML structure defined by the Association of Public-Safety Communications Officials (APCO) and the National Emergency Number Association (NENA) [VEDS]. The 'application/EmergencyCallData.VEDS+xml' MIME content-type is used to identify it. The 'VEDS' entry in the Emergency Call Additional Data registry is used to construct a 'purpose' parameter value for conveying VEDS data in a Call-Info header.

The VEDS data is attached as a body part with MIME content type 'application/EmergencyCallData.VEDS+xml' which is pointed at by a Call-Info URL of type CID with a 'purpose' parameter of 'EmergencyCallData.VEDS'.

Entities along the path between the vehicle and the PSAP are able to identify the call as an ACN call and handle it appropriately. The PSAP is able to identify the crash data as well as any other additional data attached to the INVITE by examining the Call-Info header fields for 'purpose' parameters whose values start with 'EmergencyCallData.' The PSAP is able to access and the data it is capable of handling and is interested in by checking the 'purpose' parameter values.

8. Call Routing

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 NG9-1-1 architecture adopted by NENA as well as the NG1-1-2 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).

In an environment that uses ESInets, the originating network need only detect that the service URN of an emergency call is or starts with "sos", passing all types of emergency calls to an ESInet. The ESInet is then responsible for routing such calls to an appropriate PSAP. In an environment without an ESInet, the emergency services

authorities and the originating carriers would need to determine how such calls are routed.

9. Test Calls

This document uses [I-D.ietf-ecrit-ecall], which inherits the ability to utilize test call functionality from Section 15 of [RFC6881].

A service URN starting with "test." indicates a request for an automated test. Per [I-D.ietf-ecrit-ecall], "urn:service:test.sos.ecall.automatic" indicates such a test feature. This functionality is defined in [RFC6881].

Note that since test calls are placed using "test" as the parent service URN and "sos" as a child, such calls are not treated as an emergency call and so some functionality will not apply (such as preemption or service availability for devices lacking service ("non-service-initialized" or "NSI") if those are available for emergency calls); this is by design. MNOs may recognize test calls and treat them in a way that tests as much functionality as desired, but this is outside the scope of this document.

10. Example

Figure 7 shows an emergency call placed by a vehicle whereby location information and VEDS crash data are both attached to the SIP INVITE message. The INVITE has a request URI containing the ’urn:service:sos.ecall.automatic’ service URN and is thus recognized as an ACN type of emergency call, and is also recognized as a type of emergency call because the request URI starts with ’urn:service:sos’. The mobile network operator (MNO) routes the call to an Emergency services IP Network (ESInet), as for any emergency call. The ESInet processes the call as an ACN and routes the call to an appropriate ACN-capable PSAP (using location information and the fact that that it is an ACN). (In deployments where there is no ESInet, the MNO itself needs to route directly to an appropriate ACN-capable PSAP.) The call is processed by the Emergency Services Routing Proxy (ESRP), as the entry point to the ESInet. The ESRP routes the call to an appropriate ACN-capable PSAP, where the call is received by a call taker.

```
                                +---------------------------------------+
                                |                                       |
                +------------+  |                  +-------+            |
                |            |  |                  | PSAP2 |            |
                |            |  |                  +-------+            |
                | Originating|  |                                       |
                |   Mobile   |  |  +------+     +-------+               |
     Vehicle-->|  Network   |--+->| ESRP |---->| PSAP1 |--> Call-Taker |
                |            |  |  +------+     +-------+               |
                |            |  |                                       |
                +------------+  |                  +-------+            |
                                |                  | PSAP3 |            |
                                |                  +-------+            |
                                |                                       |
                                |                                       |
                                |                                       |
                                |                ESInet                 |
                                +---------------------------------------+
```

Figure 7: Example of Vehicle-Placed Emergency Call Message Flow

The example, shown in Figure 8, illustrates a SIP emergency call INVITE that is being conveyed with location information (a PIDF-LO) and crash data (as VEDS data).

```
INVITE urn:service:sos.ecall.automatic SIP/2.0
To: urn:service:sos.ecall.automatic
From: <sip:+13145551111@example.com>;tag=9fxced76sl
Call-ID: 3848276298220188511@atlanta.example.com
Geolocation: <cid:target123@example.com>
Geolocation-Routing: no
Call-Info: cid:1234567890@atlanta.example.com;
           purpose=EmergencyCallData.VEDS
Accept: application/sdp, application/pidf+xml
CSeq: 31862 INVITE
Content-Type: multipart/mixed; boundary=boundary1
Content-Length: ...

--boundary1

Content-Type: application/sdp

...Session Description Protocol (SDP) goes here

--boundary1

Content-Type: application/pidf+xml
Content-ID: <target123@atlanta.example.com>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<presence
       xmlns="urn:ietf:params:xml:ns:pidf"
       xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model"
       xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
       xmlns:dyn="urn:ietf:params:xml:ns:pidf:geopriv10:dynamic"
       xmlns:gml="http://www.opengis.net/gml"
       xmlns:gs="http://www.opengis.net/pidflo/1.0"
       entity="sip:+13145551111@example.com">
       <dm:device id="123">
           <gp:geopriv>
               <gp:location-info>
                   <gml:Point srsName="urn:ogc:def:crs:EPSG::4326">
                      <gml:pos>-34.407 150.883</gml:pos>
                   </gml:Point>
                    <dyn:Dynamic>
                       <dyn:heading>278</dyn:heading>
                       <dyn:direction><dyn:direction>
                    </dyn:Dynamic>
               </gp:location-info>
               <gp:usage-rules/>
               <method>gps</method>
           </gp:geopriv>
           <timestamp>2012-04-5T10:18:29Z</timestamp>
           <dm:deviceID>1M8GDM9A_KP042788</dm:deviceID>
       </dm:device>
</presence>

    --boundary1

Content-Type: application/EmergencyCallData.VEDS+xml
Content-ID: 1234567890@atlanta.example.com

...VEDS data object goes here

    --boundary1--
```

Figure 8: SIP INVITE indicating a Vehicule-Initated Emergency Call

11. Security Considerations

This document does not raise security considerations beyond those described in [RFC5069]. As with emergency service systems with end host provided location information there is the possibility that that location is incorrect, either intentially (in case of an a denial of service attack against the emergency services infrastructure) or due to a malfunctioning device. The reader is referred to

[I-D.ietf-ecrit-trustworthy-location] for a discussion of some of these vulnerabilities.

12. IANA Considerations

12.1. MIME Content-type Registration for 'application/ EmergencyCall.VEDS+xml'

This specification requests the registration of a new MIME type according to the procedures of RFC 4288 [RFC4288] and guidelines in RFC 3023 [RFC3023].

MIME media type name: application

MIME subtype name: EmergencyCallData.VEDS+xml

Mandatory parameters: none

Optional parameters: charset

Indicates the character encoding of enclosed XML.

Encoding considerations: Uses XML, which can employ 8-bit characters, depending on the character encoding used. See Section 3.2 of RFC 3023 [RFC3023].

Security considerations: This content type is designed to carry vehicle crash data during an emergency call. This data may contains personal 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. Please refer to Section 7 and Section 8 of [I-D.ietf-ecrit-additional-data] for more information.

Interoperability considerations: None

Published specification: [VEDS]

Applications which use this media type: Emergency Services

Additional information: None

Magic Number: None

File Extension: .xml

Macintosh file type code: 'TEXT'

Person and email address for further information: Hannes Tschofenig, Hannes.Tschofenig@gmx.net

Intended usage: LIMITED USE

Author: This specification is a work item of the IETF ECRIT working group, with mailing list address <ecrit@ietf.org>.

Change controller: The IESG <ietf@ietf.org>

12.2. Registration of the 'VEDS' entry in the Emergency Call Additional Data registry

This specification requests IANA to add the 'VEDS' entry to the Emergency Call Additional Data registry, with a reference to this document. The Emergency Call Additional Data registry has been established by [I-D.ietf-ecrit-additional-data].

13. Contributors

We would like to thank Ulrich Dietz for his help with earlier versions of the original version of this document.

14. Acknowledgements

We would like to thank Michael Montag, Arnoud van Wijk, Ban Al-Bakri, and Gunnar Hellstrom for their feedback.

15. Changes from Previous Versions

15.1. Changes from draft-ietf-01 to draft-ietf-02

- This document now refers to [I-D.ietf-ecrit-ecall] for technical aspects including the service URN; this document no longer proposes a unique service URN for non-eCall NG-ACN calls; the same service URN is now used for all NG-ACN calls including NG-eCall and non-eCall
- Added discussion of an NG-ACN call placed to a PSAP that doesn't support it
- Minor wording improvements and clarifications

15.2. Changes from draft-ietf-00 to draft-ietf-01

- Added further discussion of test calls
- Added further clarification to the document scope
- Mentioned that multi-region vehicles may need to support other crash notification specifications such as eCall
- Minor wording improvements and clarifications

15.3. Changes from draft-gellens-02 to draft-ietf-00

- o Renamed from draft-gellens- to draft-ietf-
- o Added text to Introduction to clarify that during a CS ACN, the PSAP call taker usually needs to listen to the data and transcribe it

15.4. Changes from draft-gellens-01 to -02

- o Fixed case of ’EmergencyCallData’, in accordance with changes to [I-D.ietf-ecrit-additional-data]

15.5. Changes from draft-gellens-00 to -01

- o Now using ’EmergencyCallData’ for purpose parameter values and MIME subtypes, in accordance with changes to [I-D.ietf-ecrit-additional-data]
- o Added reference to RFC 6443
- o Fixed bug that caused Figure captions to not appear

16. References

16.1. Normative References

[I-D.ietf-ecrit-additional-data]
Randy, R., Rosen, B., Tschofenig, H., Marshall, R., and J. Winterbottom, "Additional Data related to an Emergency Call", draft-ietf-ecrit-additional-data-24 (work in progress), October 2014.

[I-D.ietf-ecrit-ecall]
Gellens, R. and H. Tschofenig, "Next-Generation Pan-European eCall", draft-ietf-ecrit-ecall (work in progress), March 2015.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3023] Murata, M., St. Laurent, S., and D. Kohn, "XML Media Types", RFC 3023, January 2001.

[RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.

[RFC4288] Freed, N. and J. Klensin, "Media Type Specifications and Registration Procedures", RFC 4288, December 2005.

[RFC5031] Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", RFC 5031, January 2008.

[RFC5491] Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations", RFC 5491, March 2009.

[RFC5962] Schulzrinne, H., Singh, V., Tschofenig, H., and M. Thomson, "Dynamic Extensions to the Presence Information Data Format Location Object (PIDF-LO)", RFC 5962, September 2010.

[RFC6443] Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling Using Internet Multimedia", RFC 6443, December 2011.

[RFC6881] Rosen, B. and J. Polk, "Best Current Practice for Communications Services in Support of Emergency Calling", BCP 181, RFC 6881, March 2013.

[VEDS] "Vehicular Emergency Data Set (VEDS) version 3", July 2012, <http://apcointl.org/resources/aacn-and-veds/2012-07-25-19-24-06.html>.

16.2. Informative references

[I-D.ietf-ecrit-trustworthy-location] Tschofenig, H., Schulzrinne, H., and B. Aboba, "Trustworthy Location", draft-ietf-ecrit-trustworthy-location-14 (work in progress), July 2014.

[RFC5012] Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", RFC 5012, January 2008.

[RFC5069] Taylor, T., Tschofenig, H., Schulzrinne, H., and M. Shanmugam, "Security Threats and Requirements for Emergency Call Marking and Mapping", RFC 5069, January 2008.

Authors' Addresses

Randall Gellens
Qualcomm Technologies, Inc
5775 Morehouse Drive
San Diego 92651
US

Email: rg+ietf@qti.qualcomm.com

Brian Rosen
NeuStar, Inc.
470 Conrad Dr
Mars, PA 16046
US

Email: br@brianrosen.net

Hannes Tschofenig
(no affiliation)

Email: Hannes.Tschofenig@gmx.net
URI: http://www.tschofenig.priv.at

ECRIT
Internet-Draft
Intended status: Informational
Expires: September 8, 2015

R. Gellens
Qualcomm Technologies, Inc.
H. Tschofenig
(no affiliation)

March 7, 2015

Next-Generation Pan-European eCall
draft-ietf-ecrit-ecall-02.txt

Abstract

This document describes how to use IP-based emergency services mechanisms to support the next generation of the Pan European in-vehicle emergency call service defined under the eSafety initiative of the European Commission (generally referred to as "eCall"). eCall is a standardized and mandated system for a special form of emergency calls placed by vehicles. eCall deployment is required in the very near future in European Union member states, and eCall (and eCall-compatible systems) are also being deployed in other regions. eCall provides an integrated voice path and a standardized set of vehicle, sensor (e.g., crash related), and location data. An eCall is recognized and handled as a specialized form of emergency call and is routed to a specialized eCall-capable Public Safety Answering Point (PSAP) capable of processing the vehicle data and trained in handling emergency calls from vehicles.

Currently, eCall functions over circuit-switched cellular telephony; work on next-generation eCall (NG-eCall, sometimes called packet-switched eCall or PS-eCall) is now in process, and this document assists in that work by describing how to support eCall within the IP-based emergency services infrastructure.

This document also registers a MIME Content Type and an Emergency Call Additional Data Block for the eCall vehicle data.

Status of This Memo

time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 8, 2015.

Copyright Notice

Table of Contents

1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

This document re-uses terminology defined in Section 3 of [RFC5012].

Additionally, we use the following abbreviations:

Term	Expansion
3GPP	3rd Generation Partnership Project
CEN	European Committee for Standardization
EENA	European Emergency Number Association
ESInet	Emergency Services IP network
IMS	Internet Multimedia Subsystem
IVS	In-Vehicle System
MNO	Mobile Network Operator
MSD	Minimum Set of Data
PSAP	Public Safety Answering Point

2. Document Scope

This document is limited to the signaling, data exchange, and protocol needs of next-generation eCall (NG-eCall, also referred to as packet-switched eCall (PS-eCall) and all-IP eCall) within the SIP framework for emergency calls, as described in [RFC6443] and [RFC6881]. eCall itself is specified by 3GPP and CEN and these specifications include far greater scope than is covered here.

The eCall service operates over cellular wireless communication, but this document does not address cellular-specific details, nor client domain selection (e.g., circuit-switched versus packet-switched). All such aspects are the purview of their respective standards bodies. The scope of this document is limited to eCall operating within a SIP-based environment (e.g., 3GPP IMS Emergency Calling).

The technical contents of this document may be suitable for use in other vehicle-initiated emergency call systems, but this is out of scope for this document.

Vehicles designed for multiple regions may need to support eCall and other Advanced Automatic Crash Notification systems, such as described in [draft-ietf-ecrit-car-crash]. That system is compatible with eCall, differing primarily in the specific data set that is sent.

3. Introduction

Emergency calls made from vehicles (e.g., in the event of a crash) assist in significantly reducing road deaths and injuries by allowing emergency services to be aware of the incident, the state of the vehicle, the location of the vehicle, and to have a voice channel with the vehicle occupants. This enables a quick and appropriate response.

The European Commission initiative of eCall was conceived in the late 1990s, and has evolved to a European Parliament decision requiring the implementation of compliant in-vehicle systems (IVS) in new vehicles and the deployment of eCall in the European Member States in the very near future. eCall (and eCall-compatible systems) are also being adopted in other regions.

The pan-European eCall system provides a standardized and mandated mechanism for emergency calls by vehicles. eCall establishes procedures for such calls to be placed by in-vehicle systems, recognized and processed by the network, and routed to a specialized PSAP where the vehicle data is available to assist the call taker in assessing and responding to the situation. eCall provides a standard set of vehicle, sensor (e.g., crash related), and location data.

An eCall may be either user-initiated or automatically triggered. Automatically triggered eCalls indicate a car crash or some other serious incident and carry a greater presumption of risk of injury. Manually triggered eCalls may be reports of serious hazards and are likely to require a different response than an automatically triggered eCall. Manually triggered eCalls are also more likely to be false (e.g., accidental) calls and may thus be subject to different handling by the PSAP.

Currently, eCall is standardized (by 3GPP [SDO-3GPP] and CEN [CEN]) as a 3GPP circuit-switched call over GSM (2G) or UMTS (3G). Flags in the call setup mark the call as an eCall, and further indicate if the call was automatically or manually triggered. The call is routed to an eCall-capable PSAP, a voice channel is established between the vehicle and the PSAP, and an eCall in-band modem is used to carry a defined set of vehicle, sensor (e.g., crash related), and location data (the Minimum Set of Data or MSD) within the voice channel. The same in-band mechanism is used for the PSAP to acknowledge successful receipt of the MSD, and to request the vehicle to send a new MSD (e.g., to check if the state of or location of the vehicle or its occupants has changed). Work on next-generation eCall (NG-eCall, also referred to as packet-switched eCall or PS eCall) is now in process. As part of this work, the European Telecommunications Standards Institute (ETSI) [SDO-ETSI] has published a Technical Report titled "Mobile Standards Group (MSG); eCall for VoIP" [MSG_TR] that presents findings and recommendations regarding support for eCall in an all-IP environment. NG-eCall moves from circuit switched to all-IP, and carries the vehicle data and other eCall-specific data as additional data associated with the call. This document describes how IETF mechanisms for IP-based emergency calls, including [RFC6443] and [additional-data-draft] are used to provide the signaling and data exchange of the next generation of pan-European eCall.

The [MSG_TR] recommendation for NG-eCall is to use 3GPP IMS emergency calling with additional elements identifying the call as an eCall and as carrying eCall data and with mechanisms for carrying the data. 3GPP IMS emergency services support multimedia, providing the ability to carry voice, text, and video. This capability is referred to within 3GPP as Multimedia Emergency Services (MMES).

A transition period will exist during which time the various entities involved in initiating and handling an eCall might support next-generation eCall, legacy eCall, or both. This transition period might last several years or longer. The issue of migration/co-existence during the transition period is very important but is outside the scope of this document. The ETSI TR "Mobile Standards Group (MSG); eCall for VoIP" [MSG_TR] discusses these issues in Clause 7.

4. eCall Requirements

Overall eCall requirements are specified by CEN in [EN_16072] and by 3GPP in [TS22.101] clauses 10.7 and A.27. Requirements specific to vehicle data are contained in EN 15722 [msd]. For convenience, the requirements most applicable to the limited scope of this document are summarized very briefly below.

eCall requires:

- The call 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
- Carrying the MSD intrinsically with the call (the MSD needs to be available to the same call-taker as the voice)
- The ability for the PSAP to acknowledge receipt of the MSD
- The ability for the PSAP to request that the vehicle generate and transmit a new MSD
- The ability of the PSAP to be able to re-contact the occupants of vehicle after the initial eCall is concluded
- The ability to perform a test call (which may be routed to a PSAP but is not treated as an emergency call and not handled by a call taker)

It is recognized that NG-eCall offers many potential enhancements, although these are not required by current EU regulations. For convenience, the enhancements most applicable to the limited scope of this document are summarized very briefly below.

NG-eCall is expected to offer:

- o The ability to carry more data (e.g., an enhanced MSD or an MSD plus additional sets of data)
- o The ability to handle video
- o The ability to handle text
- o 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)
- o The ability for the PSAP to request the vehicle to take actions (e.g., sound the horn, disable the ignition, lock/unlock doors)
- o The ability to avoid audio muting of the voice channel (because the MSD is not transferred using an in-band modem)

5. Vehicle Data

Pan-European eCall provides a standardized and mandated set of vehicle related data, known as the Minimum Set of Data (MSD). The European Committee for Standardization (CEN) has specified this data in EN 15722 [msd], along with both ASN.1 and XML encodings for the MSD [msd]. Circuit-switched eCall uses the ASN.1 encoding. The XML encoding is better suited for use in SIP messages and is used in this document. (The ASN.1 encoding is specified in Annex A of EN 15722 [msd], while the XML encoding is specified in Annex C.)

The "Additional Data related to an Emergency Call" document [additional-data-draft] establishes a general mechanism for attaching blocks of data to a SIP emergency call. This document makes use of that mechanism to carry the eCall MSD in a SIP emergency call.

This document registers the ’application/ emergencyCallData.eCall.MSD+xml’ MIME Content-Type to enable the MSD to be carried in SIP. This document also adds the ’eCall.MSD’ entry to the Emergency Call Additional Data Blocks registry (established by [additional-data-draft]) to enable the MSD to be recognized as such in a SIP-based eCall emergency call.

Note that if additional data sets are defined and registered (e.g., in the future or in other regions) and transmitted using the same mechanisms, the size and frequency of transmission during a session needs to be evaluated to be sure it is appropriate to use the signaling channel.

6. Call Setup

In circuit-switched eCall, the IVS places a special form of a 112 emergency call which carries the eCall flag (indicating that the call is an eCall and also if the call was manually or automatically triggered); the mobile network operator (MNO) recognizes the eCall flag and routes the call to an eCall-capable PSAP; vehicle data is

transmitted to the PSAP via the eCall in-band modem (in the voice channel).

```
   ///----\\\      112 voice call with eCall flag      +------+
  ||| IVS  |||----------------------------------------->+ PSAP |
   \\\----///   vehicle data via eCall in-band modem   +------+
```

Figure 1: circuit-switched eCall

An In-Vehicle System (IVS) which supports NG-eCall transmits the MSD in accordance with [additional-data-draft] by encoding it as specified (per Appendix C of EN 15722 [msd]) and attaching it to an INVITE as a MIME body part. The body part is identified by its MIME content-type (’application/emergencyCallData.eCall.MSD+xml’) in the Content-Type header field of the body part. The body part is assigned a unique identifier which is listed in a Content-ID header field in the body part. The INVITE is marked as containing the MSD by adding (or appending to) a Call-Info header field at the top level of the INVITE. This Call-Info header field contains a CID URL referencing the body part’s unique identifier, and a ’purpose’ parameter identifying the data as the eCall MSD per the registry entry; the ’purpose’ parameter’s value is ’emergencyCallData.’ and the root of the MIME type (not including the ’emergencyCallData’ prefix and any suffix such as ’+xml’ (e.g., ’purpose=emergencyCallData.eCall.MSD’).

For NG-eCall, the IVS establishes an emergency call using the 3GPP IMS solution with a Request-URI indicating an eCall type of emergency call and with vehicle data attached; the MNO or ESInet recognizes the eCall URN and routes the call to a NG-eCall capable PSAP; the PSAP interpets the vehicle data sent with the call and makes it available to the call taker.

```
  ///----\\\     IMS emergency call with eCall URN    +------+
     IVS    ----------------------------------------->+ PSAP |
  \\\----///    vehicle data included in call setup   +------+
```

Figure 2: NG-eCall

This document registers new service URN children within the "sos" subservice. These URNs provide the mechanism by which an eCall is identified, and differentiate between manually and automatically triggered eCalls (which may be subject to different treatment, depending on policy). The two service URNs are: urn:service:sos.ecall.automatic and urn:service:sos.ecall.manual

7. Call Routing

The routing rules for eCalls are likely to differ from those of other emergency calls because eCalls are special types of emergency calls (with implications for the types of response required) and need to be handled by specially designated PSAPs. In an environment that uses ESInets, the originating network passes all types of emergency calls to an ESInet (which have a request URI containing the "SOS" service URN). The ESInet is then responsible for routing such calls to the appropriate PSAP. In an environment without an ESInet, the emergency services authorities and the originating network jointly determine how such calls are routed.

7.1. ESInets

This section provides background information on ESInets for information only.

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 NG1-1-2 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 may 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). Note that in order to support legacy eCall-capable PSAPs that are not IP PSAPs and are not attached to an ESInet, an originating network may need the ability to route an eCall itself (e.g., to an interworking facility with interconnection to a suitable legacy eCall capable PSAP) based on the eCall and manual or automatic indications. The ETSI TR "Mobile Standards Group (MSG); eCall for VoIP" [MSG_TR] discusses transition issues in Clause 7.

8. Test Calls

eCall requires the ability to place test calls. These are calls that are recognized and treated to some extent as eCalls but are not given emergency call treatment and are not handled by call takers. The test call facility allows the IVS or user to verify that an eCall can be successfully established with voice communication. The IVS can also verify that the MSD was successfully received.

A service URN starting with "test." indicates a test call. For eCall, "urn:service:test.sos.ecall" indicates such a test feature. This functionality is defined in [RFC6881].

This document registers "urn:service:test.sos.ecall" for eCall test calls.

the current eCall test call facility is a non-emergency number so does not get treated as an emergency call. MNOs may treat a vehicle call in the "test" service URN in a way that tests as much functionality as desired, but this is outside the scope of this document.

PSAPs that have the ability to process NG-eCalls SHOULD accept test calls and send an acknowledgment if the MSD was successfully received, per this document. Such PSAPs MAY also play an audio clip (for example, saying that the call reached a PSAP) in addition to supporting media loopback per [RFC6881].

9. eCall-Specific Control/Metadata

eCall requires the ability for the PSAP to acknowledge successful receipt of an MSD sent by the IVS, and for the PSAP to request that the IVS send an MSD (e.g., the call taker may initiate a request for a new MSD to see if the vehicle’s state or location has changed). Future enhancements are desired to enable the PSAP to send other requests to the vehicle, such as locking or unlocking doors, sounding the horn, flashing the lights, starting a video stream from on-board cameras (such as rear focus or blind-spot), etc.

The mechanism established in [additional-data-draft], used in Section 5 of this document to carry the MSD from the IVS to the PSAP, is also used to carry a block of control data from the PSAP to the IVS. This eCall control block (sometimes referred to as eCall metadata) is an XML structure containing eCall-specific elements. When the PSAP needs to send an eCall control block that is in response to the MSD or other data sent by the IVS in a SIP request, the control block can be sent in the SIP response to that request (e.g., the INVITE). When the PSAP needs to send an eCall control

block that is not an immediate response to an MSD or other data sent by the IVS, the control block can be transmitted from the PSAP to the IVS in a SIP INFO message within the established session. The IVS can then send any requested data (such as a new MSD) in the reply to the INFO message. This mechanism flexibly allows the PSAP to send eCall-specific data to the IVS and the IVS to respond. If control data sent in a response message requests the IVS to send a new MSD or other data block, or to perform an action other than sending data, the IVS can send the requested data or an acknowledgment regarding the action in an INFO message within the session (it could also use re-INVITE but that is unnecessary when no aspect of the session or media is changing).

This mechanism requires

- o An XML definition of the eCall control object
- o An extension mechanism by which new elements can be added to the control object definition (e.g., permitting additional elements to be included by adding their namespace)
- o A MIME type registration for the control object (so it can be carried in SIP messages and responses)
- o An entry in the Emergency Call Additional Data Blocks sub-registry (established by [additional-data-draft]) so that the control block can be recognized as emergency call specific data within the SIP messages
- o An Info-Package registration per [RFC6086] permitting the control block within Info messages

9.1. The eCall Control Block

The eCall control block is an XML data structure allowing for acknowledgments, requests, and capabilities information. It is carried in a SIP body part with a specific MIME content type. Three top-level elements are defined for use within an eCall control block:

ack: Used in a control block sent by either side. The PSAP uses this to acknowledge receipt of data set sent by the IVS. The IVS uses this to acknowledge receipt of a request by the PSAP when that request would not otherwise be acknowledged (if the PSAP requests the vehicle to send data and the vehicle does so, the data serves as a success acknowledgement).

capabilities: Used in a control block sent from the IVS to the PSAP (in the initial INVITE or subsequently if desired) to inform the PSAP of the vehicle capabilities. Child elements contain all actions and data types supported by the vehicle .

request Used in a control block sent by the PSAP to the IVS, to request the vehicle to perform an action.

Mandatory Actions (the IVS and the PSAP MUST support):

- o Transmit data object

Optional Actions (the IVS and the PSAP MAY support):

- o Play and/or display static (pre-defined) message
- o Speak/display dynamic text (text supplied in action)
- o Flash lights, honk horn

The 'ack' element indicates the object being acknowledged, and reports success or failure.

The 'capabilities' element has child 'request' elements to indicate the actions supported by the IVS.

The 'request' element contains attributes to indicate the request and to supply any needed information, and MAY contain a 'text' child element to contain the text for a dynamic message. The 'action' attribute is mandatory and indicates the specific action. An IANA registry is established by this document in Section 13.8.1 to contain the allowed values.

New elements, child elements, and attributes can be defined with their own sub-namespaces. IANA registries are used to specify the permitted values of several elements and attributes. These mechanisms allow for extension.

The control block does not contain a 'request' action to play dynamic media (such as a pre-recorded audio message). The SIP re-INVITE mechanism can be used to establish a one-way media stream for this purpose.

9.1.1. The 'ack' Element

The 'ack' element is transmitted by the PSAP to acknowledge receipt of an eCall data object. An 'ack' element sent by a PSAP references the unique ID of the data object that was sent by the IVS, and further indicates if the PSAP considers the receipt successful or not. The 'ack' element is also transmitted by the IVS to the PSAP to acknowledge receipt of a 'request' element that requested the IVS to perform an action other than transmitting a data object (e.g., a request to display a message would be acknowledged, but a request to transmit a data object would not result in a separate 'ack' element being sent, since the data object itself serves as acknowledgment.)

An ’ack’ element sent by an IVS references the unique ID of the request being acknowledged, and further indicates whether the request was successfully performed.

The ’ack’ element has the following attributes and child elements:

9.1.1.1. Attributes of the ’ack’ Element

The ’ack’ element has the following attributes:

Name: ref
Usage: Mandatory
Type: anyURI
Description: References the Content-ID of the body part that contained the data object or control object being acknowledged.
Example: <ack received="yes" ref="1234567890@atlanta.example.com"/>

Name: rec
Usage: Mandatory
Type: Boolean
Description: Indicates if the referenced object was successfully received or not.
Example: <ack received="yes" ref="1234567890@atlanta.example.com"/>

9.1.1.2. Child Elements of the ’ack’ Element

The ’ack’ element has the following child elements:

Name: ActionResult
Usage: Optional
Description: An ’ActionResult’ element indicates the result of an action (other than a ’send-data’ action). It has the following attributes:

Name: action
Usage: Mandatory
Type: token
Description: Contains the value of the ’action’ attribute of the ’request’ element

Name: success
Usage: Mandatory
Type: Boolean
Description: Indicates if the action was successfully accomplished

Name: reason
Usage: Conditional
Type: token
Description: Used when ’success’ is "False", this attribute contains a reason code for a failure. A registry for reason codes is defined in Section 13.8.3.

Name: details
Usage: optional
Type: string
Description: Contains further explanation of the circumstances of a success or failure. The contents are implementation-specific and human-readable.

Example: <ActionResult action="msg-dynamic" success="true"/>

Example: <ActionResult action="lamp" success="false" reason="unable" details="The requested lamp is inoperable"/>

9.1.2. The ’capabilities’ Element

The ’capabilities’ element is transmitted by the IVS to indicate to the PSAP its capabilities. No attributes are currently defined. The following child elements may be used:

9.1.2.1. Child Elements of the ’capabilities’ Element

The ’capabilities’ element has the following child elements:

Name: request
Usage: Mandatory
Description: The ’capabilities’ element contains a <request> child element per action supported by the vehicle. Because support for a ’send-data’ action is REQUIRED, a <request> child element with a "send-data" ’action’ attribute is also REQUIRED. The ’supported-datatype’ attribute is REQUIRED in this <request> element and MUST contain all eCall data blocks supported by the IVS. Currently, only the ’eCall.MSD’ datatype is defined. All other actions are OPTIONAL. If the "msg-static" action is supported, a <request> child element with a "msg-static" ’action’ attribute is sent, with a ’msgid’ attribute set to the highest supported static message supported by the vehicle.
Examples: <request action="send-data" supported-datatype="eCall.MSD" />
<request action="send-data" supported-datatype="eCall.MSD; VEDS; eCall.type2" />
<request action="msg-dynamic"/>
<request action="msg.static" msgid="17" />

9.1.3. The ’request’ Element

A ’request’ element appears one or more times on its own or as a child of a ’capabilities’ element. The following attributes and child elements may be used:

9.1.3.1. Attributes of the ’request’ Element

The ’request’ element has the following attributes:

Name: action
Usage: Mandatory
Type: token
Description: Identifies the action that the vehicle is requested to perform. An IANA registry is established in Section 13.8.1 to contain the allowed values.
Example: action="send-data"

Name: msgid
Usage: Conditional
Type: int
Description: Mandatory with a "msg-static" action. Indicates the identifier of the static message to be displayed and/or spoken for the vehicle occupants. This document established an IANA registry for messages and their IDs, in Section 13.8.2
Example: msgid="3"

Name: persistance
Usage: Optional
Type: duration
Description: Specifies how long to carry on the specified action, for example, how long to continue honking or flashing. If absent, the default is indefinitely.
Example: persistance="PT1H"

Name: datatype
Usage: Conditional
Type: token
Description: Mandatory with a "send-data" action. Specifies the data block that the IVS is requested to transmit, using the same identifier as in the ’purpose’ attribute set in a Call-Info header field to point to the data block. Permitted values are contained in the ’Emergency Call Data Types’ IANA registry established in [additional-data-draft].
Example: datatype="eCall.MSD"

Name: supported-datatype
Usage: Conditional

Type: token
Description: Used with a 'send-data' action in a 'request' element that is a child of a 'capability' element, this attribute lists all data blocks that the vehicle can transmit, using the same identifier as in the 'purpose' attribute in a Call-Info header field to point to the data block. Permitted values are contained in the 'Emergency Call Data Types' IANA registry established in [additional-data-draft]. Multiple values are separated with a semicolon.
Example: supported-datatype="eCall.MSD; VEDS; eCall.foo"

Name: lamp-ID
Usage: Conditional
Type: token
Description: Used with a 'lamp' action, indicates which lamps the action affects. This document creates a registry of lamp-ID tokens, in Section 13.8.4
Example: lamp-ID="hazard"

Name: lamp-action
Usage: Conditional
Type: enumeration
Description: Used with a 'lamp' action, indicates if the lamp should be illuminated, turned off, or flashed. Permitted values are 'on', 'off', and 'flash'.
Example: lamp-action="flash"

9.1.3.2. Child Elements of the 'request' Element

The 'request' element has the following child elements:

Name: text
Usage: Conditional
Type: string
Description: Used within a <request action="msg-dynamic"> element to contain the text to be displayed and/or spoken (via text-to-speech) for the vehicle occupants.
Example: <text>Emergency authorities are aware of your incident and location. Due to a multi-vehicle incident in your area, no one is able to speak with you right now. Please remain calm. We will assist you soon.</text>

9.2. The emergencyCallData.eCall INFO package

This document registers the 'emergencyCallData.eCall' INFO package. Both endpoints (the IVS and the PSAP equipment) set the Recv-Info header field to 'emergencyCallData.eCall' per [RFC6086] to indicate

ability to receive INFO messages carrying eCall data or control blocks.

Support for the 'emergencyCallData.eCall' INFO package indicates the ability to receive eCall data and control blocks, which are carried in a body part whose subtype starts with 'emergencyCallData.eCall.'. At present there is only one defined eCall data block, which has the 'application/emergencyCallData.eCall.MSD+xml' MIME type, and one eCall control block, which has the 'application/ emergencyCallData.eCall.control+xml' MIME type. The eCall control block includes the ability for the IVS to indicate its capabilities, so in the event additional eCall blocks are defined, the IVS can indicate which it supports.

The use of INFO is based on an analysis of the requirements against the intent and effects of INFO versus other approaches (such as SIP MESSAGE, media plane, or non-SIP protocols). In particular, the transport of eCall data and control blocks is done only during an emergency session established with SIP, using the mechanism established in [additional-data-draft], and is normally carried in the initial INVITE and its response; the use of INFO only occurs when a data block or request needs to be sent subsequently during the call. While MESSAGE could be used, it is not tied to a SIP session as is INFO. REINVITE could also be used, but is normally used to modify the session. SUBSCRIBE/NOTIFY could be coerced into service, but the semantics are not a clean fit. Hence, INFO is appropriate.

An INFO request message carrying an eCall data or control block has an Info-Package header field set to 'emergencyCallData.eCall' per [RFC6086]. The INFO request message is marked as containing the eCall data or control block by a Call-Info header field containing a CID URL referencing the unique identifier of the body part containing the eCall data or control, and a 'purpose' parameter identifying the block. Because the eCall data or control block is being carried in an INFO request message, the body part also carries a Content-Disposition header field set to "Info-Package".

Per [additional-data-draft], emergency call related additional data MAY be included in any SIP request or response message that may contain a body. Hence, notwithstanding Section 4.3.2. of [RFC6086], INFO response messages MAY contain eCall data or control blocks, provided they are included as described in this document (with a Call-Info header field containing a CID URL referencing the unique identifier of the body part, and a 'purpose' parameter identifying the block). When eCall data or control blocks are included in an INFO response message, this is done per [additional-data-draft] and this document, and not under [RFC6086]; that is, they are included as

emergency call additional data, not as an INFO package associated data.

10. Examples

Figure 3 shows an eCall. The call uses the request URI 'urn:service:sos.ecall.automatic' service URN and is recognized as an eCall, and further as one that was invoked automatically by the IVS due to a crash or other serious incident. In this example, the originating network routes the call to an ESInet (as for any emergency call in an environment with an ESInet). The ESInet routes the call to the appropriate NG-eCall capable PSAP. The emergency call is received by the ESInet's Emergency Services Routing Proxy (ESRP), as the entry point into the ESInet. The ESRP routes the call to a PSAP, where it is received by a call taker. In deployments where there is no ESInet, the originating network routes the call directly to the appropriate NG-eCall capable PSAP.

```
                +------------+  +-------------------------------------+
                |            |  |                  +-------+          |
                |            |  |                  | PSAP2 |          |
                |            |  |                  +-------+          |
                |            |  |                                     |
                |            |  |  +------+     +-------+             |
      Vehicle-->|            |--+->| ESRP |---->| PSAP1 |--> Call-Taker |
                |            |  |  +------+     +-------+             |
                |            |  |                                     |
                |            |  |                  +-------+          |
                |            |  |                  | PSAP3 |          |
                | Originating|  |                  +-------+          |
                |   Mobile   |  |                                     |
                |  Network   |  |                ESInet               |
                +------------+  +-------------------------------------+
```

Figure 3: Example of NG-eCall Message Flow

The example, shown in Figure 4, illustrates a SIP eCall INVITE that contains an MSD.

```
INVITE urn:service:sos.ecall.automatic SIP/2.0
To: urn:service:sos.ecall.automatic
From: <sip:+13145551111@example.com>;tag=9fxced76sl
Call-ID: 3848276298220188511@atlanta.example.com
Geolocation: <cid:target123@example.com>
Geolocation-Routing: no
Call-Info: cid:1234567890@atlanta.example.com;
           purpose=emergencyCallData.eCall.MSD
Accept: application/sdp, application/pidf+xml
CSeq: 31862 INVITE
Recv-Info: emergencyCallData.eCall
Content-Type: multipart/mixed; boundary=boundary1
Content-Length: ...

--boundary1

Content-Type: application/sdp

...Session Description Protocol (SDP) goes here

--boundary1

Content-Type: application/emergencyCallData.eCall.MSD+xml
Content-ID: 1234567890@atlanta.example.com

...eCall MSD data object goes here

 --boundary1--
```

Figure 4: SIP NG-eCall INVITE

11. Security Considerations

The security considerations described in [RFC5069] apply here.

An eCall will carry two forms of location data: the network-provided location that is inherently part of IMS emergency calls (which might be determined solely by the network, or in cooperation with or possibly entirely by the originating device), and the 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.

The document [I-D.ietf-ecrit-trustworthy-location] discusses trust issues regarding location provided by or determined in cooperation with end devices.

The mechanism by which the PSAP sends acknowledgments and requests to the vehicle requires authenticity considerations; when the PSAP request is received within a session initiated by the vehicle as an eCall emergency call placed over a cellular network, there is a higher degree of trust that the source is indeed a PSAP. If the PSAP request is received in other situations, such as a call-back, the trust issues in verifying that a call-back is indeed from a PSAP are more complex (see the PSAP Callback document [RFC7090]). A further 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.

12. XML Schema

This section defines the XML schema of the eCall control block.

```
<?xml version="1.0" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:tns="http://example.com/ct-required"
           xmlns:xmime="http://www.w3.org/2005/05/xmlmime"
           targetNamespace="http://example.com/ct-required">

    <xs:import namespace="http://www.w3.org/2005/05/xmlmime"
            schemaLocation="http://www.w3.org/2005/05/xmlmime"/>



</xs:schema>
```

Figure 5: eCall Control Block Schema

13. IANA Considerations

13.1. Service URN Registrations

IANA is requested to register the URN 'urn:service:sos.ecall' under the sub-services 'sos' registry defined in Section 4.2 of [RFC5031].

This service identifies a type of emergency call (placed by a specialized in-vehicle system and a carrying standardized set of data related to the vehicle and crash or incident, and is needed to direct the call to a specialized public safety answering point (PSAP) with technical and operational capabilities to handle such calls. Two sub-services are registered as well, namely

urn:service:sos.ecall.manual

This service URN indicates that an eCall had been triggered based on the manual interaction of the driver or a passenger.

urn:service:sos.ecall.automatic

This service URN indicates that an eCall had been triggered automatically, for example, due to a crash or other serious incident (e.g., fire).

IANA is also requested to register the URN 'urn:service:test.sos.ecall' under the sub-service 'test' registry defined in Setcion 17.2 of [RFC6881].

13.2. MIME Content-type Registration for 'application/emergencyCallData.eCall.MSD+xml'

IANA is requested to add application/emergencyCallData.eCall.MSD+xml as a MIME content type, with a reference to this document, in accordance to the procedures of RFC 6838 [RFC6838] and guidelines in RFC 7303 [RFC7303].

MIME media type name: application

MIME subtype name: emergencyCallData.eCall.MSD+xml

Mandatory parameters: none

Optional parameters: charset

Indicates the character encoding of the XML content.

Encoding considerations: Uses XML, which can employ 8-bit characters, depending on the character encoding used. See Section 3.2 of RFC 7303 [RFC7303].

Security considerations: This content type is designed to carry vehicle and incident-related data during an emergency call. This data contains personal 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. Sections 7 and Section 8 of [I-D.ietf-ecrit-additional-data] contain more discussion.

Interoperability considerations: None

Published specification: Annex C of EN 15722 [msd]

Applications which use this media type: Pan-European eCall compliant systems

Additional information: None

Magic Number: None

File Extension: .xml

Macintosh file type code: 'TEXT'

Person and email address for further information: Hannes Tschofenig, Hannes.Tschofenig@gmx.net

Intended usage: LIMITED USE

Author: This specification was produced by the European Committee For Standardization (CEN). For contact information, please see <http://www.cen.eu/cen/Pages/contactus.aspx>.

Change controller: The European Committee For Standardization (CEN)

13.3. MIME Content-type Registration for 'application/emergencyCallData.eCall.control+xml'

IANA is requested to add application/emergencyCallData.eCall.control+xml as a MIME content type, with a reference to this document, in accordance to the procedures of RFC 6838 [RFC6838] and guidelines in RFC 7303 [RFC7303].

MIME media type name: application

MIME subtype name: emergencyCallData.eCall.control+xml

Mandatory parameters: none

Optional parameters: charset

Indicates the character encoding of the XML content.

Encoding considerations: Uses XML, which can employ 8-bit characters, depending on the character encoding used. See Section 3.2 of RFC 7303 [RFC7303].

Security considerations: 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 transmit a data set, which as described in Section 13.2, may contain personal information. The security implication 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 from an impostor. The first safeguard for this is the security of the cellular network over which the emergency call was placed. In particular, when the IVS initiates an eCall over a cellular network, the MNO routes the call to a PSAP. (Calls placed using other means, such as Wi-Fi or over-the-top services, do not carry the same degree of trust.) Calls received by the IVS, such as a call-back from a PSAP, also do not carry the same degree of trust, since the current mechanisms are not ideal for verifying that such a call is indeed from a PSAP in response to an emergency call placed by the IVS. See the discussion in Section 11 and the PSAP Callback document [RFC7090]. A further safeguard, and one 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. Sections 7 and Section 8 of [I-D.ietf-ecrit-additional-data] contain more discussion.

Interoperability considerations: None

Published specification: Annex C of EN 15722 [msd]

Applications which use this media type: Pan-European eCall compliant systems

Additional information: None

Magic Number: None

File Extension: .xml

Macintosh file type code: ’TEXT’

Person and email address for further information: Randall Gellens, rg+ietf@qti.qualcomm.com

Intended usage: LIMITED USE

Author: The IETF ECRIT WG.

Change controller: The IETF ECRIT WG.

13.4. Registration of the ’eCall.MSD’ entry in the Emergency Call Additional Data Blocks registry

This specification requests IANA to add the ’eCall.MSD’ entry to the Emergency Call Additional Data Blocks registry (established by [additional-data-draft]), with a reference to this document.

13.5. Registration of the ’eCall.control’ entry in the Emergency Call Additional Data Blocks registry

This specification requests IANA to add the ’eCall.control’ entry to the Emergency Call Additional Data Blocks registry (established by [additional-data-draft]), with a reference to this document.

13.6. Registration of the emergencyCallData.eCall Info Package

IANA is requested to add emergencyCallData.eCall to the Info Packages Registry under "Session Initiation Protocol (SIP) Parameters", with a reference to this document.

13.7. URN Sub-Namespace Registration

13.7.1. Registration for urn:ietf:params:xml:ns:eCall

This section registers a new XML namespace, as per the guidelines in RFC 3688 [RFC3688].

URI: urn:ietf:params:xml:ns:eCall

Registrant Contact: IETF, ECRIT working group, <ecrit@ietf.org>, as delegated by the IESG <iesg@ietf.org>.

XML:

```
BEGIN
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
 "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
 <meta http-equiv="content-type"
       content="text/html;charset=iso-8859-1"/>
 <title>Namespace for eCall Data</title>
</head>
<body>
 <h1>Namespace for eCall Data
    </h1>
<p>See [TBD: This document].</p>
</body>
</html>
END
```

13.7.2. Registration for urn:ietf:params:xml:ns:eCall:control

This section registers a new XML namespace, as per the guidelines in RFC 3688 [RFC3688].

URI: urn:ietf:params:xml:ns:eCall:control

Registrant Contact: IETF, ECRIT working group, <ecrit@ietf.org>, as delegated by the IESG <iesg@ietf.org>.

XML:

```
BEGIN
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
  "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="content-type"
        content="text/html;charset=iso-8859-1"/>
  <title>Namespace for eCall Data:
         Control Block</title>
</head>
<body>
  <h1>Namespace for eCall Data
     </h1>
  <h2>Control Block</h2>
<p>See [TBD: This document].</p>
</body>
</html>
END
```

13.8. Registry creation

This document creates a new registry called ’eCall Control Data’. The following sub-registries are created for this registry.

13.8.1. eCall Control Action Registry

This document creates a new sub-registry called "eCall Control Action Registry". As defined in [RFC5226], this registry operates under "Expert Review" rules. The expert should determine that the proposed action is within the purview of a vehicle, is sufficiently distinguishable from other actions, and the actions is clearly and fully described. In most cases, a published and stable document is referenced for the description of the action.

The content of this registry includes:

Name: The identifier to be used in the ’action’ attribute of an eCall control ’request’ element.

Description: A description of the action. In most cases this will be a reference to a published and stable document. The description MUST specify if any attributes or child elements are optional or mandatory, and describe the action to be taken by the vehicle.

The initial set of values is listed in Table 2.

Name	Description
send-data	Section xxx of this document
msg-static	Section xxx of this document
msg-dynamic	Section xxx of this document
honk	Section xxx of this document
lamp	Section xxx of this document

Table 2: eCall Control Action Registry Initial Values

13.8.2. eCall Static Message Registry

This document creates a new sub-registry called "eCall Static Message Registry". Because all compliant vehicles are expected to support all static messages translated into all languages supported by the vehicle, it is important to limit the number of such messages. As defined in [RFC5226], this registry operates under "Publication Required" rules, which require a stable, public document and imply expert review of the publication. The expert should determine that the document has been published by an appropriate emergency services organization (e.g., NENA, EENA, APCO) and that the proposed message is sufficiently distinguishable from other messages.

The content of this registry includes:

ID: An integer identifier to be used in the ’msgid’ attribute of an eCall control ’request’ element.

Message: The text of the message. Messages are listed in the registry in English; vehicles are expected to implement translations into languages supported by the vehicle.

When new messages are added to the registry, the message text is determined by the registrant; IANA assigns the IDs. Each message is assigned a consecutive integer value as its ID. This allows an IVS to indicate by a single integer value that it supports all messages with that value or lower.

The initial set of values is listed in Table 3.

ID	Message
1	Emergency authorities are aware of your incident and location. No one is free to speak with you right now. We will help you as soon as possible.

Table 3: eCall Static Message Registry

13.8.3. eCall Reason Registry

This document creates a new sub-registry called "eCall Reason Registry" which contains values for the 'reason' attribute of the 'ActionResult' element. As defined in [RFC5226], this registry operates under "Expert Review" rules. The expert should determine that the proposed reason is sufficiently distinguishable from other reasons and that the proposed description is understandable and correctly worded.

The content of this registry includes:

ID: A short string identifying the reason, for use in the 'reason' attribute of an 'ActionResult' element.

Description: A description of the reason.

The initial set of values is listed in Table 4.

ID	Description
unsupported	The 'action' is not supported.
unable	The 'action' could not be accomplished.
data-unsupported	The data item referenced in a 'send-data' request is not supported.

Table 4: eCall Reason Registry

13.8.4. eCall Lamp ID Registry

This document creates a new sub-registry called "eCall Lamp ID Registry" to standardize the names of automotive lamps (lights). As defined in [RFC5226], this registry operates under "Expert Review" rules. The expert should determine that the proposed lamp name is

clearly understandable and is sufficiently distinguishable from other lamp names.

The content of this registry includes:

Name: The identifier to be used in the 'lamp-ID' attribute of an eCall control 'request' element.

Description: A description of the lamp (light).

The initial set of values is listed in Table 5.

Name	Description
head	The main lamps used to light the road ahead
interior	Interior lamp, often at the top center
fog-front	Front fog lamps
fog-rear	Rear fog lamps
brake	Brake indicator lamps
position-front	Front position/parking/standing lamps
position-rear	Rear position/parking/standing lamps
turn-left	Left turn/directional lamps
turn-right	Right turn/directional lamps
hazard	Hazard/four-way lamps

Table 5: eCall Lamp ID Registry Initial Values

14. Contributors

Brian Rosen was a co-author of the original document upon which this document is based.

15. Acknowledgements

We would like to thank Bob Williams and Ban Al-Bakri for their feedback and suggestions, and Keith Drage for his review comments. We would like to thank Michael Montag, Arnoud van Wijk, Gunnar

Hellstrom, and Ulrich Dietz for their help with the original document upon which this document is based.

16. Changes from Previous Versions

16.1. Changes from draft-ietf-01 to draft-ietf-02

- Added clarifying text reinforcing that the data exchange is for small blocks of data infrequently transmitted
- Clarified that dynamic media is conveyed using SIP re-INVITE to establish a one-way media stream
- Clarified that the scope is the needs of eCall within the SIP emergency call environment
- Added informative statement that the document may be suitable for reuse by other ACN systems
- Clarified that normative language for the control block applies to both IVS and PSAP
- Removed ’ref’, ’supported-mime’, and ’media’ elements
- Minor wording improvements and clarifications

16.2. Changes from draft-ietf-00 to draft-ietf-01

- Added further discussion of test calls
- Added further clarification to the document scope
- Mentioned that multi-region vehicles may need to support other crash notification specifications in addition to eCall
- Added details of the eCall metadata and control functionality
- Added IANA registration for the MIME content type for the eCall control object
- Added IANA registries for protocol elements and tokens used in the eCall control object
- Minor wording improvements and clarifications

16.3. Changes from draft-gellens-03 to draft-ietf-00

- Renamed from draft-gellens- to draft-ietf-.
- Added mention of and reference to ETSI TR "Mobile Standards Group (MSG); eCall for VoIP"
- Added text to Introduction regarding migration/co-existence being out of scope
- Added mention in Security Considerations that even if the network-supplied location is just the cell site, this can be useful as a sanity check on the IVS-supplied location
- Minor wording improvements and clarifications

16.4. Changes from draft-gellens-02 to -03

- o Clarifications and editorial improvements.

16.5. Changes from draft-gellens-01 to -02

- o Minor wording improvements
- o Removed ".automatic" and ".manual" from "urn:service:test.sos.ecall" registration and discussion text.

16.6. Changes from draft-gellens-00 to -01

- o Now using 'EmergencyCallData' for purpose parameter values and MIME subtypes, in accordance with changes to [additional-data-draft]
- o Added reference to RFC 6443
- o Fixed bug that caused Figure captions to not appear

17. References

17.1. Normative References

[EN_16072]
CEN, , "Intelligent transport systems - eSafety - Pan-European eCall operating requirements", December 2011.

[I-D.ietf-ecrit-additional-data]
Randy, R., Rosen, B., Tschofenig, H., Marshall, R., and J. Winterbottom, "Additional Data related to an Emergency Call", draft-ietf-ecrit-additional-data-24 (work in progress), October 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004.

[RFC5031] Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", RFC 5031, January 2008.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC6443] Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling Using Internet Multimedia", RFC 6443, December 2011.

[RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, January 2013.

[RFC6881] Rosen, B. and J. Polk, "Best Current Practice for Communications Services in Support of Emergency Calling", BCP 181, RFC 6881, March 2013.

[RFC7303] Thompson, H. and C. Lilley, "XML Media Types", RFC 7303, July 2014.

[TS22.101] 3GPP, , "Technical Specification Group Services and System Aspects; Service aspects; Service principles", .

[additional-data-draft] Rosen, B., Tschofenig, H., Marshall, R., Gellens, R., and J. Winterbottom, "Additional Data related to an Emergency Call", draft-ietf-ecrit-additional-data-11 (work in progress), July 2013.

[msd] CEN, , "Intelligent transport systems -- eSafety -- eCall minimum set of data (MSD), EN 15722", June 2011.

17.2. Informative references

[CEN] "European Committee for Standardization", <http://www.cen.eu>.

[I-D.ietf-ecrit-trustworthy-location] Tschofenig, H., Schulzrinne, H., and B. Aboba, "Trustworthy Location", draft-ietf-ecrit-trustworthy-location-14 (work in progress), July 2014.

[MSG_TR] ETSI, , "ETSI Mobile Standards Group (MSG); eCall for VoIP", ETSI Technical Report TR 103 140 V1.1.1 (2014-04), April 2014.

[RFC5012] Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", RFC 5012, January 2008.

[RFC5069] Taylor, T., Tschofenig, H., Schulzrinne, H., and M. Shanmugam, "Security Threats and Requirements for Emergency Call Marking and Mapping", RFC 5069, January 2008.

[RFC5491] Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations", RFC 5491, March 2009.

[RFC6086] Holmberg, C., Burger, E., and H. Kaplan, "Session Initiation Protocol (SIP) INFO Method and Package Framework", RFC 6086, January 2011.

[RFC6442] Polk, J., Rosen, B., and J. Peterson, "Location Conveyance for the Session Initiation Protocol", RFC 6442, December 2011.

[RFC7090] Schulzrinne, H., Tschofenig, H., Holmberg, C., and M. Patel, "Public Safety Answering Point (PSAP) Callback", RFC 7090, April 2014.

[SDO-3GPP] "3d Generation Partnership Project", <http://www.3gpp.org/>.

[SDO-ETSI] "European Telecommunications Standards Institute (ETSI)", <http://www.etsi.org>.

[draft-ietf-ecrit-car-crash] Gellens, R., Rosen, B., and H. Tschofenig, "Next-Generation Vehicle-Initiated Emergency Calls", draft-ietf-ecrit-car-crash (work in progress), March 2015.

Authors' Addresses

Randall Gellens
Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego 92651
US

Email: rg+ietf@qti.qualcomm.com

Hannes Tschofenig
(no affiliation)

Email: Hannes.Tschofenig@gmx.net
URI: http://www.tschofenig.priv.at

ECRIT
Internet-Draft
Updates: RFC6881, RFC5985
(if approved)
Intended status: Standards Track
Expires: October 7, 2015

J. Winterbottom
Winterb Consulting Services
H. Tschofenig

L. Liess
Deutsche Telekom

April 5, 2015

A Routing Request Extension for the HELD Protocol
draft-ietf-ecrit-held-routing-02.txt

Abstract

In many circumstances public LoST servers or a distributed network of forest guides linking public LoST servers is not available. The general ECRIT calling models breakdown without publically accessible LoST servers. Sometimes location servers may have access to emergency routing information. This document defines an extension to the HELD protocol so a location request can include a request for routing information and allowing the subsequent location response to include routing information.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The general ECRIT calling models described in [RFC6443] and [RFC6881]require a local LoST server or network of forest guides in order to determine the address of the PSAP in the best position to handle a call. Networks of forest guides have not eventuated and while PSAPs are moving towards IP networks, LoST server deployment is not ubiquitous. Some regions and countries have expressed reluctance to deploy LoST servers making aspects of the current ECRIT architecture hard to realize.

Evolving architectures in Europe to address regulatory requirements, such as [M493], couple location and routing information in the access network whilst using a softswitch-centric approach to emergency call processing. This document describes adding an extension to the HELD protocol [RFC5985] so that a location information server can provide emergency routing information in the absence of a LoST server or network of forest guides.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The terms LIS, ESRP, VSP and PSAP are used as defined in [RFC6443].

The term "Access Network Provider" is used as defined in [RFC5687] and incompasses both the Internet Access Provider (IAP) and Internet Service Provider (ISP).

3. Motivation

The Internet emergency calling architecture specified in [RFC6881] describes two main models for emergency call processing. The first is a device-centric model, where a device obtains location information using a location configuration protocol, such a HELD [RFC5985], and then proceeds to determine the address of the next hop closer to the local PSAP using LoST [RFC5222]. Figure 1 shows this model in a simplified form.

```
     +---Location Request---+
     |         (1)          |
 +---+----+             +---V---+
 |        |<--Location--|  LIS  |
 | Caller |    (2)      +-------+            +--------+
 |        |                                  | ESRP/  |
 |        |----Find Service-------+          |  PSAP  |
 +------^-+     (3)               |          +--------+
    |   |                +--------V----+         ^
    |   +-----Service----| LoST Server |         |
    |         (4)        +-------------+      +---+---+
    +-------------Call Initiation------------>|  VSP  |
                     (5)                      +-------+
```

Figure 1: Device-Centric Emergency Services Model

The second approach is a softswitch-centric model, where a device initiates and emergency call and the serving softswitch detects that the call is an emergency and initiates retrieving the caller’s location from a Location Information Server (LIS) using HELD [RFC5985] with identity extensions [RFC6155] [RFC6915] and then determining the route to the local PSAP using LoST [RFC5222]. Figure 2 shows the high-level protocol interactions.

```
                                +---Location Request---+
                                |         (2)          |
                            +---V---+                  |
                            |  LIS  |                  |
                            +----+--+            +----+----+
                                 |               |         |
                                 +----Location--->|  Soft   |
    +--------+                          (3)      | Switch  |
    | Caller |------Call Initiation------------> |         |
    +--------+          (1)                      +-+-^---+-+
                   +-------------+                | |   |
                   | LoST Server |<-Find Service--+ |   |
                   +------+------+     (4)          |   |
                          |                         |   |
                          +----------Service--------+   |
                                      (5)               |
                            +-----------+               |
                            | ESRP/PSAP |<------Call----+
                            +-----------+       (6)
```

Figure 2: Softswitch-Centric Calling Model

In the softswitch-centric model when a VSP receives an emergency call it performs two tasks. The first task is to determine the correct LIS to ask for location information, this is done using a combination of reverse DNS lookup described in [RFC7216] to acquire the serving domain name and then using [RFC5986] to determine the LIS URI. Once the location is obtained from the LIS, the VSP determines the LoST server associated with the domain serving the caller and queries it for the correct PSAP address.

LoST server discovery is a domain based activity, similar to the LIS discovery technique. However, unlike the LIS that is a domain bound service, a LoST server is a geographically bound service. This means that for a domain that spans multiple geographic regions the LoST server determined may not be able to provide a route to the necessary PSAP. When this occurs, the contacted LoST server invokes the help of other LoST servers and this requires the deployment of forest guides.

At the time of writing, several countries have expressed a reluctance to deploy public LoST servers. In countries amenable to the use of LoST and forest guides no public forest guides have been deployed. There appears little interest from the public sector in establishing a global forest guide network. These issues pose threats to both the device-centric and the softswitch-centric calling approaches in terms of them operating everywhere.

The device-centric and softswitch-centric calling models both involve the notion of a LIS bound to the serving access network. In many cases the LIS already knows the destination PSAP URI for any given location. In [RFC6881] for example, the LIS validates civic locations using a location validation procedure based on the LoST protocol [RFC5222]. The LoST validation request is similar to a LoST routing request and provides the LIS with the same PSAP routing information that a routing request would. In other cases, the LIS knows the correct PSAP for a given location at provisioning time, or the access network might always route to the same emergency provider. Irrespective of the way in which the LIS learns the PSAP URI for a location, the LIS will, in a great many cases, already have this information.

This document specifies an extension to the HELD protocol so that emergency routing information can be requested from the LIS at the same time that location information is requested. The document updates [RFC6881] by requiring devices and softswitches that understand this specification to always request routing information to avoid the risk of query failure where no LoST server or forest guide network is deployed.

4. Mechanism

The mechanism consists of adding an element to the HELD locationRequest and an element to the locationResponse.

The request element indicates that the requestor wants the LIS to provide routing information based on the location of the end-device. If the routing request is sent with no attribute then URIs for urn:service:sos are returned. If the requestor wants routing information for a specific service then they may include an optional service URN. If a service is specified, and the LIS does not understand the requested service then URIs for urn:service:sos are returned.

If the LIS understands the routing request and has routing information for the location then it includes the information in a routingInformation element returned in the locationResponse. How the LIS obtains this information is left to implementation, one possible option is that the LIS acquires it from a LoST server, other possibilities are described in Section 3.

A LIS that does not understand the routing request element ignores it and returns location as normal.

A LIS that does support the routing request element SHALL support

returning URIs for urn:service:sos

A LIS that does understand the routing request element but can’t obtain any routing information for the end-device’s location SHALL only return location information.

A LIS that understands the routing request element but not the specified service URN, returns the routing URIs for the urn:service:sos service.

The routing information in the location response consists of a service element identified by a service name. The service name is a urn and might contain a general emergency service urn such as urn:service:sos or might contain a specific service urn depending on what was requested and what the LIS is able to provide. A list of one or more service destinations is provided for the service name. Each destination is expressed as a URI and each URI scheme should only appear once in this list. The routing URIs are intended to be used at the time they are received. To avoid any risks of using stale routing URIs the values MUST NOT be cached by the receiving entity.

The LoST Protocol [RFC5222] defines a <mapping> element that describes a service region and associated service URLs. Reusing this element from LoST to provide the routing URIs was considered. However, this would have meant that several of the mandatory components in the <mapping> element would have had to contain ambiguous or misleading values. Specifically, the "source" attribute is required to contain a LoST application unique string for the authoritative server. However, in the situations described in this specification there may not be an authoritative LoST server, so any value put into this attribute would be misleading. In addition to this, routing information received in the manner described in this specification should not be cached by the receiver, so detailing when the routing information expires or was last updated is irrelevant.

5. HELD Schema Extension

This section describes the schema extension to HELD.

```
<?xml version="1.0"?>
<xs:schema
  targetNamespace="urn:ietf:params:xml:ns:geopriv:held:ri"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:ri="urn:ietf:params:xml:ns:geopriv:held:ri"
  xmlns:xml="http://www.w3.org/XML/1998/namespace"
  elementFormDefault="qualified" attributeFormDefault="unqualified">

  <xs:element name="requestRoutingInformation">
     <xs:complexType name="empty">
        <xs:attribute name="service" type="xs:anyUri"
            use="optional" default="urn:service:sos"/>
     </xs:complexType>
  </xs:element>

  <xs:complexType name="service">
     <xs:complexContent>
       <xs:restriction base="xs:anyType">
          <xs:sequence>
             <xs:element name="dest" type="xs:anyURI"
                  maxOccurs="unbounded"/>
             <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="serviceUri" type="xs:anyURI"
                        use="required"/>
       </xs:restriction>
     </xs:complexContent>
  </xs:complexType>

  <xs:element name="routingInformation" type="ri:riType"/>
     <xs:complexType name="riType">
       <xs:complexContent>
         <xs:restriction base="xs:anyType">
          <xs:sequence>
            <xs:element name="service" type="ri:service"/>
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:anyAttribute namespace="##any" processContents="lax"/>
        </xs:restriction>
      </xs:complexContent>
     </xs:complexType>
```

```
</xs:schema>
```

6. Examples

Figure 3 illustrates a <locationRequest> example that contains IP flow information in the request.

```
<locationRequest xmlns="urn:ietf:params:xml:ns:geopriv:held"
                 responseTime="emergencyRouting">

        <requestRoutingInformation
            xmlns="urn:ietf:params:xml:ns:geopriv:held:ri"/>

        <flow xmlns="urn:ietf:params:xml:ns:geopriv:held:flow"
              layer4="tcp" layer3="ipv4">
           <src>
              <address>192.168.1.1</address>
              <port>1024</port>
           </src>
           <dst>
              <address>10.0.0.1</address>
              <port>80</port>
           </dst>
        </flow>
</locationRequest>
```

Figure 3: Example Location Request.

Figure 4 illustrates the <locationResponse> message containing two location URIs: a HTTPS and a SIP URI. Additionally, the response contains routing information.

```
<locationResponse xmlns="urn:ietf:params:xml:ns:geopriv:held">
      <locationUriSet expires="2006-01-01T13:00:00.0Z">
        <locationURI>
                https://ls.example.com:9768/357yc6s64ceyoiuy5ax3o
        </locationURI>
        <locationURI>
                sip:9769+357yc6s64ceyoiuy5ax3o@ls.example.com
        </locationURI>
      </locationUriSet>

      <routingInformation
          xmlns="urn:ietf:params:xml:ns:geopriv:held:ri">
        <service serviceUri="urn:service:sos">
          <dest>sip:112@example.com</dest>
          <dest>sips:112@example.com</dest>
          <dest>xmpp:112@example.com</dest>
        </service>
      </routingInformation>

   </locationResponse>
```

Figure 4: Example Location Response

7. Privacy Considerations

This document makes no changes that require privacy considerations beyond those already described in [RFC5985] and [RFC6155].

8. Security Considerations

This document imposes no additional security considerations beyond those already described in [RFC5985] and [RFC6155].

9. IANA Considerations

9.1. URN sub-namespace registration for 'urn:ietf:params:xml:ns:geopriv:held:ri'

This document calls for IANA to register a new XML namespace, as per the guidelines in [RFC3688].

URI: urn:ietf:params:xml:ns:geopriv:held:ri

Registrant Contact: IETF, ECRIT working group (ecrit@ietf.org), James Winterbottom (a.james.winterbottom@gmail.com).

XML:

```
BEGIN
 <?xml version="1.0"?>
 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
  <head>
    <title>HELD Routing Information Extensions</title>
  </head>
  <body>
   <h1>Additional Element for HELD Routing Information</h1>
   <h2>urn:ietf:params:xml:ns:geopriv:held:ri</h2>
   [[NOTE TO IANA/RFC-EDITOR: Please update RFC URL and replace XXXX
     with the RFC number for this specification.]]
   <p>See <a href="[[RFC URL]]">RFCXXXX</a>.</p>
  </body>
 </html>
END
```

9.2. XML Schema Registration

This section registers an XML schema as per the procedures in [RFC3688].

URI: urn:ietf:params:xml:schema:geopriv:held:ri

Registrant Contact: IETF, ECRIT working group, (ecrit@ietf.org), James Winterbottom (a.james.winterbottom@gmail.com).

The XML for this schema can be found as the entirety of Section 5 of this document.

10. Acknowledgements

We would like to thank Wilfried Lange for sharing his views with us. We would also like to thank Bruno Chatras for his early review comments and Bernd Henschel for his support. Thanks to Roger Marshall and Randy Gellens for their helpful suggestions.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004.

[RFC5222] Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol", RFC 5222, August 2008.

[RFC5687] Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol: Problem Statement and Requirements", RFC 5687, March 2010.

[RFC5985] Barnes, M., "HTTP-Enabled Location Delivery (HELD)", RFC 5985, September 2010.

[RFC6443] Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling Using Internet Multimedia", RFC 6443, December 2011.

[RFC6881] Rosen, B. and J. Polk, "Best Current Practice for Communications Services in Support of Emergency Calling", BCP 181, RFC 6881, March 2013.

11.2. Informative References

[M493] European Telecommunications Standards Institute, "Functional architecture to support European requirements on emergency caller location determination and transport", ES 203 178, V 1.0.5, December 2014.

[RFC5986] Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)", RFC 5986, September 2010.

[RFC6155] Winterbottom, J., Thomson, M., Tschofenig, H., and R. Barnes, "Use of Device Identity in HTTP-Enabled Location Delivery (HELD)", RFC 6155, March 2011.

[RFC6915] Bellis, R., "Flow Identity Extension for HTTP-Enabled Location Delivery (HELD)", RFC 6915, April 2013.

[RFC7216] Thomson, M. and R. Bellis, "Location Information Server

(LIS) Discovery Using IP Addresses and Reverse DNS",
RFC 7216, April 2014.

Authors' Addresses

James Winterbottom
Winterb Consulting Services
Gwynneville, NSW 2500
AU

Phone: +61 448 266004
Email: a.james.winterbottom@gmail.com

Hannes Tschofenig
Halls in Tirol 6060
Austria

Phone:
Email: Hannes.Tschofenig@gmx.net
URI: http://www.tschofenig.priv.at

Laura Liess
Deutsche Telekom Networks
Deutsche Telekom Allee 7
Darmstadt, Hessen 64295
Germany

Phone:
Email: L.Liess@telekom.de
URI: http://www.telekom.de

ECRIT
Internet-Draft
Intended status: Standards Track
Expires: September 2, 2015

R. Marshall
TCS
M. Linsner
Cisco
D. Stanley
Aruba Networks
March 1, 2015

Indoor Location Mechanisms for Emergency Services
draft-marshall-ecrit-indoor-location-00

Abstract

The application of summoning emergency assistance by using a phone to call 9-1-1 in North America has been ingrained in society for 40+ years. A successful emergency response to a caller in need, is dependent upon the responders receiving accurate location information to effect timely action. Traditional wireline telephony is able to utilize the location of the physical wires as a source of information for caller location, whereas wireless technologies require more exotic mechanisms to locate a 9-1-1 caller.

Mechanisms for locating a cellular caller dialing 9-1-1 is based on 20 year old technology, which was designed for outdoor environments, and does not perform sufficiently when used to locate an emergency caller from within a home or office building environment.

With growing trends in mobile cellular usage, large portions of subscribers are relying solely on their mobile phones to make emergency calls. Emergency response time suffers when that caller is located indoors.

This document defines the problem statement and solutions for expanding the current set of methods used to locate a cellular caller to 9-1-1. The expansion of the methods includes connections to services that are outside the normal administrative domain of the cellular provider, hence both the privacy and security aspects of connecting these systems are taken into consideration.

Status of This Memo

working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 2, 2015.

Copyright Notice

Table of Contents

1. Introduction

Most of the current mechanisms for locating a cellular caller after dialing 9-1-1 in the USA are based on 20 year old technology, and which were designed to locate devices in outdoor environments. So it's not surprising to find out that these mechanism do not always perform very well when used to locate an emergency caller from within a building or enclosed environment. The growing trend of mobile device use for requesting emergency services includes more and more emergency calls being made from inside a structure as well as outside. At the same time, some mobile wireless subscribers are removing their legacy wireline phone service from within their homes, and relying solely on their mobile phones for all calls, including those emergency calls. While replacement of wireline phones in exchange for mobile wireless-only connectivity inside the home is not ubitquitous, it is already apparent that as wireless signal coverage indoors improves, an ever increasing number of emergency calls will be initiated from mobile handsets while inside the home.

Emergency services wireless location technology when first deployed, was implemented as either a network-based or handset-based technology. Handset based implementation required special hardware and/or software in the handset. Network based solutions required additional equipment installed in the service provider's Radio Access Network (RAN), but didn't typically rely on changes to the handset. The methods and protocols used to utilize these technologies were standardized, and for the most part, wholly contained within the control of the mobile operators' networks, and were largely based on standards developed by Telecommunications Industry Association (TIA), 3rd Generation Partnership Program (3GPP), and Open Mobile Alliance (OMA).

Given recent regulatory activities and resultant voluntary carrier-industry agreements around the advancement of indoor location capabilities leveraging new location technologies, there is a need to provide some background as well as a list of assumptions and potential solutions to solve the indoor location challenge. While development of an emergency location architecture and protocols might be the primary focus for North America at the moment, there is also an opportunity to inform a broader (global) audience as to the problem space, since the challenges and benefits are not constrained.

Location information that gets used to dispatch emergency resources to a caller in reporting an emergency, needs to be in the form of a civic street address. Most emergency calls are routed to the appropriate PSAP based on coarse, cell tower location, which is then

followed up with a dynamically measured geographic (i.e., "geo") position estimate (referred to in North America as wireless Phase 2 location). This finer grain position information includes lattitude, longitude, horizontal uncertainty (HUNC) and a probability (confidence). Though the estimated position may be within a few meters to several hundred meters of the caller’s device, this updated position data is not considered by emergency responders to be good enough for direct dispatch since lat/lon coordinates are meaningless without having the ability to plot the position onto a map, or to associate the postion to a civic street address.

Even if geo position information could be accomodated within the emergency center’s dispatch system, it use doesn’t solve indoor mobile use. As a mobile caller moves indoors, traditional outdoor measurment methods become more challenging. What public safety entities require is a "dispatchable location" in the form of a civic street address along with additional data elements, such as building number, room, and floor that will allow emergency responders find the caller.

A dispatchable location is intended as a more complete description of the civic address from where the caller’s device is initiating an emergency call, often including additional data elements such as building, floor, and room, etc. Dispatchable location specifically introduces the z-axis location (i.e., vertical elevation or altitude) component that may be conveyed as floor number or distance as measured above some referenced plane, such as meters above ground or sea level. Since there are many ways to describe elevation information, it will be important to determine the best use when displaying z-axis information.

Facilitating convergence between new indoor location methods and existing emergency location methods will require architectural changes to existing standards in order to utilize technologies and methods that are outside the traditional wireless operators’ controls, but which will still need to be integrated into a wireless emergency E9-1-1 call.

The structure of this document includes terminology, Section 2, followed by a section listing basic assumptions Section 3, an example architecture, Section 13, and security Section 14 and privacy concerns that are involved in obtaining and using indoor location information.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119]

The following terms are defined in this document:

Indoor Location: The type of location information indicative of an end device that is determined from within specific location/ structure, such as within a building.

Outdoor Location: A type of location that is determined representative of a device that is under open sky conditions.

Dispatchable Location: A form of location, either civic or geo, that is considered useful for the dispatching of emergency responders by emergency service personnel. Note: Typically, dispatchable location is used interchangeably with dispatchable address.

Dispatchable Address: This is a sub-type of dispatchable location in general, and by example, may be considered to be "dispatchable" if it is a civic address representing the location of a caller’s mobile phone inside a house, office building, or multi-story apartment building, etc., as long as the address is sufficiently descriptive of the apartment, unit, floor, etc., for emergency response personnel to find the caller.

Dispatchable Position: This is a sub-type of dispatchable location, and is generally considered less popular for dispatch purposes, since responders typically require a street address. An outdoor location technology that provides a position estimate producing a Lat/Lon coordinate pair, or even 3D Lat/Lon/Alt coordinates, for example, might not be considered dispatchable by emergency service personnel, because responders may not have a way of rendering a geographic position even though the coordinates presented might be close to the actual position of the caller.

Network-based location: A target location that is determined by the radio access network and back end systems without requiring any separate interaction from the end device.

Handset-based location: A target location that is determined using techniques that interact with the end device (target) that is being located. That is, the end device plays a part in the location determination process.

User-plane location: Location that is determined using direct data interaction techniques between the end device (target) and a location generator.

Control-plane location: Location that is determined based on data interaction between the end device and the access or application service provider (ASP) location determination equipment through a managed data connection.

Enterprise location: Location information that is representative of data produced from within a managed corporate data network. Examples include an corporate WLAN within an office building, hotel, warehouse, corporate campus etc.

Residential location: Location information representative of data descriptive of a single-family home, multi-tenant apartment or condominium, etc.

Routing location: Location information that is used for the purpose of performing a location-based routing operation. This is usually in reference to coarse location, such as a cell tower civic address or representative lat/lon.

Dispatch location: The location information that is used to dispatch emergency responder resources. This is typically a civic street address.

Augmented Location: Location information that is delivered along with the basic routing and/or dispatch location information. In the case of delivering indoor location along with the normal dispatch location, the indoor location information might be considered augmented location.

Enhanced Location: Location information that is considered to be finer-grained information than the coarse location used for routing. This location information is traditionally in the form of a geographic position estimate in either 2D (Lat/Lon) or 3D (Lat/Lon/Alt).

3. Basic Assumptions for Indoor Location

A short list of assumptions that help define the need for indoor location is listed as follows.

A1. Not all wireless calls need indoor location: Many wireless calls will continue to be initiated outside. For these cases, existing technologies and processes will continue to be used to meet present regulatory requirements.

A2. No single indoor location technology is expected to be optimal for every environment:
Several indoor location technologies exist, each having its own particular set of strengths and weaknesses as to its effectivness in locating a mobile device deep within a building or structure.

A3. Dispatchable location is defined by context: The idea of what dispatchable location is inside one type of building (e.g., high-rise apartment building) may be different for a different type of structure. Also, some emergency response personnel may consider location information as dispatchable depending on the environment reported. For example, geo position information would likely be considered dispatchable by a mountain rescue group or Coast Guard personnel.

A4. Dispatchable location format: The type of location preferred for use in dispatching emergency services by a PSAP is of civic location form (ref. Dispatchable Address). Most PSAPs and emergency responders are only equipped to handle dispatch information of the form of civic street address, as compared to a geo position (e.g., Lat/Lon).

A5. Heightened location components: A geographic position estimate (geo coordinate set, etc.) that is calculated as having a maximum horizontal uncertainty (error) of 50 meters or less, and a vertical uncertainty of 3 meters, as referenced to a specified standard geographic datum.

A6. Dispatchable location vertical component: Dispatchable location includes an indication of vertical height or elevation descriptor if reporting from a significantly elevated position within a structure or building. For example, dispatching emergency resources to a location representing a structure more than 2 floors in height is effective only if the floor number is included. Other units of measurement, such as height above sea level, the ground, or a specified datum are typically considered insufficient for the purposes of dispatching responder resources.

A7. Indoor Location applicability: Dispatchable location is applicable for mobile CMRS emergency calls initiated from an indoor environment.

A8. Applicability of Indoor Location for SMS text-to-9-1-1: Indoor location is not currently applicable for use with SMS text-to-9-1-1, since it is currently not covered by any regulatory or voluntary industry agreement.

A9. Z-axis data: The vertical component of dispatchable location information may include a one or more various representations of elevation data. These could include floor number or altitude in meters above a specified geographic datum.

A10. Integration of vertical information: Mapping servers and protocols (i.e., RFC5222) will need to be changed to support the ability to perform mapping based on the included z-axis data, both for call routing and for dispatching responder resources.

4. Challenges with location indoors

This document describes a few different technologies that are being considered for obtaining accuracte location information from an indoor environment. Regardless of which type of technology, whether considered to be an outdoor technology or an indoor technology, when indoors, both strive to achieve similar goals.

The existing location systems that determine location of E9-1-1 callers while outdoors have not proven as effective in determining location when the caller’s device is deep within a building, parking garage, or other structure. And due to an increasing percentage of emergency calls being made from inside a building using a mobile phone, there is an increased need to be able to adequately locate and dispatch appropriate emergency responder resources to the caller’s actual location. Achieving this feat for calls made indoors is much more challenging than for those calls made outdoors, since the location of the caller is not as obvious to response personnel. As a result, new location solutions are needed in order to provide improved indoor location to support E9-1-1 emergency calls.

(U.S.) Government regulatory test results have taken intitial steps to qualify location technologies [CSRIC test bed], yet none of the technologies tested at that time fully met the target requirement of +/-50 meters across 3 different morphologies [ref. specific CSRIC III results]. The follow on work of CSRIC IV broadened the list of possible location technologies to be considered with regard to achieving more accurate location. The list of candidate technologies is divided into two main categories: namely, what this document refers to as separate outdoor and indoor location technologies.

5. Outdoor Location Technologies

Outdoor location technologies are designed to effectively locate target devices whether indoors or outdoors, with varying levels of measured accuracy. These are location technologies that are naturally deployed outside of any structures, and to a significant extent are able to locate devices within some types of structures as

well, depending on the surrounding environment. Some of these methods include the following:

A-GPS: Assisted Gloal Positioning System

A-GNSS: Assisted Global Navigational Satellite System

O-TDOA: Observed Time Difference Of Arrival

U-TDOA: Observed Time Difference Of Arrival

AFLT: Advanced Forward Link Trilateration

TBS: Terrestrial Beacon System

6. Indoor Location Technologies

Indoor location technologies are designed to effectively locate target devices that are within an indoor environment, usually within a building or structure for which traditional outdoor location methods prove less than optimal, or completely ineffective. These are location technologies that are deployed inside of a structure. Some of these methods include the following:

WPS: Wi-Fi Positioning System

WLAN APs: Wi-Fi Local Area Network Access Points

BLE Beacons: Bluetooth Low Energy Beacons

Small Cells: Small Cells, possibly including microcells, picocells, and femtocells

7. Type of Location Environment

Enterprise Enterprises are typically thought of as organizations that deploy and manage their own data networks for the use of their staff, students, and sometimes on behalf of their customers or visitors. Examples would include corporations, big or small, college campuses, government entities, etc.

Residential Scenarios that include individually deployed data services to a person’s place of residenc, we think of as Residential. Examples of this include single-family, multi-family homes, condominiums, and apartment complexes.

8. Provisioned Location Database

One technique to getting indoor location in a Wi-Fi or BLE laden environment is to provision each Wi-Fi access point or BLE beacon into a database along with a dispatchable location. If the specific Wi-Fi AP(s) and/or BLE beacon(s) that the mobile "sees" can be identified, then those identifiers can be used in a database query to ask for the provisioned location. This database is referred to by public safety as the National Emergency Address Database (NEAD) in the carrier voluntary agreement [provide reference].

Some challenges to this approach include, getting a complete civic location that is representative of the actual address, maintaining the database in terms of contents, and discovering the database identifier (e.g., MAC address) to query in order to obtain the dispatchable location.

The provided location database would need to contain record identifiers and location data. The record key would be MAC address, either a BSSID for a Wi-Fi access point, or UUID/Major/Minor MAC address for a BLE beacon. The database could also contain actual location data relating to a civic street address, along with additional detail information. Alternatively, it may contain a URI (pointer) to a different database that would contain the actual dispatchable location data.

9. Enterprise Provisioned Indoor Location

There are a number of different approaches to determining an indoor location within an enterprise business environment. For emergency calls that can’t be adequately located inside a building, there are ways to leverage other location relevant methods to obtain indoor location.

One technique to obtaining indoor location information within an Enterprise context is to utilize the device location capabilities of enterprise wireless local-area network (WLAN) systems where available. The enterprise WLAN device location entities include Wi-Fi Access Points that are surveyed and provisioned ahead of time into a database for later retrieval. This database could be referred to as a Location Information Server (LIS) as described in the Geopriv Architecture document [IETF RFC6280]. The identifier used in the enterprise WLAN location process is the IEEE 802.11 BSSID, otherwise known as Media Access Control (MAC) address of the Wi-Fi Access Point.

The location information that is manually input into a LIS is retrieved based on a query and the MAC adderess referencing the Wi-Fi

AP or BLE beacon. This query could be direct from a client or from a proxied query, as in the case above. This location is returned to the querying entity and displayed at the PSAP.

10. Enterprise Measured Indoor Location

An enterprise WLAN LIS that is queried with the MAC address of the target device via the HELD interface. The WLAN LIS recognizes the identifier of the device as within its management domain and and returns the associated dispatchable location, and optionally, a geo-coordinate location along with a building floor plan showing the target device's position on the map.

A key part of obtaining location from an Enterprise WLAN LIS is to know which LIS to query. For this we use a WLAN LIS discovery approach based on GIS polygons at the 911SSP. The 911SSP already knows which cell site the emergency call came from. In this way, discovery of which enterprise LIS to query could include a polygon-overlay method to identify connected enterprises with WLANs that reside within the same cell-sector as the caller (cell-sector is a known entity by the cellular network at the time of a call).

As PSAPs move toward NG9-1-1, delivery of rich content such as building floor plans is expected. Even during transition, PSAPs that opt for pre-NG9-1-1 mechanisms to display additional location related data can do so through available tools such as a browser display client.

11. Indoor Location for Residential

Many single family structures, most notably those that are wood frame construction offer limited obstruction to traditional outside location methods, including A-GPS that is used for current E9-1-1 Phase 2 locations. However, even in moderately restrictive environments A-GPS results may not always provide a very precise fix (i.e., low horizontal uncertainty) with the position information, making the resultant system provided search area considerably more challenging than a more precise fix. Dispatchable location, in this case, is intended to provide the civic street address of the home from which the call is being made from, which affords emergency responders with specific address to go to.

It is possible to get multiple location fixes from different system for the same call. This additional information, including both civic street address and geo position information can be used to provide a higher degree of certainty that the information accurately represents the caller's true location. Each of these location data types may or may not be provided by the same location technology.

Like enterprise solutions that rely on Wi-Fi radio signals to correlate or calculate location results, residential location solutions exist that leverage Wi-Fi signals from one or more access points or beacons within a residence. In the case of a residential Wi-Fi access point, the civic street address of the residence may be able to be provisioned ahead of time in order to provide at call time during an emergency situation. The challenge to using this data is the question of how it can be trusted.

Besides single family residential structures, a more challenging residential environment includes that of a multi-floor, multi-tenant apartment building that may not have consistent deployment of Wi-Fi or Bluetooth beacons, and where A-GPS or other outside location technologies may not be effective.

12. Obtaining an Identifier

In order to use a identifier that is designed to get indoor location, it must first become available to the location functions that need to use it within the network. Examples of identifiers include a MAC address of a target mobile device, a BSSID of a Wi-Fi Access Point, or a BLE UUID/Major/Minor identifier. There are several approaches to consider in seeking to obtain an identifier.

Provisioned/Associated: If we know the identifier of a mobile handset, AP, or BLE beacon ahead of time, then it can be mapped to a mobile directory number. The call processing system then maps the incoming Mobile Directory Number (MDN) to the stored MAC address. The MAC address is then used to query the location generator for location. While this approach may be okay for demo purposes, it is not feasible for a working system.

Another method for discovery of a device location while indoors is to gather ’beacon’ identifiers the calling device can see and reference a location database of known ’beacons’. The term ’beacon’ in this context includes IEEE 802.11 access points (AP) and/or a Bluetooth 4.0 Low-Energy Beacon (BLE). The beacon identifiers gathered by the calling device would include:

Handset Provided In-band: When a handset makes an emergency call, it is possible to enable the handset to scan and collect all the Wi-Fi and BLE identifiers that it sees, along with other measurement data and include those data with the emergency call. This capability will be more easily integrated into packet based access networks that use SIP, for example, than for legacy circuit-switched access networks, which would require significant standards modification. Some newer standards, such as OMA SUPL

(v2.0.2) protocol, support the return of these types of data extensions.

Handset Provided Out-of-band: An application can be installed onto a handset that can then be invoked from a direct IP connection from a trusted 911SSP network once the emergency call is initiated. The handset then scans and collects all the Wi-Fi and BLE identifiers that it sees, along with other measurement data and sends those data back to the trusted 911SSP to be matched up to the ongoing emergency call.

13. Indoor Location Example Use Case

Indoor location information is shown as augmenting the existing emergency location data that is delivered during the an emergency call scenario. In this use case, a mobile operator recognizes a caller on their network has dialed 9-1-1 and forwards the call to the designated 9-1-1 system service provider (911SSP). The MAC address of a close by Wi-Fi AP that happens to have it’s location already entered into a provisioned location database is discovered [hand waiving here] and delivered to the 911SSP which then initiates a query to the provisioned location database requesting the provisioned dispatchable address.

```
      Information    +-----------------+
          |(1)       |Internet         |            +---------+
          v          |Access           |            |         |
     +-----------+   |Provider         |            | Mapping |
     |           |   | (3)             |            | Service |
     | Emergency |<--+-----------------+----------->|         |
     | Caller    |   | (2,a) +---------+---+        +---------+
     |           |<--+------>|         |   |             ^
     |           |   |       |         |   |  +-------+  |
     +-----------+   |       |     LIS |   |  | AP/BLE|  |
          ^          +-------+---------+   |  | Data  |  |
          |                  |             |  | Store |  |
          |                  +-------------+  +-------+  |
          |                      ^     ^          ^      |
          |                      |     | (c,e)    | (d)  |
          |               (5,a)  |     v          v      |
          |                      |  +----------------+   |
          |                      |  |    Augmented   |   |
          |                      |  |    Location    |   |
          |                      |  |    Server      |   |
          |            +---------+-----------+       |   |
          |            |         |  |        |       |   |
          |            |         |  +----------------+   |
          |            |         |     ^     |    ^      |
          |            |         |     |(b,f)|    | (g)  |
          |            |         v     v     |    |      |
          |            |    +------------+   |    |      |
          |  (4)       |    |            |   |    |      |
          +------------+--->|    ESRP    |<--+----+------+
          |            |    |            |   |    |   (6)
          |            |    +------------+   |    |
          |            |          ^          |    v
          |            |      (7) |          |  +----+--+
          |    (8)     |          +------------>|       |
          +------------+------------------------>| PSAP  |
                       |                      |  |       |
                       |Application/          |  +----+--+
                       |Voice                 |
                       |Service               |
                       |Provider              |
                       +----------------------+
```

The diagram shows new interaction between the entities involved in the call in order to get indoor location. There are a number of different deployment models possible, so this document will provide a single example only.

Even through the Application/Voice Service Provider could be the same entity as the Internet Access Provider, this figure shows them as separate boxes. It does however show that the Location Information Server may be deployed within the Internet Access Provider's control, or may be outside of it.

Likewise, the Augmented Location Server - useful for getting Indoor Location information in some morphologies, could also be deployed within the Application/Voice Service Provider, or without. There is no requirement either way. Moreover, we consider but don't show the enterprise or residential scenarios where end systems might act as their own ASP/VSP.

Various interaction scenarios between the entities for emergency call initiation and processing are described in [ref. RFC5012]. The below description highlights only the augmented location interaction:

a. Coarse Location information might be available to the end host directly, obtainable via the Internet Access Provider's LIS, or retrievable by the ESRP during call routing.

b. During call routing, the ESRP may ask the Augmented Location Server for additional location, namely Indoor Location either because of call marking, or by some rule, in which case it queries the Augmented Location Server.

c. The Augmented Location Server discovers the MAC address of the device currently making an emergency call and maps it to the device's existing MDN. The MAC address may be obtained through user plane query techniques as implied here, or via some other method [ref. section MAC-discovery-TBD].

d. Having obtained the MAC address of the target device, the Augmented Location Server uses it to perform a location query a public Wi-Fi Access Point/Bluetooth beacon database. Note: Enterprise WLAN query for Wi-Fi location not shown.

e. The resulting data returned from the Enterprise WLAN location server or AP/BLE Data Store can be either of the type of civic address or geographic position, either in 2D or 3D format. If the returned information is geographic, it will either return a measured, surveyed, or estimated coordinate set, including some indication of error (uncertainty and confidence). If the ALS returns a civic address, it will be in the form of a PIDF-LO, and MUST indicate any elevation infomation, such as floor number, especially important if the actual location where the call is coming from is a multi-story building.

f. The ALS then makes this information available to the ESRP either in by-value or by-reference format, supplying a generated URL if by-reference.

g. The augmented indoor location gets sent to the PSAP, again by-value or by-reference. If a URL is provided to the PSAP, the PSAP will dereference the augmented location information and get back the indoor location information by-value.

14. Security Considerations

There are two glaring security issues when locating a caller to emergency services.

1. The privacy of the caller’s location data is of the utmost importance to protect. Hence, any mechanism for the discovery of the caller’s location and the transport of the discovered data MUST be protected by strong authentication and encryption. Any method or protocol that is unique to emergency calls that could be identified by monitoring uncrypted wireless networks MUST NOT be used.

2. It is the utmost importance to protect the owners of enterprise WLANs. These networks are the lifeblood of communications within a business entity. At the same time, enterprises have a strong desire to protect human life for employees, visitors, and customers while on enterprise property. Any connection to the enterprise LIS from the cellular network must utilize strong encryption and strong authentication. The nature of the connection is very low traffic, hence it is advised to utilize a keep-alive method and accounting method with alarming on each so any failure in the connection can be rectified in a reasonable timeframe. The privacy of location data must be protected and only shared with the CMRS provider during an emergency call. In the US, CMRS providers are constrained by policy to perform device location queries only during a 9-1-1 call. The location data must be protected from the discovery method to the PSAP, requiring both data integrity and data security end-to-end.

15. IANA Considerations

There are currently no IANA considerations.

16. Acknowledgements

17. Changes from Previous Versions

17.1. Changes from draft-

- o
- o

18. References

18.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.

[RFC6280] Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", BCP 160, RFC 6280, July 2011.

18.2. Informative References

[RFC5222] Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol", RFC 5222, August 2008.

Authors' Addresses

Roger Marshall
TeleCommunication Systems, Inc.
2401 Elliott Avenue
2nd Floor
Seattle, WA 98121
US

Phone: +1 206 792 2424
Email: rmarshall@telecomsys.com
URI: http://www.telecomsys.com

Marc Linsner
Cisco Systems
Marco Island, FL 34145
US

Email: marc.linsner@cisco.com
URI: http://www.cisco.com

Dorothy Stanley
Aruba Networks
1322 Crossman Ave
Sunnyvale, CA
US

Phone: 630-363-1389
Email: dstanley@arubanetworks.com
URI: http://www.arubanetworks.com