Internet Engineering Task Force (IETF)
Request for Comments: 8147
Category: Standards Track
ISSN: 2070-1721

R. Gellens
Core Technology Consulting
H. Tschofenig
Individual

May 2017

Next-Generation Pan-European eCall

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, providing real-time communications and an integrated set of related data.

This document also registers MIME media types and an Emergency Call Data Type for the eCall vehicle data and metadata/control data, and an INFO package to enable carrying this data in SIP INFO requests.

Although this specification is designed to meet the requirements of next-generation Pan-European eCall (NG-eCall), it is specified generically such that the technology can be reused or extended to suit requirements across jurisdictions.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8147.

Table of Contents

1. 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 (condition) of the vehicle, and the location of the vehicle and to have a voice communications 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 a compliant in-vehicle system (IVS) in new vehicles and the deployment of eCall in the European Member States in the very near future. Other regions are developing eCall-compatible systems.

The Pan-European eCall system is a standardized and mandated mechanism for emergency calls by vehicles, providing a voice channel and transmission of data. eCall establishes procedures for such calls to be placed by in-vehicle systems, recognized and processed by the mobile network, and routed to a specialized Public Safety Answering Point (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 can be either user initiated or automatically triggered. Automatically triggered eCalls indicate a car crash or some other serious incident. Manually triggered eCalls might be reports of witnessed crashes or serious hazards, a request for medical assistance, etc. PSAPs might apply specific operational handling to manual and automatic eCalls.

Legacy eCall is standardized (by 3GPP [SDO-3GPP] and the European Committee for Standardization (CEN) [CEN]) as a 3GPP circuit-switched call over Global System for Mobile communications (GSM) (2G) or Universal Mobile Telecommunications System (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). NG-eCall moves from circuit switched to all-IP and carries the vehicle data and eCall signaling as additional data carried with the call. This document describes how IETF mechanisms for IP-based emergency calls (including [RFC6443] and [RFC7852]) are used to provide the signaling and data exchange of the next generation of Pan-European eCall.

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. The recommendations include the use of 3GPP Internet Multimedia System (IMS) emergency calling with additional elements identifying the call as an eCall and as carrying eCall data and mechanisms for carrying the data and eCall signaling. 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 NG-eCall, legacy eCall, or both. The issues of migration and co-existence during the transition period are outside the scope of this document.

This document indicates how to use IP-based emergency services mechanisms to support NG-eCall.

This document also registers MIME media types and Emergency Call Data Types for the eCall vehicle data (MSD) and metadata/control data, and an INFO package to enable carrying this data in SIP INFO requests.

The MSD is carried in the MIME type application/ EmergencyCallData.eCall.MSD and the metadata/control block is carried in the MIME type application/EmergencyCallData.Control+xml (both of which are registered in Section 14). An INFO package is defined (in

Section 14.9) to enable these MIME types to be carried in SIP INFO requests, per [RFC6086].

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].

This document reuses terminology defined in Section 3 of [RFC5012].

Additionally, we use the following abbreviations:

3GPP: 3rd Generation Partnership Project

CEN: European Committee for Standardization

EENA: European Emergency Number Association

ESInet: Emergency Services IP network

IMS: IP Multimedia Subsystem

IVS: In-Vehicle System

MNO: Mobile Network Operator

MSD: Minimum Set of Data

PSAP: Public Safety Answering Point

3. Document Scope

This document is focused on the signaling, data exchange, and protocol needs of NG-eCall (also referred to as packet-switched eCall or 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 [TS23.167]).

Although this specification is designed to meet the requirements of Pan-European NG-eCall, it is specified generically such that the technology can be reused or extended to suit requirements across jurisdictions (see, e.g., [RFC8148]), and extension points are provided to facilitate this.

Note that vehicles designed for multiple regions might need to support eCall and other Advanced Automatic Crash Notification (AACN) systems (such as described in [RFC8148]), but this is out of scope of this document.

4. eCall Requirements

eCall requirements are specified by CEN in [EN_16072] and by 3GPP in [TS22.101], Section 10.7 and Annex A.27, and [TS24.229], Section 4.7.6. Requirements specific to vehicle data are contained in EN 15722 [MSD].

5. Vehicle Data

Pan-European eCall provides a standardized and mandated set of vehicle-related data (including VIN, vehicle type, propulsion type, current and optionally previous location coordinates, and the number of occupants) known as the Minimum Set of Data (MSD). CEN has specified this data in EN 15722 [MSD], along with both ASN.1 and XML encodings. Both circuit-switched eCall and this document use the ASN.1 PER encoding, which is specified in Annex A of EN 15722 [MSD] (the XML encoding specified in Annex C is not used in this document, per 3GPP [SDO-3GPP]).

This document registers the application/EmergencyCallData.eCall.MSD MIME media type to enable the MSD to be carried in SIP. As an ASN.1 PER-encoded object, the data is binary and transported using binary content transfer encoding within SIP messages. This document also adds "eCall.MSD" to the "Emergency Call Data Types" registry to enable the MSD to be recognized as such in a SIP-based eCall emergency call. (See [RFC7852] for more information about the registry and how it is used.)

See Section 6 for a discussion of how the MSD vehicle data is conveyed in an NG-eCall.

6. Data Transport

[RFC7852] establishes a general mechanism for conveying blocks of data within a SIP emergency call. This document makes use of that mechanism to include vehicle data (the MSD; see Section 5) and metadata/control information (see Section 9) within SIP messages.

This document also registers an INFO package (in Section 14.9) to enable eCall-related data blocks to be carried in SIP INFO requests (per [RFC6086], new INFO usages require the definition of an INFO package).

Note that if other data sets need to be transmitted in the future, the appropriate signaling mechanism for such data needs to be evaluated, including factors such as the size and frequency of such data.

An IVS transmits an MSD (see Section 5) by encoding it per Annex A of EN 15722 [MSD] and including it as a MIME body part within a SIP message per [RFC7852]. The body part is identified by its MIME media type (application/EmergencyCallData.eCall.MSD) in the Content-Type header field of the body part. The body part is assigned a unique identifier that is listed in a Content-ID header field in the body part. The SIP message is marked as containing the MSD by adding (or appending to) a Call-Info header field at the top level of the SIP message. This Call-Info header field contains a Content Identifier (CID) URL referencing the body part's unique identifier and a "purpose" parameter identifying the data as the eCall MSD per the entry in the "Emergency Call Data Types" registry; the "purpose" parameter's value is "EmergencyCallData.eCall.MSD". Per [RFC6086], an MSD is carried in a SIP INFO request by using the INFO package defined in Section 14.9.

A PSAP or IVS transmits a metadata/control object (see Section 9) by encoding it per the description in this document and including it within a SIP message as a MIME body part per [RFC7852]. The body part is identified by its MIME media type (application/ EmergencyCallData.Control+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 SIP message is marked as containing the metadata/control object by adding (or appending to) a Call-Info header field at the top level of the SIP message. This Call-Info header field contains a CID URL referencing the body part's unique identifier and a "purpose" parameter identifying the data as an eCall metadata/control block per the entry in the "Emergency Call Data Types" registry; the "purpose" parameter's value is "EmergencyCallData.Control". Per [RFC6086], a metadata/control object is carried in a SIP INFO request by using the INFO package defined in Section 14.9.

An MSD or a metadata/control block is always enclosed in a multipart body part (even if it would otherwise be the only body part in the SIP message).

A body part containing an MSD or metadata/control object has a Content-Disposition header field value containing "By-Reference".

An IVS initiating an NG-eCall includes an MSD as a body part within the initial INVITE and optionally also includes a metadata/control object informing the PSAP of its capabilities as another body part. The MSD body part (and metadata/control and Presence Information Data Format Location Object (PIDF-LO) body parts, if included) have a Content-Disposition header field with the value "By-Reference; handling=optional". Specifying "handling=optional" prevents the SIP INVITE request from being rejected if it is processed by a legacy element (e.g., a gateway between SIP and circuit-switched environments) that does not understand the MSD (or metadata/control object or PIDF-LO).

The PSAP creates a metadata/control object acknowledging receipt of the MSD and includes it as a body part within the SIP final response to the SIP INVITE request per [RFC7852]. A metadata/control object is not included in provisional (e.g., 180) responses.

A PSAP is able to reject a call while indicating that it is aware of the situation by including a metadata/control object acknowledging the MSD and containing "received=true" within a final response using SIP response code 600 (Busy Everywhere), 486 (Busy Here), or 603 (Decline), per [RFC7852].

If the IVS receives an acknowledgment for an MSD containing "received=false", this indicates that the PSAP was unable to properly decode or process the MSD. The IVS action is not defined (e.g., it might only log an error). Since the PSAP is able to request an updated MSD during the call, if an initial MSD is unsatisfactory in any way, the PSAP can choose to request another one.

A PSAP can request that the vehicle send an updated MSD during a call (e.g., upon manual request of the PSAP call taker who suspects the vehicle state may have changed). To do so, the PSAP creates a metadata/control object requesting an MSD and includes it within a SIP INFO request sent within the dialog. The IVS then includes an updated MSD within a SIP INFO request and sends it within the dialog. If the IVS is unable to send an MSD, it instead sends a metadata/control object acknowledging the request, containing an <actionResult> element with a "success" parameter set to "false" and a "reason" parameter (and optionally a "details" parameter) indicating why the request could not be accomplished. Per [RFC6086], metadata/control objects and MSDs are sent using the INFO package defined in Section 14.9. In addition, to align with how an MSD or metadata/control block is transmitted in a SIP message other than an INFO request, a Call-Info header field is included in the SIP INFO

request to reference the MSD or metadata/control block per [RFC7852]. See Section 14.9 for information about the use of SIP INFO requests to carry data within an eCall.

The IVS is not expected to send an unsolicited MSD after the initial INVITE.

This document does not mandate support for the data blocks defined in [RFC7852].

7. Call Setup

In a circuit-switched eCall, the IVS places a special form of a 112 emergency call, which carries an 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, and vehicle data is transmitted to the PSAP via the eCall in-band modem (in the voice channel).

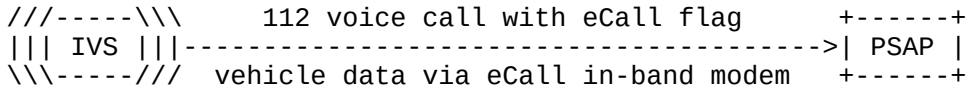

Figure 1: Circuit-Switched eCall

For NG-eCall, the IVS establishes an emergency call using a Request-URI indicating a manual or automatic eCall; the MNO (or ESInet) recognizes the eCall URN and routes the call to an NG-eCall-capable PSAP; and the PSAP interprets the vehicle data sent with the call and makes it available to the call taker.

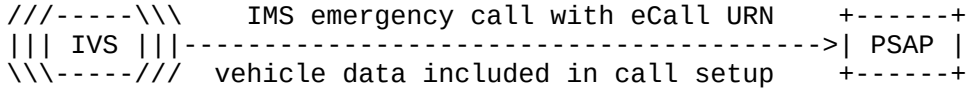

Figure 2: NG-eCall

See Section 6 for information on how the MSD is transported within an NG-eCall.

This document adds 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 might be subject to different treatment, depending on policy). The two service URNs are: urn:service:sos.ecall.automatic and urn:service:sos.ecall.manual, which request resources associated with an emergency call placed by

an in-vehicle system, carrying a standardized set of data related to the vehicle and incident. These are registered in Section 14.2.

Call routing is outside the scope of this document.

8. Test Calls

eCall requires the ability to place test calls (see [TS22.101], clause 10.7 and [EN_16062], clause 7.2.2). 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 specific handling of test eCalls is outside the scope of this document; typically, the test call facility allows the IVS or user to verify that an eCall can be successfully established with voice communication. The IVS might also be able to 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. The "test" service URN is defined in [RFC6881].

This document specifies "urn:service:test.sos.ecall" for eCall test calls. This is registered in Section 14.2.

The circuit-switched eCall test call facility is a non-emergency number, so it does not get treated as an emergency call. For NG-eCall, MNOs, emergency authorities, and PSAPs can determine how to treat a vehicle call requesting the "test" service URN so that the desired functionality is tested, but this is outside the scope of this document.

9. The Metadata/Control Object

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 can initiate a request for a new MSD to see if there have been changes in the vehicle’s state, such as location, direction, or number of fastened seat belts).

This document defines a block of metadata/control data as an XML structure containing elements used for eCall and other related emergency call systems and extension points. (This metadata/control block is in effect a high-level protocol between the PSAP and IVS.)

This document registers the application/EmergencyCallData.Control+xml MIME media type to enable the metadata/control data to be carried in SIP. This document also adds "Control" to the "Emergency Call Data Types" registry to enable the metadata/control block to be recognized

as such in a SIP-based eCall emergency call. (See [RFC7852] for more information about the registry and how it is used.)

See Section 6 for a discussion of how the metadata/control data is conveyed in an NG-eCall.

When the PSAP sends a metadata/control block in response to data sent by the IVS in a SIP request other than INFO (e.g., the MSD in the initial INVITE), the metadata/control block is sent in the SIP response to that request (e.g., the response to the INVITE request). When the PSAP sends a control block in other circumstances (e.g., mid call), the control block is transmitted from the PSAP to the IVS in a SIP INFO request within the established dialog. The IVS sends the requested data (the MSD) in a new SIP INFO request (per [RFC6086]). This mechanism flexibly allows the PSAP to send eCall-specific data to the IVS and the IVS to respond. SIP INFO requests are sent using an appropriate INFO package. See Section 6 for more information on sending a metadata/control block within a SIP message. See Section 14.9 for information about the use of SIP INFO requests to carry data within an eCall.

When the IVS includes an unsolicited MSD in a SIP request (e.g., the initial INVITE), the PSAP sends a metadata/control block indicating successful/unsuccessful receipt of the MSD in the SIP response to the request. This also informs the IVS that an NG-eCall is in operation. If the IVS receives a SIP final response without the metadata/control block, it indicates that the SIP dialog is not an NG-eCall (e.g., some part of the call is being handled as a legacy call). When the IVS sends a solicited MSD (e.g., in a SIP INFO request sent following receipt of a SIP INFO request containing a metadata/control block requesting an MSD), the PSAP does not send a metadata/control block indicating successful or unsuccessful receipt of the MSD. (Normal SIP retransmission handles non-receipt of requested data; note that, per [RFC6086], a 200 OK response to a SIP INFO request indicates only that the receiver has successfully received and accepted the SIP INFO request, and it says nothing about the acceptability of the payload.) If the IVS receives a request to send an MSD but it is unable to do so for any reason, the IVS instead sends a metadata/control object acknowledging the request, containing an <actionResult> element with a "success" parameter set to "false" and a "reason" parameter (and optionally a "details" parameter) indicating why the request could not be accomplished.

This provides flexibility to handle various circumstances. For example, if a PSAP is unable to accept an eCall (e.g., due to overload or too many calls from the same location), it can reject the INVITE. Since a metadata/control object is also included in the SIP response that rejects the call, the IVS knows if the PSAP received

the MSD and can inform the vehicle occupants that the PSAP successfully received the vehicle location and information but can't talk to the occupants at that time. Especially for SIP response codes that indicate an inability to conduct a call (as opposed to a technical inability to process the request), the IVS can also determine that the call was successful on a technical level (e.g., not helpful to retry as circuit switched). (Note that there could be edge cases where the PSAP response is not received by the IVS, e.g., if an intermediary sends a CANCEL, and an error response is forwarded towards the IVS before the error response from the PSAP is received, the response will be dropped, but these are unlikely to occur here.)

The metadata/control block is carried in the MIME type application/EmergencyCallData.Control+xml.

The metadata/control block is designed for use with Pan-European eCall and also eCall-like systems (i.e., in other regions), and it has extension points. Note that eCall-like systems might define their own vehicle data blocks and might need to register a new INFO package to accommodate the new data MIME media type and the metadata/control object.

9.1. The Control Block

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

ack	Acknowledges receipt of data or a request.
capabilities	Used in a control block sent from the IVS to the PSAP (e.g., in the initial INVITE) to inform the PSAP of the vehicle capabilities. Child elements contain all actions and data types supported by the vehicle. It is OPTIONAL for the IVS to send this block. Omitting the block indicates that the IVS supports only the mandatory functionality defined in this document.
request	Used in a control block sent by the PSAP to the IVS to request the vehicle to perform an action.

The <ack> element indicates the object being acknowledged and reports success or failure.

The <request> element contains attributes to indicate the request and to supply related information. The "action" attribute is mandatory and indicates the specific action. An IANA registry is created in Section 14.8.1 to contain the allowed values.

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

9.1.1. The <ack> Element

The <ack> element acknowledges receipt of an eCall data object or request. An <ack> element references the Content-ID of the object being acknowledged. The PSAP MUST send an <ack> element acknowledging receipt of an unsolicited MSD (e.g., sent by the IVS in the INVITE); this <ack> element indicates if the PSAP considers the MSD successfully received or not. An <ack> element is not sent for a <capabilities> element.

9.1.1.1. Attributes of the <ack> Element

The <ack> element has the following attributes:

Name:	ref
Usage:	Mandatory
Type:	anyURI
Direction:	Sent in either direction
Description:	References the Content-ID of the body part being acknowledged.
Example:	<ack received="true" ref="1234567890@atlanta.example.com"/>

Name:	received
Usage:	Conditional: mandatory in an <ack> element sent by a PSAP
Type:	boolean
Direction:	In this document, sent from the PSAP to the IVS
Description:	Indicates if the referenced object was considered successfully received or not.
Example:	<ack received="true" ref="1234567890@atlanta.example.com"/>

9.1.1.2. Child Element of the <ack> Element

For extensibility, the <ack> element has the following child element:

Name: actionResult
Usage: Optional
Direction: Sent from the IVS to the PSAP
Description: An <actionResult> element indicates the result of an action (other than a successfully executed "send-data" action). The <ack> element contains an <actionResult> element for each <request> element that is not a successfully executed "send-data" action. The <actionResult> element 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 14.8.2. The initial values are: damaged (required components are damaged), data-unsupported (the data item referenced in a "send-data" request is not supported), security-failure (the authenticity of the request or the authority of the requestor could not be verified), unable (a generic error for use when no other code is appropriate), and unsupported (the "action" value is not supported).

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. This is intended for internal use and troubleshooting, not for display to vehicle occupants.

9.1.1.3. Example of the <ack> Element

```
<?xml version="1.0" encoding="UTF-8"?>
<EmergencyCallData.Control
    xmlns="urn:ietf:params:xml:ns:EmergencyCallData:control"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<ack received="true" ref="1234567890@atlanta.example.com"/>

</EmergencyCallData.Control>
```

Figure 3: <ack> Example from PSAP to IVS

9.1.2. The <capabilities> Element

The <capabilities> element is transmitted by the IVS to indicate its capabilities to the PSAP. No attributes for this element are currently defined. There is one child element defined.

9.1.2.1. Child Element of the <capabilities> Element

The <capabilities> element has the following child element:

Name: request
Usage: Mandatory
Description: The <capabilities> element contains a <request> child element per action supported by the vehicle.

Example:

```
<capabilities>

   <request action="send-data" supported-values="eCall.MSD" />

</capabilities>
```

It is OPTIONAL for the IVS to support the <capabilities> element. If the IVS does not send a <capabilities> element, this indicates that the only <request> action supported by the IVS is "send-data" with "datatype" set to "eCall.MSD".

9.1.2.2. Example of the <capabilities> Element

```
<?xml version="1.0" encoding="UTF-8"?>
<EmergencyCallData.Control
    xmlns="urn:ietf:params:xml:ns:EmergencyCallData:control">

<capabilities>
    <request action="send-data" supported-values="eCall.MSD"/>
</capabilities>

</EmergencyCallData.Control>
```

Figure 4: <capabilities> Element Example

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. It allows the PSAP to request that the IVS perform an action. The only action that MUST be supported is to send an MSD. The attributes and child elements are defined as follows.

9.1.3.1. Attributes of the <request> Element

The <request> element has the following attributes:

Name: action
Usage: Mandatory
Type: token
Direction: Sent in either direction
Description: Identifies the action that the vehicle is requested to perform (in a <request> element within a <capabilities> element; indicates an action that the vehicle is capable of performing). An IANA registry is established in Section 14.8.1 to contain the allowed values.
Example: action="send-data"

Name: int-id
Usage: Conditional
Type: unsignedInt
Direction: Sent in either direction
Description: Defined for extensibility. Documents that make use of it are expected to explain when it is required and how it is used.
Example: int-id="3"

Name: persistence
Usage: Optional
Type: duration
Direction: Sent in either direction

Description: Defined for extensibility. Specifies how long to carry on the specified action. If absent, the default is for the duration of the call.
Example: persistence="PT1H"

Name: datatype
Usage: Conditional
Type: token
Direction: Sent in either direction
Description: Mandatory with a "send-data" action within a <request> element that is not within a <capabilities> element. 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 IANA's "Emergency Call Data Types" registry established in [RFC7852]. Only the "eCall.MSD" value is mandatory to support.
Example: datatype="eCall.MSD"

Name: supported-values
Usage: Conditional
Type: string
Direction: Sent from the IVS to the PSAP
Description: Defined for extensibility. Used in a <request> element that is a child of a <capability> element, this attribute lists all supported values of the action type. Permitted values depend on the action value. Multiple values are separated with a semicolon. White space is ignored. Documents that make use of it are expected to explain when it is required, the permitted values, and how it is used.

Name: requested-state
Usage: Conditional
Type: token
Direction: Sent from the PSAP to the IVS
Description: Defined for extension. Indicates the requested state of an element associated with the request type. Permitted values depend on the request type. Documents that make use of it are expected to explain when it is required, the permitted values, and how it is used.

Name: element-id
Usage: Conditional
Type: token
Direction: Sent from the PSAP to the IVS
Description: Defined for extension. Identifies the element to be acted on. Permitted values depend on the request type. Documents that make use of it are expected to explain when it is required, the permitted values, and how it is used.

9.1.3.2. Child Element of the <request> Element

For extensibility, the <request> element has the following child element:

Name: text
Usage: Optional
Type: string
Direction: Sent from the PSAP to the IVS
Description: Defined for extension.

9.1.3.3. Request Example

```
<?xml version="1.0" encoding="UTF-8"?>
<EmergencyCallData.Control
    xmlns="urn:ietf:params:xml:ns:EmergencyCallData:control">

<request action="send-data" datatype="eCall.MSD"/>

</EmergencyCallData.Control>
```

Figure 5: <request> Element Example

10. Examples

Figure 6 illustrates 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, which 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, an illustration of which would be identical to the one below except without an ESInet or ESRP.

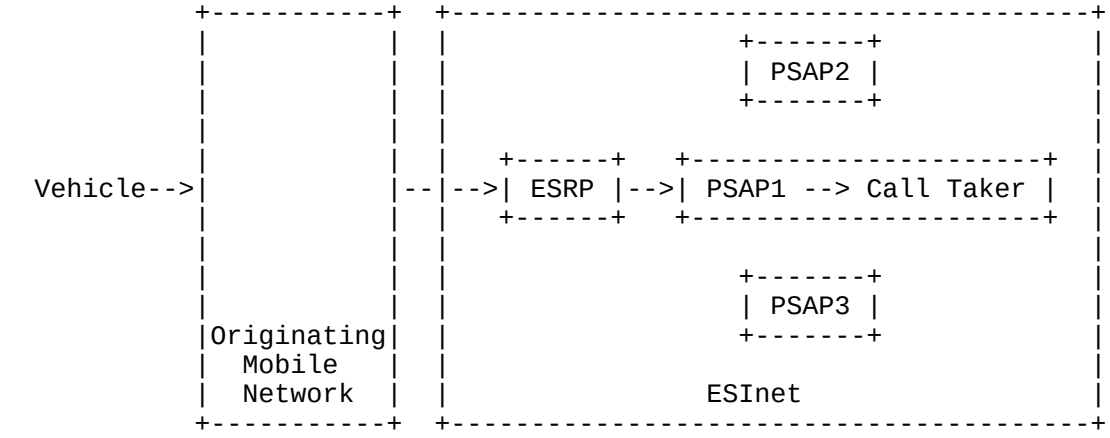

Figure 6: Example of NG-eCall Message Flow

Figure 7 illustrates an eCall call flow with a mid-call PSAP request for an updated MSD. The call flow shows the IVS initiating an emergency call, including the MSD in the INVITE. The PSAP includes in the 200 OK response a metadata/control object acknowledging receipt of the MSD. During the call, the PSAP sends a request for an MSD in an INFO request. The IVS sends the requested MSD in a new INFO request.

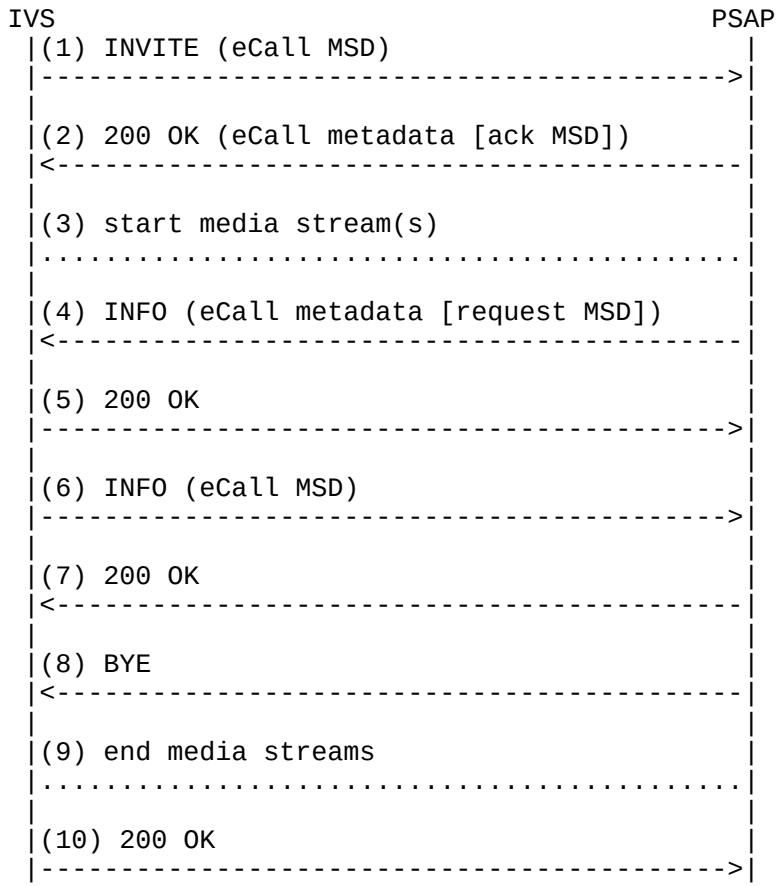

Figure 7: NG-eCall Call Flow Illustration

Figure 8 illustrates a SIP eCall INVITE request containing an MSD. For simplicity, the example does not show all SIP headers, nor the Session Description Protocol (SDP) contents, nor does it show any additional data blocks added by the IVS or the originating mobile network. Because the MSD is encoded in ASN.1 PER, which is a binary encoding, its contents cannot be included in a text document.

```
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,
        application/EmergencyCallData.Control+xml
CSeq: 31862 INVITE
Recv-Info: EmergencyCallData.eCall.MSD
Allow: INVITE, ACK, PRACK, INFO, OPTIONS, CANCEL, REFER, BYE,
       SUBSCRIBE, NOTIFY, UPDATE
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@example.com>
Content-Disposition: by-reference;handling=optional

      ...PIDF-LO goes here...

--boundary1
Content-Type: application/EmergencyCallData.eCall.MSD
Content-ID: <1234567890@atlanta.example.com>
Content-Disposition: by-reference;handling=optional

     ...MSD in ASN.1 PER encoding goes here...

 --boundary1--
```

Figure 8: SIP NG-eCall INVITE

Continuing the example, Figure 9 illustrates a SIP 200 OK response to the INVITE request of Figure 8, containing a metadata/control block acknowledging successful receipt of the eCall MSD. (For simplicity, the example does not show all SIP headers.)

```
SIP/2.0 200 OK
To: urn:service:sos.ecall.automatic;tag=8gydfe65t0
From: <sip:+13145551111@example.com>;tag=9fxced76sl
Call-ID: 3848276298220188511@atlanta.example.com
Call-Info: <cid:2345678901@atlanta.example.com>;
           purpose=EmergencyCallData.Control
Accept: application/sdp, application/pidf+xml,
        application/EmergencyCallData.Control+xml,
        application/EmergencyCallData.eCall.MSD
CSeq: 31862 INVITE
Recv-Info: EmergencyCallData.eCall.MSD
Allow: INVITE, ACK, PRACK, INFO, OPTIONS, CANCEL, REFER, BYE,
       SUBSCRIBE, NOTIFY, UPDATE
Content-Type: multipart/mixed; boundary=boundaryX
Content-Length: ...

--boundaryX
Content-Type: application/sdp

     ...Session Description Protocol (SDP) goes here...

--boundaryX
Content-Type: application/EmergencyCallData.Control+xml
Content-ID: <2345678901@atlanta.example.com>
Content-Disposition: by-reference

<?xml version="1.0" encoding="UTF-8"?>
<EmergencyCallData.Control
    xmlns="urn:ietf:params:xml:ns:EmergencyCallData:control">

<ack received="true" ref="1234567890@atlanta.example.com"/>
</EmergencyCallData.Control>

--boundaryX--
```

Figure 9: 200 OK Response to INVITE

Figure 10 illustrates a SIP INFO request containing a metadata/ control block requesting an eCall MSD. (For simplicity, the example does not show all SIP headers.)

```
INFO sip:+13145551111@example.com SIP/2.0
To: <sip:+13145551111@example.com>;tag=9fxced76sl
From: Exemplar PSAP <urn:service:sos.ecall.automatic>;tag=8gydfe65t0
Call-ID: 3848276298220188511@atlanta.example.com
Call-Info: <cid:3456789012@atlanta.example.com>;
           purpose=EmergencyCallData.Control
CSeq: 41862 INFO
Info-Package: EmergencyCallData.eCall.MSD
Allow: INVITE, ACK, PRACK, INFO, OPTIONS, CANCEL, REFER, BYE,
       SUBSCRIBE, NOTIFY, UPDATE
Content-Type: multipart/mixed; boundary=boundaryZZZ
Content-Disposition: Info-Package
Content-Length: ...

--boundaryZZZ
Content-Disposition: by-reference
Content-Type: application/EmergencyCallData.Control+xml
Content-ID: <3456789012@atlanta.example.com>

<?xml version="1.0" encoding="UTF-8"?>
<EmergencyCallData.Control
    xmlns="urn:ietf:params:xml:ns:EmergencyCallData:control">

<request action="send-data" datatype="eCall.MSD"/>

</EmergencyCallData.Control>
 --boundaryZZZ--
```

Figure 10: INFO Requesting MSD

Figure 11 illustrates a SIP INFO request containing an MSD. For simplicity, the example does not show all SIP headers. Because the MSD is encoded in ASN.1 PER, which is a binary encoding, its contents cannot be included in a text document.

```
INFO urn:service:sos.ecall.automatic SIP/2.0
To: urn:service:sos.ecall.automatic;tag=8gydfe65t0
From: <sip:+13145551111@example.com>;tag=9fxced76sl
Call-ID: 3848276298220188511@atlanta.example.com
Call-Info: <cid:4567890123@atlanta.example.com>;
           purpose=EmergencyCallData.eCall.MSD
CSeq: 51862 INFO
Info-Package: EmergencyCallData.eCall.MSD
Allow: INVITE, ACK, PRACK, INFO, OPTIONS, CANCEL, REFER, BYE,
       SUBSCRIBE, NOTIFY, UPDATE
Content-Type: multipart/mixed; boundary=boundaryLine
Content-Disposition: Info-Package
Content-Length: ...

--boundaryLine
Content-Type: application/EmergencyCallData.eCall.MSD
Content-ID: <4567890123@atlanta.example.com>
Content-Disposition: by-reference

     ...MSD in ASN.1 PER encoding goes here...

--boundaryLine--
```

Figure 11: INFO Containing MSD

11. Security Considerations

The security considerations described in [RFC5069] (on marking and routing emergency calls) apply here.

In addition to any network-provided location (which might be determined solely by the network or in cooperation with or possibly entirely by the originating device), an eCall carries an IVS-supplied location within the MSD. This is likely to be useful to the PSAP, especially when no network-provided location is included, or 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 [RFC7378] discusses trust issues regarding location provided by or determined in cooperation with end devices.

Security considerations specific to the mechanism by which the PSAP sends acknowledgments and requests to the vehicle are discussed in the "Security Considerations" block of Section 14.4. Note that an attacker that has access to and is capable of generating a response to the initial INVITE request could generate a 600 (Busy Everywhere), 486 (Busy Here), or 603 (Decline) response that includes a metadata/control object containing a reference to the MSD in the initial INVITE and a "received=true" field, which could result in the IVS perceiving the PSAP to be overloaded and hence not attempting to reinitiate the call. The risk can be mitigated as discussed in the "Security Considerations" block of Section 14.4.

Data received from external sources inherently carries implementation risks. For example, depending on the platform, buffer overflows can introduce remote code execution vulnerabilities, null characters can corrupt strings, numeric values used for internal calculations can result in underflow/overflow errors, malformed XML objects can expose parsing bugs, etc. Implementations need to be cognizant of the potential risks, observe best practices (which might include sufficiently capable static code analysis, fuzz testing, component isolation, avoiding use of unsafe coding techniques, third-party attack tests, signed software, over-the-air updates, etc.), and have multiple levels of protection. Implementors need to be aware that, potentially, the data objects described here and elsewhere (including the MSD and metadata/control objects) might be malformed, contain unexpected characters, have excessively long attribute values and elements, etc.

The security considerations discussed in [RFC7852] apply here (see especially the discussion of Transport Layer Security (TLS), TLS versions, cipher suites, and PKI).

When vehicle data or control/metadata is contained in a signed or encrypted body part, the enclosing multipart (e.g., multipart/signed or multipart/encrypted) has the same Content-ID as the enclosed data part. This allows an entity to identify and access the data blocks it is interested in without having to dive deeply into the message structure or decrypt parts it is not interested in. (The "purpose" parameter in a Call-Info header field identifies the data and contains a CID URL pointing to the data block in the body, which has a matching Content-ID body part header field.)

12. Privacy Considerations

The privacy considerations discussed in [RFC7852] apply here. The MSD carries some identifying and personal information (mostly about the vehicle and less about the owner), as well as location information, so it needs to be protected against unauthorized disclosure. Local regulations may impose additional privacy protection requirements.

Privacy considerations specific to the data structure containing vehicle information are discussed in the "Security Considerations" block of Section 14.3.

Privacy considerations specific to the mechanism by which the PSAP sends acknowledgments and requests to the vehicle are discussed in the "Security Considerations" block of Section 14.4.

13. XML Schema

This section defines an XML schema for the control block. The text description of the control block in Section 9.1 is normative and supersedes any conflicting aspect of this schema.

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

    <xs:import namespace="http://www.w3.org/XML/1998/namespace"/>

    <xs:element name="EmergencyCallData.Control"
                type="pi:controlType"/>

    <xs:complexType name="controlType">
       <xs:complexContent>
          <xs:restriction base="xs:anyType">
             <xs:choice>
                <xs:element name="capabilities"
                            type="pi:capabilitiesType"/>
                <xs:element name="request" type="pi:requestType"/>
                <xs:element name="ack" type="pi:ackType"/>
```

```
                <xs:any namespace="##any" processContents="lax"
                        minOccurs="0"
                        maxOccurs="unbounded"/>
              </xs:choice>
              <xs:anyAttribute/>
            </xs:restriction>
          </xs:complexContent>
        </xs:complexType>

        <xs:complexType name="ackType">
            <xs:complexContent>
                <xs:restriction base="xs:anyType">
                    <xs:sequence minOccurs="1" maxOccurs="unbounded">
                        <xs:element name="actionResult" minOccurs="0"
                                    maxOccurs="unbounded">
                            <xs:complexType>
                                <xs:attribute name="action"
                                              type="xs:token"
                                              use="required"/>
                                <xs:attribute name="success"
                                              type="xs:boolean"
                                              use="required"/>
                                <xs:attribute name="reason"
                                              type="xs:token">
                                    <xs:annotation>
                                        <xs:documentation>
                                            conditionally mandatory
                                            when @success="false"
                                            to indicate reason code
                                            for a failure
                                        </xs:documentation>
                                    </xs:annotation>
                                </xs:attribute>
                                <xs:attribute name="details"
                                              type="xs:string"/>
                                <xs:anyAttribute
                                    processContents="skip"/>
                            </xs:complexType>
                        </xs:element>
                        <xs:any namespace="##any" processContents="lax"
                                minOccurs="0"
                                maxOccurs="unbounded"/>
                    </xs:sequence>
                    <xs:attribute name="ref"
                                  type="xs:anyURI"
                                  use="required"/>
```

```
                <xs:attribute name="received"
                              type="xs:boolean"/>
                <xs:anyAttribute/>
            </xs:restriction>
        </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="capabilitiesType">
        <xs:complexContent>
            <xs:restriction base="xs:anyType">
                <xs:sequence minOccurs="1" maxOccurs="unbounded">
                    <xs:element name="request"
                                type="pi:requestType"
                                minOccurs="1"
                        maxOccurs="unbounded"/>
                    <xs:any namespace="##any" processContents="lax"
                             minOccurs="0"
                        maxOccurs="unbounded"/>
                </xs:sequence>
                <xs:anyAttribute/>
            </xs:restriction>
        </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="requestType">
       <xs:complexContent>
            <xs:restriction base="xs:anyType">
                <xs:choice minOccurs="1" maxOccurs="unbounded">
                    <xs:element name="text" minOccurs="0"
                                maxOccurs="unbounded">
                        <xs:complexType>
                            <xs:simpleContent>
                                <xs:extension base="xs:string">
                                    <xs:anyAttribute
                                        namespace="##any"
                                        processContents="skip"/>
                                </xs:extension>
                            </xs:simpleContent>
                        </xs:complexType>
                    </xs:element>
                    <xs:any namespace="##any" processContents="lax"
                            minOccurs="0"
                            maxOccurs="unbounded"/>
                </xs:choice>
                <xs:attribute name="action" type="xs:token"
                              use="required"/>
```

```
                    <xs:attribute name="int-id" type="xs:unsignedInt"/>
                    <xs:attribute name="persistence"
                                  type="xs:duration"/>
                    <xs:attribute name="datatype" type="xs:token"/>
                    <xs:attribute name="supported-values"
                                  type="xs:string"/>
                    <xs:attribute name="element-id" type="xs:token"/>
                    <xs:attribute name="requested-state"
                                  type="xs:token"/>
                    <xs:anyAttribute/>
                </xs:restriction>
            </xs:complexContent>
        </xs:complexType>

    </xs:schema>
```

Figure 12: Control Block Schema

14. IANA Considerations

14.1. The EmergencyCallData Media Subtree

This document establishes the "EmergencyCallData" media (MIME) subtype tree, a new media subtree rooted at "application/EmergencyCallData". This subtree is used only for content associated with emergency communications. New subtypes in this subtree follow the rules specified in Section 3.1 of [RFC6838], with the additional restriction that the standards-related organization MUST be responsible for some aspect of emergency communications.

This subtree initially contains the following subtypes (defined here or in [RFC7852]):

- EmergencyCallData.Comment+xml
- EmergencyCallData.Control+xml
- EmergencyCallData.DeviceInfo+xml
- EmergencyCallData.eCall.MSD
- EmergencyCallData.ProviderInfo+xml
- EmergencyCallData.ServiceInfo+xml
- EmergencyCallData.SubscriberInfo+xml

14.2. Service URN Registrations

IANA has registered the URN urn:service:sos.ecall under the "'sos' Sub-Services" registry defined in Section 4.2 of [RFC5031].

This service requests resources associated with an emergency call placed by an in-vehicle system, carrying a standardized set of data related to the vehicle and incident. The "Description" registry field is "Vehicle-initiated emergency calls". Two sub-services are registered as well:

urn:service:sos.ecall.automatic

Used with an eCall invoked automatically, for example, due to a crash or other serious incident. The "Description" registry field is "Automatic vehicle-initiated emergency calls".

urn:service:sos.ecall.manual

Used with an eCall invoked due to manual interaction by a vehicle occupant. The "Description" registry field is "Manual vehicle-initiated emergency calls".

IANA has also registered the URN urn:service:test.sos.ecall under the "'test' Sub-Services" registry defined in Section 17.2 of [RFC6881]. This service requests resources associated with a test (non-emergency) call placed by an in-vehicle system. See Section 8 for more information on the test eCall request URN.

14.3. MIME Media Type Registration for application/EmergencyCallData.eCall.MSD

IANA has added application/EmergencyCallData.eCall.MSD as a MIME media type, with a reference to this document, in accordance with the procedures of RFC 6838 [RFC6838] and guidelines in RFC 7303 [RFC7303].

MIME media type name: application

MIME subtype name: EmergencyCallData.eCall.MSD

Mandatory parameters: none

Optional parameters: none

Encoding scheme: binary

Encoding considerations:
Uses ASN.1 PER, which is a binary encoding; when transported in SIP, binary content transfer encoding is used.

Security considerations:
This media 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. Sections 9 and 10 of [RFC7852] contain more discussion.

Interoperability considerations: None

Published specification: Annex A of EN 15722 [MSD]

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

Additional information: None

Magic Number: None

File Extension: None

Macintosh file type code: BINA

Person and email address for further information:
Randall Gellens, rg+ietf@randy.pensive.org

Intended usage: LIMITED USE

Author: The MSD 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)

14.4. MIME Media Type Registration for application/EmergencyCallData.Control+xml

IANA has added application/EmergencyCallData.Control+xml as a MIME media 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.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 media type carries metadata and control information and requests, such as from a Public Safety Answering Point (PSAP) to an In-Vehicle System (IVS) during an emergency call.

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 security implications. The privacy concern arises from the ability to request the vehicle to transmit a data set, which as described in Section 14.3 can contain personal information. The security concern is the ability to request the vehicle to perform an action. Control information needs to originate only from a PSAP or other emergency services providers and not be modified en route. The level of integrity of the cellular network over which the emergency call is placed is a consideration: when the IVS initiates an eCall over a cellular network, in most cases it relies on the MNO to route the call to a PSAP. (Calls placed using other means, such as Wi-Fi or over-the-top services, generally incur somewhat higher levels of risk than calls placed "natively" using cellular networks.) A callback from a PSAP merits additional consideration, since current mechanisms are not ideal for verifying that such a call is indeed a callback 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].

Sections 7 and 8 of [RFC7852] contain more discussion.

Interoperability considerations: None

Published specification: This document

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@randy.pensive.org

Intended usage: LIMITED USE

Author: The IETF ECRIT working group

Change controller: The IETF ECRIT working group

14.5. Registration of the "eCall.MSD" Entry in the Emergency Call Data Types Registry

IANA has added the "eCall.MSD" entry to the "Emergency Call Data Types" registry, with a reference to this document; the "Data About" value is "The Call".

14.6. Registration of the "Control" Entry in the Emergency Call Data Types Registry

IANA has added the "Control" entry to the "Emergency Call Data Types" registry, with a reference to this document; the "Data About" value is "The Call".

14.7. Registration for urn:ietf:params:xml:ns:EmergencyCallData:control

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

URI: urn:ietf:params:xml:ns:EmergencyCallData: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 Emergency Call Data Control Block</title>
</head>
<body>
     <h1>Namespace for Emergency Call Data Control Block</h1>
<p>See RFC 8147</p>
</body>
</html>
END
```

14.8. Registry Creation

This document creates a new registry called "Emergency Call Metadata/Control Data". The following sub-registries are created for this registry.

14.8.1. Emergency Call Actions Registry

This document creates a new sub-registry called "Emergency Call Actions". 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 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 a 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 1.

Name	Description
send-data	See Section 9.1.3.1 of this document

Table 1: Emergency Call Actions Registry Initial Values

14.8.2. Emergency Call Action Failure Reasons Registry

This document creates a new sub-registry called "Emergency Call Action Failure Reasons", 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 2.

ID	Description
damaged	Required components are damaged.
data-unsupported	The data item referenced in a "send-data" request is not supported.
security-failure	The authenticity of the request or the authority of the requestor could not be verified.
unable	The action could not be accomplished (a generic error for use when no other code is appropriate).
unsupported	The "action" value is not supported.

Table 2: Emergency Call Action Failure Reasons Registry Initial Values

14.9. The EmergencyCallData.eCall.MSD INFO Package

This document registers the EmergencyCallData.eCall.MSD INFO package in the "Info Packages Registry".

Both endpoints (the IVS and the PSAP equipment) include EmergencyCallData.eCall.MSD in a Recv-Info header field per [RFC6086] to indicate the ability to receive INFO requests carrying data as described here.

Support for the EmergencyCallData.eCall.MSD INFO package indicates the ability to receive eCall related body parts as specified in this document.

An INFO request message carrying body parts related to an emergency call as described in this document has an Info-Package header field set to "EmergencyCallData.eCall.MSD" per [RFC6086].

The requirements of Section 10 of [RFC6086] are addressed in the following sections.

14.9.1. Overall Description

This section describes what type of information is carried in INFO requests associated with the INFO package and for what types of applications and functionalities User Agents (UAs) can use the INFO package.

INFO requests associated with the EmergencyCallData.eCall.MSD INFO package carry data associated with emergency calls as defined in this document. The application is vehicle-initiated emergency calls established using SIP. The functionality is to carry vehicle data and metadata/control information between vehicles and PSAPs.

14.9.2. Applicability

This section describes why the INFO package mechanism, rather than some other mechanism, has been chosen for the specific use case.

The use of the SIP INFO method is based on an analysis of the requirements against the intent and effects of the INFO method versus other approaches (which included the SIP MESSAGE method, the SIP OPTIONS method, the SIP re-INVITE method, media-plane transport, and non-SIP protocols). In particular, the transport of emergency call data blocks occurs within a SIP emergency dialog, per Section 6, and is normally carried in the initial INVITE request and response; the use of the SIP INFO method only occurs when emergency-call-related data needs to be sent mid call. While the SIP MESSAGE method could

be used, it is not tied to a SIP dialog as is the SIP INFO method and thus might not be associated with the dialog. Either SIP OPTIONS or re-INVITE methods could also be used, but they are seen as less clean than the SIP INFO method. The SIP SUBSCRIBE/NOTIFY method could be coerced into service, but the semantics are not a good fit, e.g., the subscribe/notify mechanism provides one-way communication consisting of (often multiple) notifications from notifier to subscriber indicating that certain events in notifier have occurred, whereas what's needed here is two-way communication of data related to the emergency dialog. Use of media-plane mechanisms was discounted because the number of messages needing to be exchanged in a dialog is normally zero or very few, and the size of the data is likewise very small. The overhead caused by user-plane setup (e.g., to use the Message Session Relay Protocol (MSRP) as transport) would be disproportionately large.

Based on the analyses, the SIP INFO method was chosen to provide for mid-call data transport.

14.9.3. INFO Package Name

The INFO package name is EmergencyCallData.eCall.MSD

14.9.4. INFO Package Parameters

None

14.9.5. SIP Option-Tags

None

14.9.6. INFO Request Body Parts

The body for an EmergencyCallData.eCall.MSD INFO package is a multipart (normally multipart/mixed) body containing zero or one application/EmergencyCallData.eCall.MSD parts (containing an MSD) and zero or more application/EmergencyCallData.Control+xml (containing a metadata/control object) parts. At least one MSD or metadata/control body part is expected; the behavior upon receiving an INFO request with neither is undefined.

The body parts are sent per [RFC6086], and in addition, to align with how these body parts are sent in SIP messages other than INFO requests, each associated body part is referenced by a Call-Info header field at the top level of the SIP message. The body part has a Content-Disposition header field set to "By-Reference".

An MSD or metadata/control block is always enclosed in a multipart body part (even if it would otherwise be the only body part in the SIP message). The outermost multipart that contains only body parts associated with the INFO package has a Content-Disposition value of "Info-Package".

14.9.7. INFO Package Usage Restrictions

Usage is limited to vehicle-initiated emergency calls as defined in this document.

14.9.8. Rate of INFO Requests

The SIP INFO request is used within an established emergency call dialog for the PSAP to request the IVS to send an updated MSD and for the IVS to send a requested MSD. Because this is normally done only on manual request of the PSAP call taker (who suspects some aspect of the vehicle state has changed), the rate of SIP INFO requests associated with the EmergencyCallData.eCall.MSD INFO package is normally quite low (most dialogs are likely to contain zero INFO requests, while others might carry an occasional request).

14.9.9. INFO Package Security Considerations

The MIME media type registrations specified for use with this INFO package (Sections 14.3 and 14.4) contain a discussion of the security and/or privacy considerations specific to that data block. See Sections 11 and 12 for a discussion of the security and privacy considerations of the data carried in eCalls.

14.9.10. Implementation Details

See Sections 6 and 7 for protocol details.

14.9.11. Examples

See Section 10 for protocol examples.

15. References

15.1. Normative References

[MSD] European Committee for Standardization, "Intelligent transport systems - eSafety - eCall minimum set of data (MSD)", Standard: CEN - EN 15722, April 2015.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <http://www.rfc-editor.org/info/rfc3688>.

[RFC5031] Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", RFC 5031, DOI 10.17487/RFC5031, January 2008, <http://www.rfc-editor.org/info/rfc5031>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC6086] Holmberg, C., Burger, E., and H. Kaplan, "Session Initiation Protocol (SIP) INFO Method and Package Framework", RFC 6086, DOI 10.17487/RFC6086, January 2011, <http://www.rfc-editor.org/info/rfc6086>.

[RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, DOI 10.17487/RFC6838, January 2013, <http://www.rfc-editor.org/info/rfc6838>.

[RFC6881] Rosen, B. and J. Polk, "Best Current Practice for Communications Services in Support of Emergency Calling", BCP 181, RFC 6881, DOI 10.17487/RFC6881, March 2013, <http://www.rfc-editor.org/info/rfc6881>.

[RFC7303] Thompson, H. and C. Lilley, "XML Media Types", RFC 7303, DOI 10.17487/RFC7303, July 2014, <http://www.rfc-editor.org/info/rfc7303>.

[RFC7852] Gellens, R., Rosen, B., Tschofenig, H., Marshall, R., and J. Winterbottom, "Additional Data Related to an Emergency Call", RFC 7852, DOI 10.17487/RFC7852, July 2016, <http://www.rfc-editor.org/info/rfc7852>.

15.2. Informative references

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

[EN_16062] European Committee for Standardization, "Intelligent transport systems - eSafety - eCall High Level Application Requirements (HLAP) Using GSM/UMTS Circuit Switched Networks", Standard: CEN - EN 16062, April 2015.

[EN_16072] European Committee for Standardization, "Intelligent transport systems - eSafety - Pan-European eCall operating requirements", Standard: CEN - EN 16072, April 2015.

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

[RFC5012] Schulzrinne, H. and R. Marshall, Ed., "Requirements for Emergency Context Resolution with Internet Technologies", RFC 5012, DOI 10.17487/RFC5012, January 2008, <http://www.rfc-editor.org/info/rfc5012>.

[RFC5069] Taylor, T., Ed., Tschofenig, H., Schulzrinne, H., and M. Shanmugam, "Security Threats and Requirements for Emergency Call Marking and Mapping", RFC 5069, DOI 10.17487/RFC5069, January 2008, <http://www.rfc-editor.org/info/rfc5069>.

[RFC6443] Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling Using Internet Multimedia", RFC 6443, DOI 10.17487/RFC6443, December 2011, <http://www.rfc-editor.org/info/rfc6443>.

[RFC7090] Schulzrinne, H., Tschofenig, H., Holmberg, C., and M. Patel, "Public Safety Answering Point (PSAP) Callback", RFC 7090, DOI 10.17487/RFC7090, April 2014, <http://www.rfc-editor.org/info/rfc7090>.

[RFC7378] Tschofenig, H., Schulzrinne, H., and B. Aboba, Ed., "Trustworthy Location", RFC 7378, DOI 10.17487/RFC7378, December 2014, <http://www.rfc-editor.org/info/rfc7378>.

[RFC8148] Gellens, R., Rosen, B., and H. Tschofenig, "Next-Generation Vehicle-Initiated Emergency Calls", RFC 8148, DOI 10.17487/RFC8148, May 2017, <http://www.rfc-editor.org/info/rfc8148>.

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

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

[TS22.101] 3GPP, "Universal Mobile Telecommunications System (UMTS); Service aspects; Service principles", 3GPP TS 22.101, version 8.7.0, Release 8, January 2008.

[TS23.167] 3GPP, "IP Multimedia Subsystem (IMS) emergency sessions", 3GPP TS 23.167, version 9.6.0, Release 9, March 2011.

[TS24.229] 3GPP, "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3", 3GPP TS 24.229, version 12.6.0, Release 12, October 2014.

Acknowledgments

We would like to thank Bob Williams and Ban Al-Bakri for their feedback and suggestions; Rex Buddenberg, Lena Chaponniere, Alissa Cooper, Keith Drage, Stephen Edge, Wes George, Mirja Kuehlewind, Allison Mankin, Alexey Melnikov, Ivo Sedlacek, and James Winterbottom for their review and comments; Robert Sparks and Paul Kyzivat for their help with the SIP mechanisms; and Mark Baker and Ned Freed for their help with the media subtype registration issue. 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. Christer Holmberg deserves special mention for his many detailed reviews.

Contributors

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

Authors' Addresses

Randall Gellens
Core Technology Consulting

Email: rg+ietf@coretechnologyconsulting.com
URI: http://www.coretechnologyconsulting.com

Hannes Tschofenig
Individual

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