

ECRIT Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: November 4, 2011

C. Holmberg  
Ericsson  
May 3, 2011

Session Initiation Protocol (SIP) Media Feature Tag to identity a Public  
Safety Answering Point (PSAP) Callback Call  
draft-holmberg-ecrit-callback-00.txt

## Abstract

This specification defines a new Session Initiation Protocol (SIP) media feature tag, sip.psap.callback, that SIP entities can use to identity Public Safety Answering Point (PSAP) callback calls, and to associate them with a previously made emergency call.

## Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute 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 November 4, 2011.

## Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Terminology . . . . .	3
3. Applicability and Limitation . . . . .	3
4. User Agent Client behavior . . . . .	3
4.1. General . . . . .	3
4.2. Registration . . . . .	3
4.3. Emergency call . . . . .	4
4.4. PSAP callback call . . . . .	4
5. User Agent Server behavior . . . . .	4
5.1. General . . . . .	4
6. Registrar behavior . . . . .	4
6.1. General . . . . .	5
6.2. Registration . . . . .	5
6.3. PSAP callback call . . . . .	5
7. Message Flow Examples . . . . .	5
7.1. Example . . . . .	5
8. Security Considerations . . . . .	6
9. IANA Considerations . . . . .	6
9.1. IANA Registration of the sip.psap.callback media feature tag . . . . .	6
10. Acknowledgements . . . . .	6
11. Change Log . . . . .	7
12. References . . . . .	7
12.1. Normative References . . . . .	7
12.2. Informational References . . . . .	7
Author's Address . . . . .	7

## 1. Introduction

TBD

## 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].

## 3. Applicability and Limitation

TBD

## 4. User Agent Client behavior

### 4.1. General

TBD

### 4.2. Registration

When a UAC sends a SIP REGISTER request [RFC3261], and it wants to be able to receive explicit PSAP callback calls associated with that registration, it MUST insert a sip.psap.callback media feature tag in the Contact header field [RFC3261] of the request.

The value of the sip.psap.callback MUST uniquely identify the User Agent (UA). If the UA supports the "sip.instance" media feature tag [RFC5626], it is STRONGLY RECOMMENDED that it uses the same value for the sip.psap.callback feature tag.

OPEN ISSUE: Need to discuss whether the usage of a "static" value (e.g. the sip.instance value), that might also be known by other users, causes some security issues, and whether another value (that might change between emergency registrations, should be used instead.

If the UAC applies the SIP Outbound mechanism [RFC5626], and establishes multiple registration flows associated with a registration, it MUST include the sip.psap.callback media feature tag in each REGISTER requests associated with every registration flow for which it wants to be able to receive explicit PSAP callback calls. The UAC MUST use the same media feature tag value for each registration flow associated with a registration.

Unless the UAC wants the registrar to remove the media feature tag associated with a registration/registration flow, the UAC MUST include the sip.psap.callback media feature tag in every SIP REGISTER request associated with the registration (or registration flow), apart from when it terminates a registration (or registration flow).

#### 4.3. Emergency call

When a UAC sends an initial SIP INVITE request [RFC3261] for an emergency call, it MUST insert a sip.psap.callback media feature tag in the Contact header field of the request. The UAC MUST use the same media feature tag value that has been used for the registration associated with the emergency call.

OPEN ISSUE: Should the UAC also include the media feature tag in calls that are not identified as emergency calls by the UAC, but will be determined as emergency calls by the network?

#### 4.4. PSAP callback call

When a UAC, representing a PSAP, sends an initial SIP INVITE request for an PSAP callback call, it SHOULD insert a sip.psap.callback media feature tag in the Accept-Contact header field [RFC3841] of the request. The UAC MUST use the same media feature tag value that was used for the emergency call associated with the callback call.

If the PSAP callback call comes from a Public Switched Telephony Network (PSTN), or from another interworking network, the UAC representing the PSAP will normally be located in a network interworking gateway controller, such as a in a Media Gateway Controller (MGC). If the interworking gateway controller is able to determine that the call is a PSAP callback call it MUST insert a media feature tag. If the interworking gateway controller is not aware of the media feature tag value associated with the called user, it inserts an empty media feature tag.

### 5. User Agent Server behavior

#### 5.1. General

TBD

### 6. Registrar behavior

## 6.1. General

TBD

## 6.2. Registration

When a registrar performs registration procedures for a user, if the associated SIP REGISTER request contains a sip.psap.callback media feature tag with a media feature tag value, the registrar MUST store the media feature tag value together with other registration data associated with the registering user.

OPEN ISSUE: Is there a need for the registrar to inform the UAC that it supports, and has stored the value of, the sip.psap.callback media feature tag?

## 6.3. PSAP callback call

When a registrar receives an initial SIP INVITE request for a call, and the Accept-Contact header field of the request contains a sip.psap.callback media feature tag, if the media feature tag value matches a value registered for the called user, and if the registrar trusts the originator of the request, the registrar can decide that the call is a PSAP callback call.

If the media feature tag of the request does not contain a media feature tag value (this might be the case if the requests comes from an MGC that has been able the identity the call as a PSAP callback call, but is not aware of the media feature tag value associated with the called user), if the registrar trusts the originator of the request, and a media feature tag value has been registered for the called user, the registrar MAY decide that the call is a PSAP callback call.

OPEN ISSUE: If the registrar receives a request with an empty media feature tag, and decides that the call is a PSAP callback call, should the registrar add the registered media feature tag value to the media feature tag in the request?

## 7. Message Flow Examples

### 7.1. Example

TBD

Add example flow

Figure 1: Example call flow

## 8. Security Considerations

TBD

## 9. IANA Considerations

### 9.1. IANA Registration of the sip.psap.callback media feature tag

This section registers a new media feature tag, sip.psap.callback, into the SIP media feature tag tree. The required information for this registration, as specified in section 3.4 of [RFC2506], is:

RFC Number: RFC XXXX [[NOTE TO IANA: Please replace XXXX with the RFC number of this specification]]

Media feature tag name: sip.psap.callback

ASN.1 identifier associated with feature tag: New assignment by IANA

Summary of the media feature indicated by this feature tag: This feature tag indicates

a unique value for a User Agent (UA), which is used to associate PSAP callback calls with emergency calls placed by the user.

Values appropriate for use with this feature tag: String (equality relationship)

Examples of typical use: Associating a PSAP callback call with a previously placed emergency call.

Related standards or documents: RFC 3840

Security Considerations: General security considerations for media feature tags are discussed in Section 11.1 of RFC 3840.

## 10. Acknowledgements

The original idea of using a token based mechanism to associate PSAP callback calls with emergency calls was presented by Cullen Jennings.

Thanks to Fredrik Lindholm, Jan Holm and Ivo Sedlacek for their comments and feedbacks on the initial draft.

Thanks to xxx for their feedback and suggestions on the ECRIT mailing

list.

## 11. Change Log

[RFC EDITOR NOTE: Please remove this section when publishing]

Changes from draft-holmberg-ecrit-callback-xx

- o Indicate changes from previous version

## 12. References

### 12.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2506] Holtman, K., Mutz, A., and T. Hardie, "Media Feature Tag Registration Procedure", BCP 31, RFC 2506, March 1999.
- [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.
- [RFC3840] Rosenberg, J., Schulzrinne, H., and P. Kyzivat, "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)", RFC 3840, August 2004.
- [RFC3841] Rosenberg, J., Schulzrinne, H., and P. Kyzivat, "Caller Preferences for the Session Initiation Protocol (SIP)", RFC 3841, August 2004.

### 12.2. Informational References

- [RFC5626] Jennings, C., Mahy, R., and F. Audet, "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)", RFC 5626, October 2009.

Author's Address

Christer Holmberg  
Ericsson  
Hirsalantie 11  
Jorvas 02420  
Finland

Email: [christer.holmberg@ericsson.com](mailto:christer.holmberg@ericsson.com)





This Internet-Draft, draft-ietf-ecrit-additional-data-00.txt, has expired, and has been deleted from the Internet-Drafts directory. An Internet-Draft expires 185 days from the date that it is posted unless it is replaced by an updated version, or the Secretariat has been notified that the document is under official review by the IESG or has been passed to the RFC Editor for review and/or publication as an RFC. This Internet-Draft was not published as an RFC.

Internet-Drafts are not archival documents, and copies of Internet-Drafts that have been deleted from the directory are not available. The Secretariat does not have any information regarding the future plans of the authors or working group, if applicable, with respect to this deleted Internet-Draft. For more information, or to request a copy of the document, please contact the authors directly.

Draft Authors:

Brian Rosen<br@brianrosen.net>

Hannes Tschofenig<Hannes.Tschofenig@gmx.net>

This Internet-Draft, draft-ietf-ecrit-data-only-ea-01.txt, has expired, and has been deleted from the Internet-Drafts directory. An Internet-Draft expires 185 days from the date that it is posted unless it is replaced by an updated version, or the Secretariat has been notified that the document is under official review by the IESG or has been passed to the RFC Editor for review and/or publication as an RFC. This Internet-Draft was not published as an RFC.

Internet-Drafts are not archival documents, and copies of Internet-Drafts that have been deleted from the directory are not available. The Secretariat does not have any information regarding the future plans of the authors or working group, if applicable, with respect to this deleted Internet-Draft. For more information, or to request a copy of the document, please contact the authors directly.

Draft Authors:

Brian Rosen<br@brianrosen.net>

Henning Schulzrinne<hgs+ecrit@cs.columbia.edu>

Hannes Tschofenig<Hannes.Tschofenig@gmx.net>

This Internet-Draft, draft-ietf-ecrit-trustworthy-location-01.txt, has expired, and has been deleted from the Internet-Drafts directory. An Internet-Draft expires 185 days from the date that it is posted unless it is replaced by an updated version, or the Secretariat has been notified that the document is under official review by the IESG or has been passed to the RFC Editor for review and/or publication as an RFC. This Internet-Draft was not published as an RFC.

Internet-Drafts are not archival documents, and copies of Internet-Drafts that have been deleted from the directory are not available. The Secretariat does not have any information regarding the future plans of the authors or working group, if applicable, with respect to this deleted Internet-Draft. For more information, or to request a copy of the document, please contact the authors directly.

Draft Authors:

Hannes Tschofenig<Hannes.Tschofenig@gmx.net>  
Henning Schulzrinne<hgs@cs.columbia.edu>  
Bernard Aboba<Bernard\_Aboba@hotmail.com>

ECRIT  
Internet-Draft  
Intended status: Standards Track  
Expires: January 12, 2012

H. Schulzrinne  
Columbia University  
S. McCann  
Research in Motion UK Ltd  
G. Bajko  
Nokia  
H. Tschofenig  
Nokia Siemens Networks  
D. Kroeselberg  
Siemens  
July 11, 2011

Extensions to the Emergency Services Architecture for dealing with  
Unauthenticated and Unauthorized Devices  
draft-ietf-ecrit-unauthenticated-access-03.txt

#### Abstract

The IETF emergency services architecture assumes that the calling device has acquired rights to use the access network or that no authentication is required for the access network, such as for public wireless access points. Subsequent protocol interactions, such as obtaining location information, learning the address of the Public Safety Answering Point (PSAP) and the emergency call itself are largely decoupled from the underlying network access procedures.

In some cases, however, the device does not have these credentials for network access, does not have a VoIP service provider, or the credentials have become invalid, e.g., because the user has exhausted their prepaid balance or the account has expired.

This document provides a problem statement, introduces terminology and describes an extension for the base IETF emergency services architecture to address these scenarios.

#### Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute 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 January 12, 2012.

#### Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	4
2. Terminology . . . . .	7
3. Use Case Categories . . . . .	8
4. ZBP Considerations . . . . .	10
5. NASP Considerations . . . . .	11
5.1. End Host Profile . . . . .	13
5.1.1. LoST Server Discovery . . . . .	13
5.1.2. ESRP Discovery . . . . .	13
5.1.3. Location Determination and Location Configuration . . . . .	13
5.1.4. Emergency Call Identification . . . . .	13
5.1.5. SIP Emergency Call Signaling . . . . .	13
5.1.6. Media . . . . .	14
5.1.7. Testing . . . . .	14
5.2. IAP/ISP Profile . . . . .	14
5.2.1. ESRP Discovery . . . . .	14
5.2.2. Location Determination and Location Configuration . . . . .	14
5.3. ESRP Profile . . . . .	14
5.3.1. Emergency Call Routing . . . . .	14
5.3.2. Emergency Call Identification . . . . .	14
5.3.3. SIP Emergency Call Signaling . . . . .	15
6. Lower Layer Considerations for NAA Case . . . . .	16
6.1. Link Layer Emergency Indication . . . . .	16
6.2. Securing Network Attachment in NAA Cases . . . . .	17
7. Security Considerations . . . . .	20
8. Acknowledgments . . . . .	21
9. IANA Considerations . . . . .	22
10. References . . . . .	23
10.1. Normative References . . . . .	23
10.2. Informative References . . . . .	23
Authors' Addresses . . . . .	26

## 1. Introduction

Summoning police, the fire department or an ambulance in emergencies is one of the fundamental and most-valued functions of the telephone. As telephone functionality moves from circuit-switched telephony to Internet telephony, its users rightfully expect that this core functionality will continue to work at least as well as it has for the older technology. New devices and services are being made available that could be used to make a request for help, which are not traditional telephones, and users are increasingly expecting them to be used to place emergency calls.

Roughly speaking, the IETF emergency services architecture (see [I-D.ietf-ecrit-phonebcpl] and [I-D.ietf-ecrit-framework]) divides responsibility for handling emergency calls between the access network (ISP), the application service provider (ASP) that may be a VoIP service provider and the provider of emergency signaling services, the emergency service network (ESN). The access network may provide location information to end systems, but does not have to provide any ASP signaling functionality. The emergency caller can reach the ESN either directly or through the ASP's outbound proxy. Any of the three parties can provide the mapping from location to PSAP URI by offering LoST [RFC5222] services.

In general, a set of automated configuration mechanisms allows a device to function in a variety of architectures, without the user being aware of the details on who provides location, mapping services or call routing services. However, if emergency calling is to be supported when the calling device lacks access network authorization or does not have an ASP, one or more of the providers may need to provide additional services and functions.

In all cases, the end device has to be able to perform a LoST lookup and otherwise conduct the emergency call in the same manner as when the three exceptional conditions discussed below do not apply.

We distinguish between three conditions:

**No Access Authentication (NAA):** In the NAA case, the emergency caller does not possess valid credentials for the access network. This includes the case where the access network allows pay-per-use, as is common for wireless hotspots, but there is insufficient time to enter credit card details and other registration information required for access. It also covers all cases where either no credentials are available at all, or the available credentials do not work for the given IAP/ISP. As a result, the NAA case basically combines the below NASP and ZBP cases, but at the IAP/ISP level. Support for emergency call handling in the NAA



case is subject to the local policy of the ISP. Such policy may vary substantially between ISPs and typically depends on external factors that are not under the ISP control.

No ASP (NASP): The caller does not have an ASP at the time of the call. This can occur either in case the caller does not possess any valid subscription for a reachable ASP, or in case none of the ASPs where the caller owns a valid subscription is reachable through the ISP.

Note: The interoperability need is increased with this scenario since the client software used by the emergency caller must be compatible with the protocols and extensions deployed by the ESN.

Zero-balance ASP (ZBP): In the case of zero-balance ASP, the ASP can authenticate the caller, but the caller is not authorized to use ASP services, e.g., because the contract has expired or the prepaid account for the customer has been depleted.

These three cases are not mutually exclusive. A caller in need for help may find himself/herself in, for example, a NAA and NASP situation, as explained in more details in Figure 1. Depending on local policy and regulations, it may not be possible to place emergency calls in the NAA case. Unless local regulations require user identification, it should always be possible to place calls in the NASP case, with minimal impact on the ISP. Unless the ESN requires that all calls traverse a known set of VSPs, it is technically possible to let a caller place an emergency call in the ZBP case. We discuss each case in more details in Section 3.

Note: At the time of writing there is no regulation in place that demands the functionality described in this memo. SDOs have started their work on this subject in a proactive fashion in the anticipation that national regulation will demand it for a subset of network environments.

There are also indications that the functionality of unauthenticated emergency calls (called SIM-less calls) in today's cellular system in certain countries leads to a fair amount of hoax or test calls. This causes overload situations at PSAPs which is considered harmful to the overall availability and reliability of emergency services.

As an example, Federal Office of Communications (OFCOM, Switzerland) provided statistics about emergency (112) calls in Switzerland from Jan. 1997 to Nov. 2001. Switzerland did not offer SIM-less emergency

calls except for almost a month in July 2000 where a significant increase in hoax and test calls was reported. As a consequence, the functionality was disabled again. More details can be found in the panel presentations of the 3rd SDO Emergency Services Workshop [esw07].

## 2. Terminology

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

This document reuses terminology from [RFC5687] and [RFC5012], namely Internet Access Provider (IAP), Internet Service Provider (ISP), Application Service Provider (ASP), Voice Service Provider (VSP), Emergency Service Routing Proxy (ESRP), Public Safety Answering Point (PSAP), Location Configuration Server (LCS), (emergency) service dial string, and (emergency) service identifier.

### 3. Use Case Categories

On a very high-level, the steps to be performed by an end host not being attached to the network and the user starting to make an emergency call are the following:

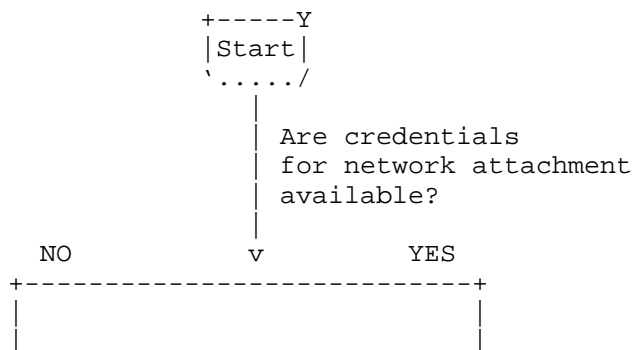
**Link Layer Attachment:** Some radio networks have added support for unauthenticated emergency access, some other type of networks advertise these capabilities using layer beacons. The end host learns about these unauthenticated emergency services capabilities either from the link layer type or from advertisement.

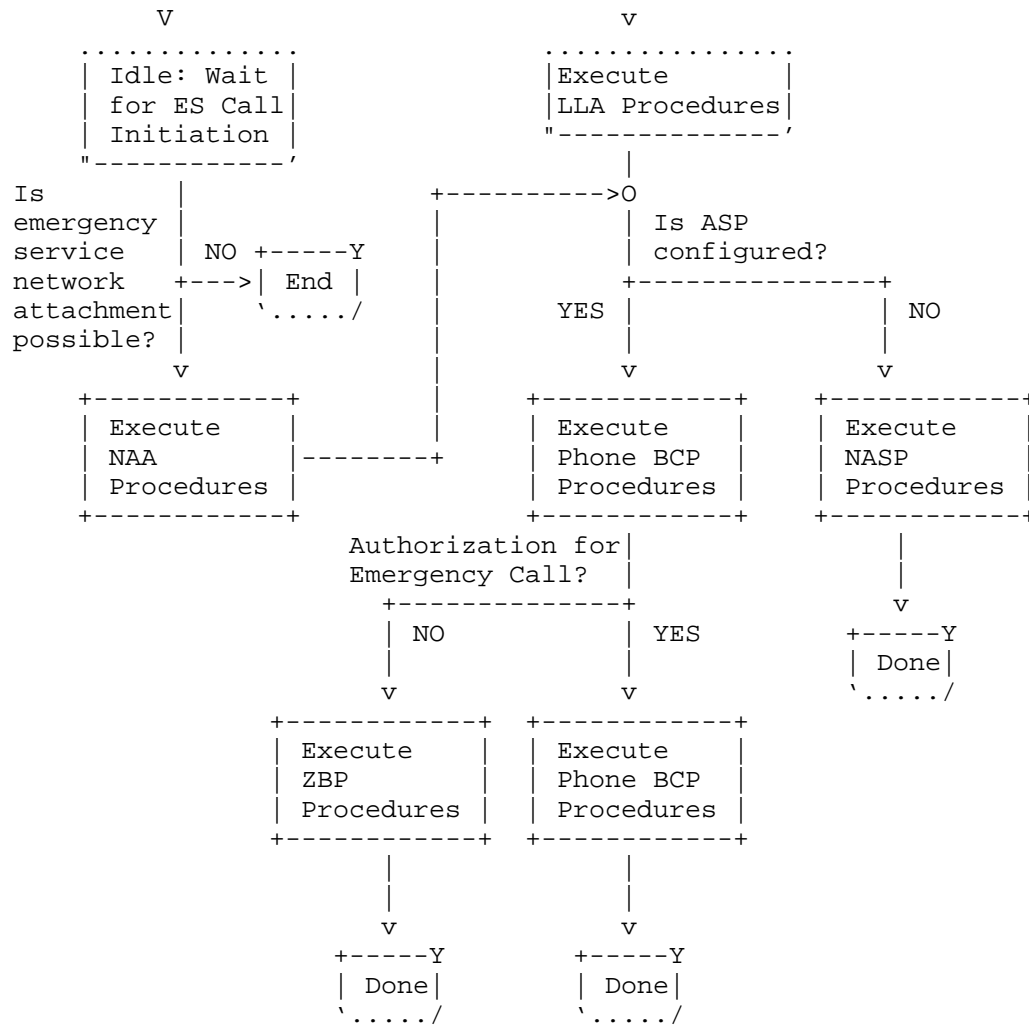
The end host uses the link layer specific network attachment procedures defined for unauthenticated network access in order to get access to the network.

**Pre-Emergency Service Configuration:** When the link layer network attachment procedure is completed the end host learns basic configuration information using DHCP from the ISP. The end host uses a Location Configuration Protocol (LCP) to retrieve location information. Subsequently, the LoST protocol [RFC5222] is used to learn the relevant emergency numbers, and to obtain the PSAP URI applicable for that location.

**Emergency Call:** In case of need for help, a user dials an emergency number and the SIP UA initiates the emergency call procedures by communicating with the PSAP.

Figure 1 compiles the basic logic taking place during network entry for requesting an emergency service and shows the interrelation between the three conditions described in the above section.





## Abbreviations:

LLA: Link Layer Attachment

ES: Emergency Services

Figure 1: Flow Diagram

#### 4. ZBP Considerations

ZBP includes all cases where a subscriber is known to an ASP, but lacks the necessary authorization to access regular ASP services. Example ZBP cases include empty prepaid accounts, barred accounts, roaming and mobility restrictions, or any other conditions set by ASP policy.

Local regulation might demand that emergency calls are always authorized. An ASP can identify emergency sessions by identifying the service URN [RFC5031] used in call setup. Emergency calls can then be authorized accordingly. The ZBP case therefore only affects the ASP.

Permitting a call with limited authorization could present an opportunity for abuse. The ASP MAY choose to validate session initiation messages for valid destinations, see Section 7.

An ASP without a regulatory requirement to authorize emergency calls can deny emergency call setup. Where an ASP does not authorize an emergency call, the caller can fall back to NASP procedures.

## 5. NASP Considerations

To start the description we consider the sequence of steps that are executed in an emergency call based on Figure 2.

- o As an initial step the device attaches to the network as shown in step (1). This step is outside the scope of this section.
- o When the link layer network attachment procedure is completed the end host learns basic configuration information using DHCP from the ISP, as shown in step (2).
- o When the IP address configuration is completed then the end host starts an interaction with the discovered Location Configuration Server at the ISP, as shown in step (3). The ISP may in certain deployments need to interact with the IAP. This protocol exchange is shown in step (4).
- o Once location information is obtained the end host triggers the LoST protocol to obtain the address of the ESRP/PSAP. This step is shown in (5).
- o In step (6), the SIP UA initiates a SIP INVITE towards the indicated ESRP. The INVITE message contains all the necessary parameters required by Section 5.1.5.
- o The ESRP receives the INVITE and processes it according to the description in Section 5.3.3.
- o The ESRP routes the call to the PSAP, as shown in (8), potentially interacting with a LoST server first to determine the route.
- o The PSAP evaluates the initial INVITE and aims to complete the call setup.
- o Finally, when the call setup is completed media traffic can be exchanged between the PSAP and the SIP UA.

For editorial reasons the end-to-end SIP and media exchange between the PSAP and SIP UA are not shown in Figure 2.

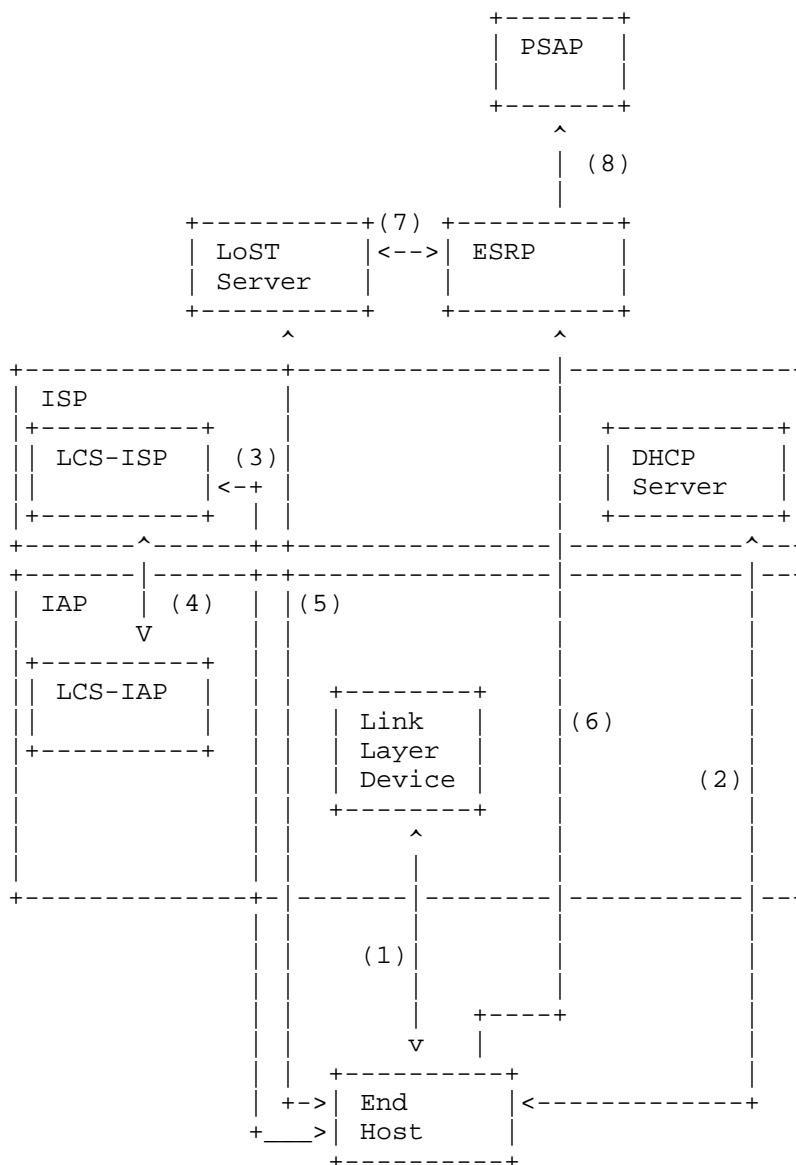


Figure 2: Architectural Overview

Note: Figure 2 does not indicate who operates the ESRP and the LoST server. Various deployment options exist.



## 5.1. End Host Profile

### 5.1.1. LoST Server Discovery

The end host MUST discover a LoST server [RFC5222] using DHCP [RFC5223].

### 5.1.2. ESRP Discovery

The end host MUST discover the ESRP using the LoST protocol [RFC5222].

### 5.1.3. Location Determination and Location Configuration

The end host MUST support location acquisition and the LCPs described in Section 6.5 of [I-D.ietf-ecrit-phonebcpl]. The description in Section 6.5 and 6.6 of [I-D.ietf-ecrit-phonebcpl] regarding the interaction between the device and the LIS applies to this document.

The SIP UA in the end host MUST attach available location information in a PIDF-LO [RFC4119] when making an emergency call. When constructing the PIDF-LO the guidelines in PIDF-LO profile [RFC5491] MUST be followed. For civic location information the format defined in [RFC5139] MUST be supported.

### 5.1.4. Emergency Call Identification

To determine which calls are emergency calls, some entity needs to map a user entered dialstring into this URN scheme. A user may "dial" 1-1-2, but the call would be sent to urn:service:sos. This mapping SHOULD be performed at the endpoint device.

End hosts MUST use the Service URN mechanism [RFC5031] to mark calls as emergency calls for their home emergency dial string.

### 5.1.5. SIP Emergency Call Signaling

SIP signaling capabilities [RFC3261] are mandated for end hosts.

The initial SIP signaling method is an INVITE. The SIP INVITE request MUST be constructed according to the requirements in Section 9.2 [I-D.ietf-ecrit-phonebcpl].

Regarding callback behavior SIP UAs SHOULD place a globally routable URI in a Contact: header.

#### 5.1.6. Media

End points MUST comply with the media requirements for end points placing an emergency call found in Section 14 of [I-D.ietf-ecrit-phonebcg].

#### 5.1.7. Testing

The description in Section 15 of [I-D.ietf-ecrit-phonebcg] is fully applicable to this document.

### 5.2. IAP/ISP Profile

#### 5.2.1. ESRP Discovery

An ISP MUST provision a DHCP server with information about LoST servers [RFC5223]. An ISP operator may choose to deploy a LoST server or to outsource it to other parties.

#### 5.2.2. Location Determination and Location Configuration

The ISP is responsible for location determination and exposes this information to the end points via location configuration protocols. The considerations described in [I-D.ietf-ecrit-location-hiding-req] are applicable to this document.

The ISP MUST support one of the LCPs described in Section 6.5 of [I-D.ietf-ecrit-phonebcg]. The description in Section 6.5 and 6.6 of [I-D.ietf-ecrit-phonebcg] regarding the interaction between the end device and the LIS applies to this document.

The interaction between the LIS at the ISP and the IAP is often proprietary but the description in [I-D.winterbottom-geopriv-lis2lis-req] may be relevant to the reader.

### 5.3. ESRP Profile

#### 5.3.1. Emergency Call Routing

The ESRP continues to route the emergency call to the PSAP responsible for the physical location of the end host. This may require further interactions with LoST servers but depends on the specific deployment.

#### 5.3.2. Emergency Call Identification

The ESRP MUST understand the Service URN mechanism [RFC5031] (i.e., the 'urn:service:sos' tree).

### 5.3.3. SIP Emergency Call Signaling

SIP signaling capabilities [RFC3261] are mandated for the ESRP. The ESRP MUST process the messages sent by the client, according to Section 5.1.5.

## 6. Lower Layer Considerations for NAA Case

Some radio networks have added support for unauthenticated emergency access, some other type of networks advertise these capabilities using layer beacons. The end host learns about these unauthenticated emergency services capabilities either from the link layer type or from advertisement.

This section discusses different methods to indicate an emergency service request as part of network attachment. It provides some general considerations and recommendations that are not specific to the access technology.

To perform network attachment and get access to the resources provided by an IAP/ISP, the end host uses access technology specific network attachment procedures, including for example network detection and selection, authentication, and authorization. For initial network attachment of an emergency service requester, the method of how the emergency indication is given to the IAP/ISP is specific to the access technology. However, a number of general approaches can be identified:

Link layer emergency indication: The end host provides an indication, e.g. an emergency parameter or flag, as part of the link layer signaling for initial network attachment. Examples include an emergency bit signalled in the IEEE 802.16-2009 wireless link. In IEEE 802.11 WLAN, an emergency support indicator allows the STA to download before association an NAI which it can use to request server side authentication only for an 802.1x network.

Higher-layer emergency indication: Typically emergency indication in access authentication. The emergency caller's end host provides an indication as part of the access authentication exchanges. EAP based authentication is of particular relevance here. Examples are the EAP NAI decoration used in WiMAX networks and modification of the authentication exchange in IEEE 802.11. [nwgstg3].

### 6.1. Link Layer Emergency Indication

In general, link layer emergency indications provide good integration into the actual network access procedure regarding the enabling of means to recognize and prioritize an emergency service request from an end host at a very early stage of the network attachment procedure. However, support in end hosts for such methods cannot be considered to be commonly available.

No general recommendations are given in the scope of this memo due to the following reasons:

- o Dependency on the specific access technology.
- o Dependency on the specific access network architecture. Access authorization and policy decisions typically happen at a different layers of the protocol stack and in different entities than those terminating the link-layer signaling. As a result, link layer indications need to be distributed and translated between the different involved protocol layers and entities. Appropriate methods are specific to the actual architecture of the IAP/ISP network.
- o An advantage of combining emergency indications with the actual network attachment procedure performing authentication and authorization is the fact that the emergency indication can directly be taken into account in the authentication and authorization server that owns the policy for granting access to the network resources. As a result, there is no direct dependency on the access network architecture that otherwise would need to take care of merging link-layer indications into the AA and policy decision process.
- o EAP signaling happens at a relatively early stage of network attachment, so it is likely to match most requirements for prioritization of emergency signaling. However, it does not cover early stages of link layer activity in the network attachment process. Possible conflicts may arise e.g. in case of MAC-based filtering in entities terminating the link-layer signaling in the network (like a base station). In normal operation, EAP related information will only be recognized in the NAS. Any entity residing between end host and NAS should not be expected to understand/parse EAP messages.
- o An emergency indication can be given by forming a specific NAI that is used as the identity in EAP based authentication for network entry.

## 6.2. Securing Network Attachment in NAA Cases

For network attachment in NAA cases, it may make sense to secure the link-layer connection between the device and the IAP/ISP. This especially holds for wireless access with examples being IEEE 802.11 or IEEE 802.16 based access. The latter even mandates secured communication across the wireless link for all IAP/ISP networks based on [nwgstg3].

Therefore, for network attachment that is by default based on EAP authentication it is desirable also for NAA network attachment to use a key-generating EAP method (that provides an MSK key to the authenticator to bootstrap further key derivation for protecting the wireless link).

The following approaches to match the above can be identified:

1) Server-only Authentication:

The device of the emergency service requester performs an EAP method with the IAP/ISP EAP server that performs server side authentication only. An example for this is EAP-TLS. This provides a certain level of assurance about the IAP/ISP to the device user. It requires the device to be provisioned with appropriate trusted root certificates to be able to verify the server certificate of the EAP server (unless this step is explicitly skipped in the device in case of an emergency service request). This method is used to provide access of devices without existing credentials to an 802.1x network. The details are incorporated into the not yet published 802.11-2011 specification.

2) Null Authentication:

In one case (e.g. WiMAX) an EAP method is performed. However, no credentials specific to either the server or the device or subscription are used as part of the authentication exchange. An example for this would be an EAP-TLS exchange with using the TLS\_DH\_anon (anonymous) ciphersuite. Alternatively, a publicly available static key for emergency access could be used. In the latter case, the device would need to be provisioned with the appropriate emergency key for the IAP/ISP in advance. In another case (e.g. IEEE 802.11), no EAP method is used, so that empty frames are transported during the over the air IEEE 802.1X exchange. In this case the authentication state machine completes with no cryptographic keys being exchanged.

3) Device Authentication:

This case extends the server-only authentication case. If the device is configured with a device certificate and the IAP/ISP EAP server can rely on a trusted root allowing the EAP server to verify the device certificate, at least the device identity (e.g., the MAC address) can be authenticated by the IAP/ISP in NAA cases. An example for this are WiMAX devices that are shipped with device

certificates issued under the global WiMAX device public-key infrastructure. To perform unauthenticated emergency calls, if allowed by the IAP/ISP, such devices perform EAP-TLS based network attachment with client authentication based on the device certificate.

## 7. Security Considerations

The security threats discussed in [RFC5069] are applicable to this document.

There are a couple of new vulnerabilities raised with unauthenticated emergency services in NASP/NAA cases since the PSAP operator will typically not possess any identity information about the emergency call via the signaling path itself. In countries where this functionality is used for GSM networks today this has lead to a significant amount of misuse.

In the context of NAA, the IAP and the ISP will probably want to make sure that the claimed emergency caller indeed performs an emergency call rather than using the network for other purposes, and thereby acting fraudulent by skipping any authentication, authorization and accounting procedures. By restricting access of the unauthenticated emergency caller to the LoST server and the PSAP URI, traffic can be restricted only to emergency calls. This can be accomplished with traffic separation. The details, however, e.g. for using filtering, depend on the deployed ISP architecture and are beyond the scope of this document.

We only illustrate a possible model. If the ISP runs its own LoST server, it would maintain an access control list including all IP addresses contained in responses returned by the LoST server, as well as the LoST server itself. (It may need to translate the domain names returned to IP addresses and hope that the resolution captures all possible DNS responses.) Since the media destination addresses are not predictable, the ISP also has to provide a SIP outbound proxy so that it can determine the media addresses and add those to the filter list.

For the ZBP case the additional aspect of fraud has to be considered. Unless the emergency call traverses a PSTN gateway or the ASP charges for IP-to-IP calls, there is little potential for fraud. If the ASP also operates the LoST server, the outbound proxy MAY restrict outbound calls to the SIP URIs returned by the LoST server. It is NOT RECOMMENDED to rely on a fixed list of SIP URIs, as that list may change.

Finally, a number of security vulnerabilities discussed in [I-D.ietf-geopriv-arch] around faked location information are less problematic in the context of unauthenticated emergency since location information does not need to be provided by the end host itself or it can be verified to fall within a specific geographical area.



## 8. Acknowledgments

Parts of this document are derived from [I-D.ietf-ecrit-phonebcpl]. Participants of the 2nd and 3rd SDO Emergency Services Workshop provided helpful input.

We would like to thank Richard Barnes, Brian Rosen, James Polk, Marc Linsner, and Martin Thomson for their feedback at the IETF#80 ECRIT meeting.

Furthermore, we would like to thank Martin Thomson and Bernard Aboba for their detailed document review in preparation of the 81st IETF meeting.

## 9. IANA Considerations

This document does not require actions by IANA.

## 10. References

### 10.1. Normative References

- [RFC5031] Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", RFC 5031, January 2008.
- [RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.
- [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.
- [RFC5139] Thomson, M. and J. Winterbottom, "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)", RFC 5139, February 2008.
- [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [I-D.ietf-ecrit-phonebcpl] Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling", draft-ietf-ecrit-phonebcpl-17 (work in progress), March 2011.
- [RFC5222] Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol", RFC 5222, August 2008.
- [RFC5223] Schulzrinne, H., Polk, J., and H. Tschofenig, "Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)", RFC 5223, August 2008.

### 10.2. Informative References

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

- [I-D.ietf-ecrit-framework]  
Rosen, B., Schulzrinne, H., Polk, J., and A. Newton,  
"Framework for Emergency Calling using Internet  
Multimedia", draft-ietf-ecrit-framework-12 (work in  
progress), October 2010.
- [I-D.ietf-geopriv-res-gw-lis-discovery]  
Thomson, M. and R. Bellis, "Location Information Server  
(LIS) Discovery using IP address and Reverse DNS",  
draft-ietf-geopriv-res-gw-lis-discovery-01 (work in  
progress), March 2011.
- [RFC5985] Barnes, M., "HTTP-Enabled Location Delivery (HELD)",  
RFC 5985, September 2010.
- [RFC5012] Schulzrinne, H. and R. Marshall, "Requirements for  
Emergency Context Resolution with Internet Technologies",  
RFC 5012, January 2008.
- [I-D.ietf-ecrit-location-hiding-req]  
Schulzrinne, H., Liess, L., Tschofenig, H., Stark, B., and  
A. Kuett, "Location Hiding: Problem Statement and  
Requirements", draft-ietf-ecrit-location-hiding-req-04  
(work in progress), February 2010.
- [I-D.winterbottom-geopriv-lis2lis-req]  
Winterbottom, J. and S. Norreys, "LIS to LIS Protocol  
Requirements", draft-winterbottom-geopriv-lis2lis-req-01  
(work in progress), November 2007.
- [RFC5069] Taylor, T., Tschofenig, H., Schulzrinne, H., and M.  
Shanmugam, "Security Threats and Requirements for  
Emergency Call Marking and Mapping", RFC 5069,  
January 2008.
- [I-D.ietf-geopriv-arch]  
Barnes, R., Lepinski, M., Cooper, A., Morris, J.,  
Tschofenig, H., and H. Schulzrinne, "An Architecture for  
Location and Location Privacy in Internet Applications",  
draft-ietf-geopriv-arch-03 (work in progress),  
October 2010.
- [esw07] "3rd SDO Emergency Services Workshop,  
<http://www.emergency-services-coordination.info/2007Nov/>",  
October 30th - November 1st 2007.
- [nwgstg3] "WiMAX Forum WMF-T33-001-R015V01, WiMAX Network  
Architecture Stage-3

[http://www.wimaxforum.org/sites/wimaxforum.org/files/technical\\_document/2009/09/DRAFT-T33-001-R015v01-O\\_Network-Stage3-Base.pdf](http://www.wimaxforum.org/sites/wimaxforum.org/files/technical_document/2009/09/DRAFT-T33-001-R015v01-O_Network-Stage3-Base.pdf)",  
September 2009.

## Authors' Addresses

Henning Schulzrinne  
Columbia University  
Department of Computer Science  
450 Computer Science Building  
New York, NY 10027  
US

Phone: +1 212 939 7004  
Email: [hgs+ecrit@cs.columbia.edu](mailto:hgs+ecrit@cs.columbia.edu)  
URI: <http://www.cs.columbia.edu>

Stephen McCann  
Research in Motion UK Ltd  
200 Bath Road  
Slough, Berks SL1 3XE  
UK

Phone: +44 1753 667099  
Email: [smccann@rim.com](mailto:smccann@rim.com)  
URI: <http://www.rim.com>

Gabor Bajko  
Nokia

Email: [Gabor.Bajko@nokia.com](mailto:Gabor.Bajko@nokia.com)

Hannes Tschofenig  
Nokia Siemens Networks  
Linnoitustie 6  
Espoo 02600  
Finland

Phone: +358 (50) 4871445  
Email: [Hannes.Tschofenig@gmx.net](mailto:Hannes.Tschofenig@gmx.net)  
URI: <http://www.tschofenig.priv.at>

Dirk Kroeselberg  
Siemens  
Germany

Phone:

Email: [dirk.kroeselberg@siemens.com](mailto:dirk.kroeselberg@siemens.com)





ECRIT  
Internet-Draft  
Intended status: Standards Track  
Expires: January 13, 2012

R. Marshall  
J. Martin  
TCS  
B. Rosen  
Neustar  
July 12, 2011

A LoST extension to support return of complete and similar location info  
draft-marshall-ecrit-similar-location-01

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

## Abstract

This document introduces a new way to provide returned location information in LoST responses that is either of a completed or similar form to the original input civic location, based on whether a valid or invalid location is returned within the findServiceResponse message. This document defines a new extension to the findServiceResponse message within the LoST protocol [RFC5222] that enables the LoST protocol to return a completed civic location element set for a valid response, and one or more suggested sets of civic location information for invalid LoST responses. These two types of civic addresses are referred to as either "complete" or "similar" locations, and are included as compilation of ca type xml elements within the existing response message structure.

## Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute 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 January 13, 2012.

## Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	5
2. Terminology . . . . .	6
3. Overview of Returned Location Information . . . . .	7
4. Returned Location Information . . . . .	9
5. Complete Location returned for Valid response . . . . .	10
6. Similar Location returned for Invalid Response . . . . .	12
7. Relax NG schema . . . . .	14
8. Security Considerations . . . . .	16
9. IANA Considerations . . . . .	17
10. Acknowledgements . . . . .	18
11. References . . . . .	19
11.1. Normative References . . . . .	19
11.2. Informative References . . . . .	19
Authors' Addresses . . . . .	20

## 1. Introduction

The LoST protocol [RFC5222] supports the validation of civic location information as input, by providing a set of validation result status indicators. The current usefulness of the supported xml elements, "valid", "invalid", and "unchecked", is limited, because while they each provide an indication of validity for any one element as a part of the whole address, the mechanism is insufficient in providing either the complete set of address elements that the LoST server contains, or of providing alternate suggestions (hints) as to which civic address is intended.

Whether the input civic location is valid and missing information, or invalid due to missing or wrong information during input, this document provides a mechanism to return full address information for those valid or invalid cases.

This enhancement to the validation feature within LoST is required in order to ensure a high level of address matching, to overcome user and system input errors, and to support the usefulness of location-based systems in general.

The structure of this document includes terminology, Section 2, followed by a discussion of the basic elements involved in location validation. These use of these elements, by way of example, is discussed in an overview section, Section 3, with accompanying rationale, and a brief discussion of the impacts to LoST, and its current schema.

## 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], with the important qualification that, unless otherwise stated, these terms apply to the design of the Location Configuration Protocol and the Location Dereferencing Protocol, not its implementation or application.

The following terms are defined in this document:

**Address:** The term Address is used interchangeably with the concept of Civic Location.

**Invalid:** The result of the attempt to match an individual input data as part of a larger set of data that has already been successfully matched.

**Invalid Civic Element:** An unmatched result of an individual civic location element as part of a broader set of elements that make up a civic location.

**Invalid Civic Location:** An unmatched result of an input civic location, when taken as a whole, based on one or more individual unmatched civic address elements.

**Complete Location:** An expanded civic location that includes additional address elements in addition to the existing validated civic elements provided.

**Similar Location:** A suggested civic location that is comparatively close to the civic location which was input, but which had one or more invalid element.

**Returned Location Information:** A set of standard civic location elements returned in a LoST response.

### 3. Overview of Returned Location Information

This document describes an extension to LoST [RFC5222], to allow additional location information to be returned in a `findServiceResponse` for two different use cases.

Since a LoST server often contains more data than what is often included within a `findService` request, it is expected that this additional location information could be returned within response messages that may be both valid and invalid. For valid responses, where a LoST server contains additional location information relating to that civic address, the `findServiceResponse` message can return additional location information along with the original validated elements in order to form a complete civic location.

On the other hand, for an invalid LoST response that contains address elements returned with one or more of them marked as invalid, and constituting an invalid location, this document introduces the idea of reusing this same mechanism, but for a different purpose - to supply similar location information - again, information that is contained within the LoST server, but is provided as a complete "similar" civic location put forward as a suggested alternative address that is also a valid location.

In valid location responses, this works in the following way: when a LoST server returns a response to a `findService` request that contains a set of CAtype elements considered valid, the location information in the `findServiceResponse` is extended to include additional location information specific for that location. As an example, the query may contain a HNO (house number), RD (road name) and A3 (city) but may not contain A1, A2, PC (Postal Code) CAtypes. The RD and PC elements may be sufficient to locate the address specified in the request and thus be considered valid. Yet, downstream entities may find it helpful to have the additional A1, A2, and PC location elements that exist, and so the mechanism described here supports their inclusion. Since [RFC5222] currently does not have a way for this additional location information to be returned in the `findServiceResponse`, this document extends RFC5222 so that it can include a `completeLocation` element within the `findServiceResponse` message, representing a "complete" civic location.

input address: 6000 15th Ave NW Seattle

completed address: 6000 15th Ave NW Seattle, WA 98105 US

When invalid location responses are received, the same mechanism works as follows: when a LoST server returns a response to a `findService` request that contains a set of CAtype elements with one

or more that are tagged as invalid, the location information in the `findServiceResponse` is extended to include additional location information specific for that location. Differing results in the same data used in the above example, where the RD and PC elements are not sufficient to locate a unique address leads to an "invalid" result. This is the case, despite the fact that the LoST server typically contains additional location elements which could have resulted in a uniquely identifiable location if additional data had been supplied in the query. Since [RFC5222] currently does not have a way for this additional location information to be returned in the `findServiceResponse`, this document extends RFC5222 so that it can include one or more `similarLocation` elements within the `findServiceResponse` message representing "similar" civic locations.

To show this, suppose that a similar address as above is inserted within a Lost `findService` request:

input address: 6000 15th Ave Seattle, WA.

Different from the above case, this time we make the assumption that the address is deemed "invalid" by the LoST server because there is no plain "15th Ave" in the city of Seattle with a house number that matches 6000. However there are two addresses within the address dataset that are "similar", when all parts of the address are taken as a whole. These similar addresses that could be suggested to the user are as follows:

similar address #1: 6000 15th Ave NW Seattle, WA 98107

similar address #2: 6000 15th Ave NE Seattle, WA 98105

This document proposes to include the above similar addresses as `civicAddress` elements in the response to `locationValidation`. The next section shows examples of the LoST request and response xml message fragments for the above valid and invalid scenarios, returning the complete or similar addresses, respectively:



#### 4. Returned Location Information

The LoST server knows the data that is available internally, and can determine which additional elements can be provided either as part of a complete civic location (CCL) or a similar civic location (SCL). The inclusion of either CCL or SCL is not triggered by any message parameter, but is triggered based on whether the returned location information is valid or invalid. It is not turned on or off, but is implementation specific.

## 5. Complete Location returned for Valid response

Based on the example input request, returned location information is provided in a findServiceResponse message when the original input address is considered valid, but is missing some additional data that the LoST server has.

```
<!-- ===== -->

<findService xmlns="urn:ietf:params:xml:ns:lost1"
  validateLocation="true">

  <location id="587cd3880" profile="civic">
    <civicAddress
      xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">

      <A3>Seattle</A3>
      <A6>15th</A6>
      <STS>Ave</STS>
      <POD>NW</POD>
      <HNO>6000</HNO>

    </civicAddress>
  </location>

  <service>urn:service:sos</service>

</findService>

<!-- ===== -->

<findServiceResponse xmlns="urn:ietf:params:xml:ns:lost1" >

  <mapping
    expires="NO-CACHE"
    lastUpdated="2006-11-01T01:00:00Z"
    source="authoritative.example"
    sourceId="8799e346000098aa3e">

    <displayName xml:lang="en">Seattle 911</displayName>
    <service>urn:service:sos</service>
    <uri>sip:seattle-911@example.com</uri>
    <serviceNumber>911</serviceNumber>
```

```
</mapping>

<locationValidation
  xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">

  <valid>ca:A3 ca:A6 ca:STS ca:POD ca:HNO</valid>
  <invalid></invalid>
  <unchecked></unchecked>

  <rli:completeLocation>  <!-- completed address -->
    <ca:civicAddress>
      <ca:country>US</ca:country>
      <ca:A1>WA</ca:A1>
      <ca:A3>SEATTLE</ca:A3>
      <ca:RD>15TH</ca:RD>
      <ca:STS>AVE</ca:STS>
      <ca:POD>NW</ca:POD>
      <ca:HNO>6000</ca:HNO>
      <ca:PC>98106</ca:PC>
      <ca:PCN>SEATTLE</ca:PCN>
    </ca:civicAddress>

  </rli:completeLocation>

</locationValidation>

<path>
  <via source="authoritative.example"/>
</path>

<locationUsed id="587cd3880"/>

</findServiceResponse>

<!-- ===== -->
```

## 6. Similar Location returned for Invalid Response

The following example shows returned location information provided in a findServiceResponse message when the original input address is considered invalid, because (in this case) of missing data that the LoST server needs to provide a unique mapping.

```
<!-- ===== -->

<findService xmlns="urn:ietf:params:xml:ns:lost1"
  validateLocation="true">

  <location id="587cd3880" profile="civic">
    <civicAddress
      xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">

      <country>US</country>
      <A1>WA</A1>
      <A3>Seattle</A3>
      <A6>15th Ave</A6>
      <HNO>6000</HNO>

    </civicAddress>
  </location>

  <service>urn:service:sos</service>
</findService>

<!-- ===== -->

<findServiceResponse xmlns="urn:ietf:params:xml:ns:lost1" >

  <mapping
    expires="NO-CACHE"
    lastUpdated="2006-11-01T01:00:00Z"
    source="authoritative.example"
    sourceId="8799e346000098aa3e">

    <displayName xml:lang="en">Seattle 911</displayName>
    <service>urn:service:sos</service>
    <uri>sip:seattle-911@example.com</uri>
    <serviceNumber>911</serviceNumber>

  </mapping>
```

```
<locationValidation
  xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">

  <valid>ca:country ca:A1 ca:A3</valid>
  <invalid>ca:A6</invalid>
  <unchecked>ca:HNO</unchecked>

  <rli:similarLocation>  <!-- similar location info -->
    <ca:civicAddress>  <!-- similar address #1 -->
      <ca:country>US</ca:country>
      <ca:A1>WA</ca:A1>
      <ca:A3>SEATTLE</ca:A3>
      <ca:RD>15TH</ca:RD>
      <ca:STS>AVE</ca:STS>
      <ca:POD>NW</ca:POD>
      <ca:HNO>6000</ca:HNO>
      <ca:PC>98106</ca:PC>
      <ca:PCN>SEATTLE</ca:PCN>
    </ca:civicAddress>

    <ca:civicAddress>  <!-- similar address #2 -->
      <ca:country>US</ca:country>
      <ca:A1>WA</ca:A1>
      <ca:A3>SEATTLE</ca:A3>
      <ca:RD>15TH</ca:RD>
      <ca:STS>AVE</ca:STS>
      <ca:POD>NE</ca:POD>
      <ca:HNO>6000</ca:HNO>
      <ca:PC>98105</ca:PC>
      <ca:PCN>SEATTLE</ca:PCN>
    </ca:civicAddress>
  </rli:similarLocation>

</locationValidation>

<path>
  <via source="authoritative.example"/>
</path>

<locationUsed id="587cd3880"/>

</findServiceResponse>

<!-- ===== -->
```

## 7. Relax NG schema

This section provides the Relax NG schema of LoST extensions in the compact form. The verbose form is included in a later section [TBA].

```
namespace a = "http://relaxng.org/ns/compatibility/annotations/1.0"
default namespace ns1 = "urn:ietf:params:xml:ns:lost-ext2"

##
##   Extensions to the Location-to-Service Translation (LoST)
##   Protocol

##
##   LoST Extensions define two new elements: completeLocation and
##   similarLocation.
##
start =
  completeLocation
  | similarLocation

##
##   complete Location
##
div {
  completeLocation=
    element completeLocation
}

##
##   similar Location
##
div {
  similarLocation=
    element completeLocation
}

##
##   Patterns for inclusion of elements from schemas in
##   other namespaces.
##
div {

  ##
  ##   Any element not in the LoST Extensions
  ##   namespace.
```

```
##
notLostExt = element * - (ns1:* | ns1:*) { anyElement }

##
##   A wildcard pattern for including any element
##   from any other namespace.
##
anyElement =
  (element * { anyElement }
   | attribute * { text }
   | text)*

##
##   A point where future extensions
##   (elements from other namespaces)
##   can be added.
##
extensionPoint = notLostExt*
}
```

[Editor's note: above needs refinement]

## 8. Security Considerations

Whether the input to the LoST server is valid or invalid, the LoST server ultimately determines what it considers to be valid. In the case where the input location is valid, the requester still may not actually understand where that location is. For valid location use cases, this extension returns more location information than the requester may have had which, in turn, may reveal more about the location. While this may be very desirable when, for example, supporting an emergency call, it may not be as desirable for other services. The LoST server implementation should consider the risk of releasing more detail versus the value in doing so. Generally, we do not believe this is a significant problem as the requester must have enough location information to be considered valid, which in most cases is enough to uniquely locate the address. Providing more CAtypes generally doesn't actually reveal anything more.



## 9. IANA Considerations

## 10. Acknowledgements

## 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.

### 11.2. 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](mailto:rmarshall@telecomsys.com)  
URI: <http://www.telecomsys.com>

Jeff Martin  
TeleCommunication Systems, Inc.  
2401 Elliott Avenue  
2nd Floor  
Seattle, WA 98121  
US

Phone: +1 206 792 2584  
Email: [jmartin@telecomsys.com](mailto:jmartin@telecomsys.com)  
URI: <http://www.telecomsys.com>

Brian Rosen  
Neustar  
470 Conrad Dr  
Mars, PA 16046  
US

Phone:  
Email: [br@brianrosen.net](mailto:br@brianrosen.net)  
URI:



Network Working Group  
Internet-Draft  
Expires: December 6, 2011  
Intended Status: Standards Track

James Polk  
Cisco Systems  
June 6, 2011

IANA Registering a SIP Resource Priority Header Field  
Namespace for Local Emergency Communications  
draft-polk-local-emergency-rph-namespace-01

## Abstract

This document creates the new Session Initiation Protocol (SIP) Resource Priority header field namespace "esnet" for local emergency usage to a public safety answering point (PSAP), between PSAPs, and between a PSAP and first responders and their organizations, and places this namespace in the IANA registry.

## Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on December 6, 2011.

## Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Rules of Usage of the Resource Priority Header . . . . .	3
3. "esnet" Namespace Definition . . . . .	5
3.1 Namespace Definition Rules and Guidelines . . . . .	5
3.2 The "esnet" Namespace . . . . .	5
4. IANA Considerations . . . . .	6
4.1 IANA Resource-Priority Namespace Registration . . . . .	6
4.2 IANA Priority-Value Registrations . . . . .	6
5. Security Considerations . . . . .	6
6. Acknowledgements . . . . .	7
7. References . . . . .	7
7.1 Normative References . . . . .	7
7.2 Informative References . . . . .	7
Author's Address . . . . .	7

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].

## 1. Introduction

This document creates the new Session Initiation Protocol (SIP) Resource Priority header field namespace "esnet" for local emergency usage and places this namespace in the IANA registry. The SIP Resource-Priority header field is defined in RFC 4412 [RFC4412]. This new namespace can be used for inbound calls towards a public safety answering point (PSAP), between PSAPs, and between a PSAP and first responders or their organizations.

This new namespace can be included in SIP requests to provide an explicit priority indication within controlled environments, such as an IMS infrastructure or Emergency Services network (ESInet) where misuse can be reduced to a minimum because these types of networks have great controls in place. The function is to facilitate differing treatment of emergency SIP requests according to local policy, or more likely, a contractual agreement between the network organizations. This indication is used solely to differentiate certain SIP requests, transactions or dialogs, from other SIP requests, transactions or dialogs that do not have the need for priority treatment. If there are differing, yet still understandable and valid Resource-Priority header values in separate SIP requests, then this indication can be used by local policy to determine which SIP request, transaction or dialog receives which treatment (likely better or worse than another).

It can also be imagined that Application Service Providers (ASP)

directly attached to an ESInet can have a trust relationship with the ESInet such that within these networks, SIP requests (thereby the session they establish) make use of this "esnet" namespace for appropriate treatment.

This document merely creates the namespace, per the rules within [RFC4412], necessitating a Standards Track RFC for IANA registering new RPH namespaces and their relative priority-value order.

There is the possibility that within emergency services networks, provided local policy supports enabling this function, a Multilevel Precedence and Preemption (MLPP)-like behavior can be achieved (likely without the 'preemption' part). This will ensure more the important calls are established or retained; therefore the "esnet" namespace is given 5 priority-levels. MLPP-like SIP signaling is not defined in this document for 911/112/999 style emergency calling, but it is not prevented either.

Within the ESInet, there will be emergency calls requiring different treatments, according to the type of call. Does a citizen's call to a PSAP require the same, a higher or a lower relative priority than a PSAP's call to a police department, or the police chief? What about either relative to a call from within the ESInet to a federal government's department of national security, such as the US Department of Homeland Security? For this reason, the "esnet" namespace is given multiple priority levels.

This document does not define any of these behaviors, outside of reminding readers that the rules of RFC 4412 apply - though examples of usage are included for completeness. This document IANA registers the "esnet" RPH namespace for use within any emergency services networks, not just of those from citizens to PSAPs.

## 2. Rules of Usage of the Resource Priority Header field

This document retains the behaviours of the SIP Resource Priority header field, defined in [RFC4412], during the treatment options surrounding this new "esnet" namespace. The usage of the "esnet" namespace does not have a 'normal', or routine call level, given the environment this is to be used within (i.e., within an ESInet). That is for local jurisdictions to define within their respective parts of the ESInet- which could be islands of local administration.

RFC 4412 states that modifying the relative priority ordering or the number of priority-values to a registered namespace SHOULD NOT occur within the same administrative domain due to interoperability issues with dissimilar implementations.

The "esnet" namespace SHOULD only be used in times of an emergency, where at least one end of the signaling is within a local emergency organization.



The "esnet" namespace has 5 priority-values, in a specified relative priority order, and is registered as a queue-based namespace in compliance with [RFC4412]. Individual jurisdictions MAY configure their SIP entities for preemption treatment. This is OPTIONAL, subject to local policy decisions.

The following network diagram provides one example of local policy choices for the use of the "esnet" namespace:

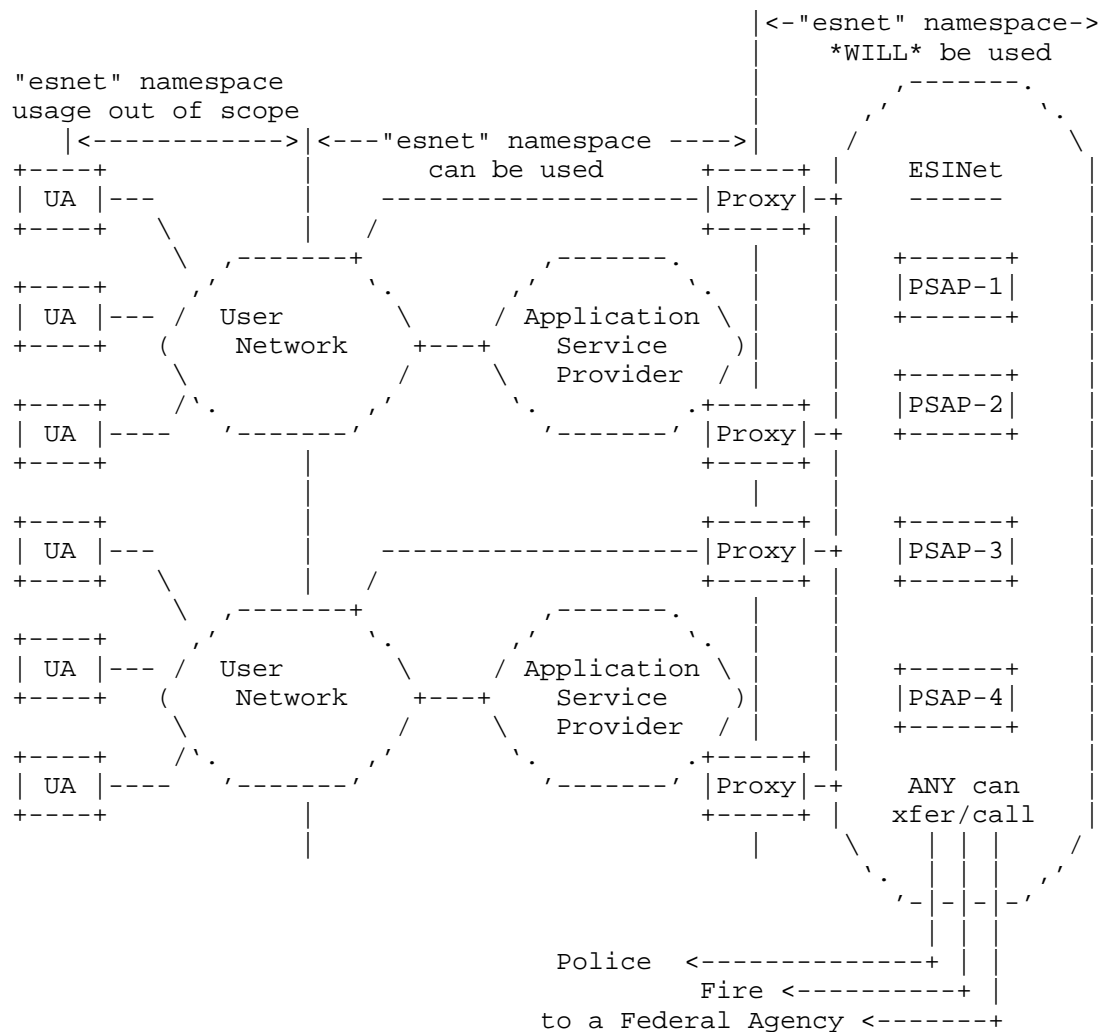


Figure 1: A possible network architecture using "esnet" namespace

In Figure 1., the "esnet" namespace is intended for usage within the ESInet on the right side of the diagram. How it is specifically utilized is out of scope for this document, and left to local jurisdictions to define. Adjacent ASPs to the ESInet MAY have a

trust relationship that includes allowing this/these neighboring ASP(s) to use the "esnet" namespace to differentiate SIP requests and dialogs within the ASP's network. The exact mapping between the internal and external sides of the edge proxy at the ESInet boundaries is out of scope of this document.

### 3. "esnet" Namespace Definition

The "esnet" namespace should not to be considered generic for all emergencies because there are a lot of different kinds of emergencies, some on a military scale ([RFC4412] defines 3 of these), some on a national scale ([RFC4412] defines 2 of these), some on an international scale. Each type of emergency can also have its own namespace(s), and although there are 45 defined for other uses, more are possible - so the 911/112/999 style of public user emergency calling for police or fire or ambulance (etc) does not have a monopoly on the word "emergency".

The namespace "esnet" has been chosen, roughly to stand for "Emergency Services NETwork", for a citizen's call for help from a public authority type of organization. This namespace will also be used for communications between emergency authorities, and MAY be used for emergency authorities calling public citizens. An example of the latter is a PSAP operator calling back someone who previously called 911/112/999 and the communication was terminated before it - in the PSAP operator's judgment - should have been. Here is an example of a Resource-Priority header field using the "esnet" namespace:

Resource-Priority: esnet.0

#### 3.1. Namespace Definition Rules and Guidelines

This specification defines one unique namespace for emergency calling scenarios, "esnet", constituting its registration with IANA. This IANA registration contains the facets defined in Section 9 of [RFC4412].

#### 3.2. The "esnet" Namespace

Per the rules of [RFC4412], each namespace has a finite set of relative priority-value(s), listed (below) from lowest priority to highest priority. In an attempt to not limit this namespace's use in the future, more than one priority-value is assigned to the "esnet" namespace. This document does not recommend which Priority-value is used where. That is for another document to specify. This document does RECOMMEND the choice within a national jurisdiction be coordinated by all sub-jurisdictions to maintain uniform SIP behavior throughout an emergency calling system of that country.

The relative priority order for the "esnet" namespace is as follows:

```
(lowest)  esnet.0
          esnet.1
          esnet.2
          esnet.3
(highest) esnet.4
```

The "esnet" namespace will be designated into the priority queuing algorithm (Section 4.5.2 of [RFC4412]). However, as a policy decision, local jurisdiction(s) MAY configure their SIP infrastructure to use the this namespace in a preemption algorithm way, defined in RFC 4412. This document does not recommend this usage, but it is permissible according to this specification.

The remaining rules originated in RFC 4412 apply with regard to an RP actor, who understands more than one namespace, and MUST maintain its locally significant relative priority order.

## 4. IANA Considerations

### 4.1 IANA Resource-Priority Namespace Registration

Within the "Resource-Priority Namespaces" of the sip-parameters section of IANA (created by [RFC4412]), the following entries will be added to this table:

Namespace	Levels	Intended Algorithm	New warn- code	New resp. code	Reference
-----	-----	-----	-----	-----	-----
esnet	5	queue	no	no	[This doc]

### 4.2 IANA Priority-Value Registrations

Within the Resource-Priority Priority-values registry of the sip-parameters section of IANA, the following (below) is to be added to the table:

```
Namespace: esnet
Reference: (this document)
Priority-Values (least to greatest): "0", "1", "2", "3", "4"
```

## 5. Security Considerations

The Security considerations that apply to RFC 4412 [RFC4412] apply here.

Within a network that is enabled to act on the Resource-Priority header field within SIP requests, the implications of using this

namespace within the field incorrectly can potentially cause a large impact on a network, given that this indication is to give preferential treatment of marked traffic great preference within the network verses other traffic. This document does not indicate this marking is intended for use by endpoints, yet protections need to be taken to prevent granting preferential treatment to unauthorized users not calling for emergency help.

A simple means of preventing this usage into an ESInet is to not allow "esnet" marked traffic to get preferential treatment unless the destination is towards the local/regional ESInet. This is not a consideration for internetwork traffic within the ESInet, or generated out of the ESInet. 911/112/999 type of calling is fairly local in nature, with a finite number of URIs that are considered valid.

## 6. Acknowledgements

Thanks to Ken Carlberg, Janet Gunn, Fred Baker and Keith Drage for help and encouragement with this effort. Thanks to Henning Schulzrinne, Ted Hardie, Hannes Tschofenig, Brian Rosen, Janet Gunn and Marc Linsner for constructive comments.

## 7. References

### 7.1 Normative References

- [RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997
- [RFC4412] Schulzrinne, H., Polk, J., "Communications Resource Priority for the Session Initiation Protocol (SIP)", RFC 4411, Feb 2006

### 7.2 Informative References

none

## Author's Address

James Polk  
3913 Treemont Circle  
Colleyville, Texas 76034  
USA  
Phone: +1-817-271-3552  
Email: jmpolk@cisco.com