ECRIT Direct Emergency Calling
draft-winterbottom-ecrit-direct-02.txt

Abstract

The specified IETF emergency services architecture puts a strong emphasis on emergency call and emergency messaging via the Voice Service Provider (VSP) / Application Service Provider (ASP). There are two reasons for this design decision: The call routing via the VSP/ASP is more natural as it follows the standard communication pattern and transition deployments assume non-updated end hosts.
As the deployment of the Location-to-Service Translation protocol progresses there are possibilities for upgraded end devices to directly communicate with the IP-based emergency services network without the need to interact with a VSP/ASP, which simplifies the task of regulators as the involved parties are within the same jurisdiction. This memo describes the procedures and operations of a generic emergency calling client utilizing the available building blocks.

Status of this Memo

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html.
This Internet-Draft will expire on September 9, 2010.

Copyright Notice

Table of Contents

---

1. Introduction   TOC

The description of the IETF emergency services architecture, found in
[I-D.ietf-ecrit-phonebcp] (Rosen, B. and J. Polk, "Best Current
Practice for Communications Services in support of Emergency Calling,"

January 2010.) and in [I-D.ietf-ecrit-framework] (Rosen, B.,
Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency
Calling using Internet Multimedia," July 2009.), focuses on devices
where emergency calls are routed primarily through the subscriber's
home VSP and the direct signaling communication between the end host
and the Public Safety Answering Point (PSAP) that contains the IP-based
PSAP is only an exception. This is a convenient assumption if one
considers the regular communication patterns of the device and the
potential proprietary protocol implementations used between the end
host and the VSP and the ability to move the interoperability
challenges away from the end device and closer to VSPs. There are,
however, challenges for regulators to enforce emergency services
functionality when the VSP is located in a different jurisdiction.
Inclusion of a VSP introduces unnecessary elements into the emergency
call path making the overall solution more cumbersome.
With the help of the Location-to-Service Translation protocol a PSAP
URI is discovered that allows the end device to directly send SIP
communication requests towards the PSAP.
Note that the information returned by LoST may not necessarily be the
address of the PSAP itself but might rather be an entity that gets the
emergency call closer to the PSAP by returning the address of an
Emergency Services Routing Proxy (ESRP).
The intent of this client is that it will be able to use the available
ECRIT building blocks to allow any IP enabled device with access to the
Internet to make an emergency call without requiring the signaling
interaction with the VSP. In fact, there is no assumption or
requirement for a VSP subscription to exist. The interacting entities
are shown in Figure 1 (Network Configuration).

```
                     ....    ....
                   ,'     ','     ',
                  ;               ;
     +--------+   ;               ;      +------+
     | Device |--->:      ISP     :----->| ESRP |
     +--------+   ;               ;      +------+
                  `,       ,',      ,'
                   '     ,' ',     ,'
                    '   ,'   ',   ,'
                     ````     ````
```
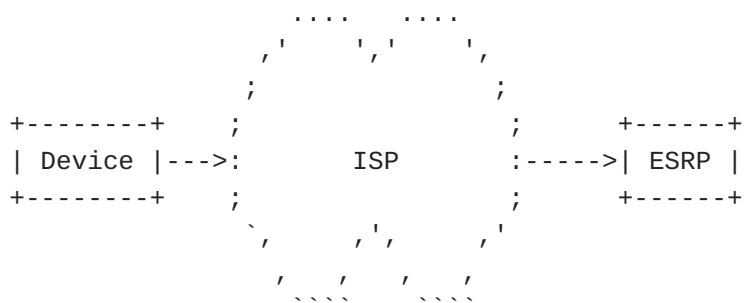
**Figure 1: Network Configuration**

Furthermore, a means for call-back in the event of a dropped call is
also described.

## 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] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.).

## 3.  The Jurisdictional Problem

The jurisdictional problem is illustrated with Figure 2 (Jurisdictional Boundaries in Internet Emergency Calling) that highlights that provided the data in the Location Information Server (LIS) and the LoST server are correct, that the caller and the PSAP are assured of being in the same regulatory jurisdiction. This is important, because it shows that it is the access component of the network and not the service component against which reguatory obligations can be imposed with any hope of enforcement. Regulation without the possibility of enforcement is challenging as there is very little coordination between regulators world wide in this area, consequently any emergency calling procedure should ensure that all nodes against which the procedures apply fall within the same regulatory boundary.

```
                          +-----+
                          | VSP |
                          |  #  |
                          +-----+


       o-------------o----------------------o------------o
      /                                                   \
     /   +---------+                    +--------+     \
    /    |  Access  \                  /  ESINet  \       \
   o     | Network   \                /            \       o
   |     +           +               +     O        +      |
   |    /    O        |             /     <P\       |      |
   |   +    <C\       o   REGULATORY  +    /'\       +      |
   |   |    /'\      /               |    PSAP       /      o
   o   +  Caller   +   JURISDICTION  +  +-------+  +      /
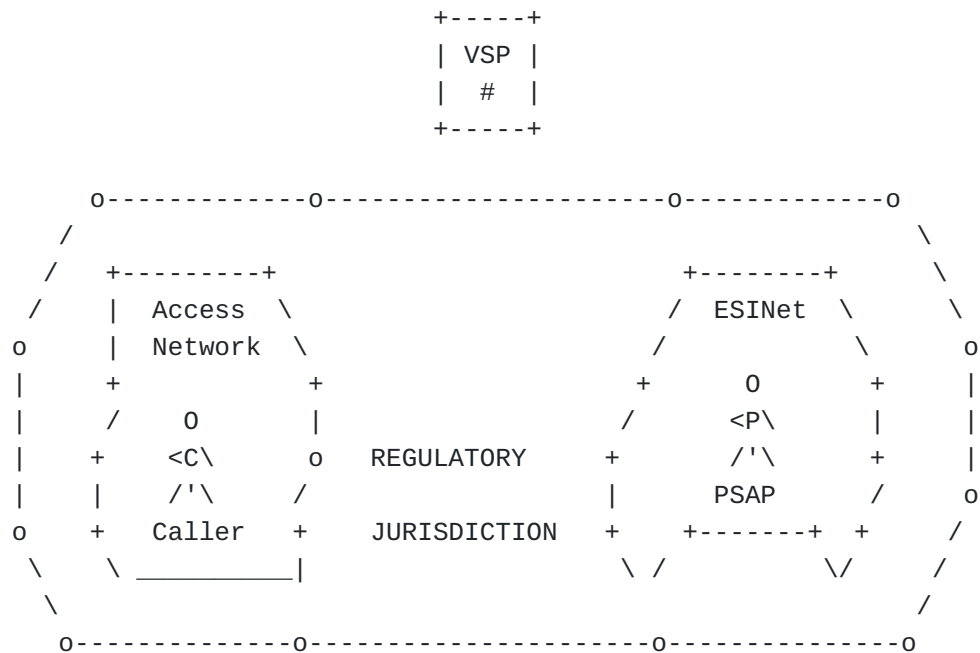    \    \ _____|               \ /          \/     /
     \                               \                 /
      o-------------o----------------------o---------------o
```

Figure 2: Jurisdictional Boundaries in Internet Emergency Calling

---

4. ESRP Route Determination [TOC]

The ESRP is discovered by the emergency client obtaining its location from a LIS, for example, using HELD, and then using LoST to resolve the location and 'urn:services.sos' Service URN to the ESRP URI.
When the emergency client is started the device needs to perform LIS and LoST server discovery, as described in Section 7 of [I-D.ietf-ecrit-phonebcp] (Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling," January 2010.).
The emergency client MUST support location acquisition and the LCPs described in Section 6.5 of [I-D.ietf-ecrit-phonebcp] (Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling," January 2010.). The description in Section 6.5 and 6.6 of [I-D.ietf-ecrit-phonebcp] (Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling," January 2010.) regarding the interaction between the device and the LIS applies to this document.
The emergency client MUST use LoST [RFC5222] (Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol," August 2008.) to obtain an ESRP URI. The exact

timing of individual LoST lookups may vary based on a number of
factors, including the design of the user interface. For example, a
hypothetical user interface may offer an emergency call button that
triggers a <listServicesByLocation> interaction to learn about the
available emergency services (potentially using the serviceListBoundary
extension defined in [I-D.ietf-ecrit-lost-servicelistboundary] (Wolf,
K., "LoST Service List Boundary Extension," February 2010.)). The
service options may be presented to the emergency caller in a graphical
fashion and once a specific service is selected a LoST query would be
initiated (unless a cached mapping is available that makes this request
obsolete). The LoST <findService> query to obtain the ESRP URI for the
selected service is in this example initiated at the time the emergency
call setup is performed. It is recommended that ESRP discovery occurs
at call time.

---

5. Emergency Client Registration

Emergency registration is only necessary when an emergency call
procedure is initiated. Immediately prior to making an emergency call,
the emergency client performs a SIP emergency registration with the
registrar in the ESRP, the ESRP-registrar. The emergency registration
is a SIP registration with specific options and headers which are
required in order to guard the emergency network and ensure callback
should it be required.
Each emergency client MUST provide an instance-id, as defined in
[I-D.ietf-sip-outbound] (Jennings, C., "Managing Client Initiated
Connections in the Session Initiation Protocol (SIP)," June 2009.),
this allows the ESRP-registrar to generate a GRUU [RFC5627] (Rosenberg,
J., "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in
the Session Initiation Protocol (SIP)," October 2009.) that can be used
as a callback identifier. A GRUU is necessary as the callback
identifier because the emergency client does not provide a longer-term
contact address to the ESRP-registrar prior to registration, and the
GRUU provides a handle by which the PSAP can identify the calling
emergency client. To simplify the emergency client and ESRP-registrar
implementations, only public GRUUs are provided by the ESRP-registrar.
The public GRUU is guaranteed to be the same for a device regardless of
re-registration with a different call-id, which may occur if the device
unexpectedly reboots. This is not true for temporary GRUUs, which makes
temporary GRUUs undesriable in the scope of this application space.
The PSAP is able to define and mandate the time over which callback is
possible. This needs to be a reasonable period of time, nominally 10s
of minutes, as the device may well be transient with regards to network
attachment. The ESRP-registrar selects a registration period based on
local policy. The emergency client MUST accept a registration for at

least 60 minutes, but MAY accept longer registrations based on its own policy.

In the event that a registration is lost by the emergency client prior to reaching registration expiry then the emergency client MUST re-register with the ESRP-registrar and SHOULD use the same call-id. In this circumstance the ESRP-registrar SHOULD match the instance-id and the call-id to recognize that it is a re-registration for a dropped connection, and expiry time in the registration response SHOULD be set to the time remaining when the original registration occurred.

[I-D.ietf-sip-outbound] (Jennings, C., "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)," June 2009.) requires a device to support at least 2 registrations to different proxies. The emergency client requirements in this memo relax this requirement down to one registration, but more than one is allowed. There are several reasons for relaxing the connection redundancy requirement. Firstly, ESRPs are expected to have inbuilt redundancy, so if a connection is dropped due to a failed proxy in the ESRP, then a new connection or registration will automatically be directed to an active proxy in the ESRP cluster. If the connection dropped because of some other failure along the path from the emergency client to the ESRP, then multiple SIP registrations are unlikely to provide any measurable reliability improvements since single points of failure in this path are inherently likely. Secondly, re-registrations only occur immediately prior to call placement, so any outbound failure will also likely result in the call dropping. If this occurs then the emergency client MUST re-register with the ESRP-registrar, and since instance-id and public GRUU will remain unchanged as a result of this, the emergency client can either receive a callback from the PSAP, or it can initiate a new call to the emergency network.

Location information is critical to emergency calling. Providing location information to the calling-entity with sufficient granularity to allow ESRP route determination is crucial. Since this must occur prior to the emergency client registering with the ESRP-registrar, the emergency client must have access to a certain amount of location information (and the amount varies depending on the specific emergency services deployment architecture).

The device SHOULD include all the location information it has when registering with the ERSP-registrar. Inclusion of location information in SIP REGISTER messages is specified in [I-D.ietf-sipcore-location-conveyance] (Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol," February 2010.). There are three possible execution paths for the ESRP-registrar when receiving a REGISTER message:

1. If the REGISTER message does not include location information the ESRP-registrar MUST use HELD identity [I-D.ietf-geopriv-held-identity-extensions] (Winterbottom, J., Thomson, M., Tschofenig, H., and R. Barnes, "Use of Device Identity in HTTP-Enabled Location Delivery (HELD),"

February 2010.) to obtain the location of the device as both a location value and reference. In order to contact the LIS the ESRP-registrar SHOULD determine the LIS address using the mechanism described in [I-D.thomson-geopriv-res-gw-lis-discovery] (Thomson, M. and R. Bellis, "Location Information Server (LIS) Discovery using IP address and Reverse DNS," January 2010.). The ESRP-registrar MAY use other methods for LIS determination where available.

2. If the REGISTER message contains a location URI then the ESRP-registrar MUST dereference it so that it has a location available to route the impending emergency call. The ESRP-registrar MAY validate the LIS address in the location URI with that of the LIS serving the network from which the REGISTER message originated.

3. The REGISTER message contains location information by value. Any actions performed by the ESRP-registrar to valid this information are specific to the jurisdiction in which the ESRP operates and are out of the scope of this document.

Where location conveyance is used confidentiality protection SHOULD be provided using Transport Layer Security (TLS).
Figure 3 (Example Registration Message Flow) show the registration message exchange graphically.

```
+--------+                +-----+              +------+          +------+
| Device |                | LIS |              | LoST |          | ESRP |
+--------+                +-----+              +------+          +------+
    |                        |                    |                 |
    +<----LIS Discovery---->+                    |                 |
    |                        |                    |                 |
    +----locationRequest--->+                    |                 |
    |                        |                    |                 |
    +<---locationResponse---|                    |                 |
    |                        |                    |                 |
    +------------------findService------------->+                 |
    |                        |                    |                 |
    +<--------------findServiceResponse---------+                 |
    |                        |                    |                 |
    +----------------------REGISTER----------------------------->+
    |                        |                    |                 |
    |                       +<------locationRequest-----------+
    |                        |                    |                 |
    |                       +-------locationResponse--------->+
    |                        |                    |                 |
    +<-----------------------200 OK ----------------------------+
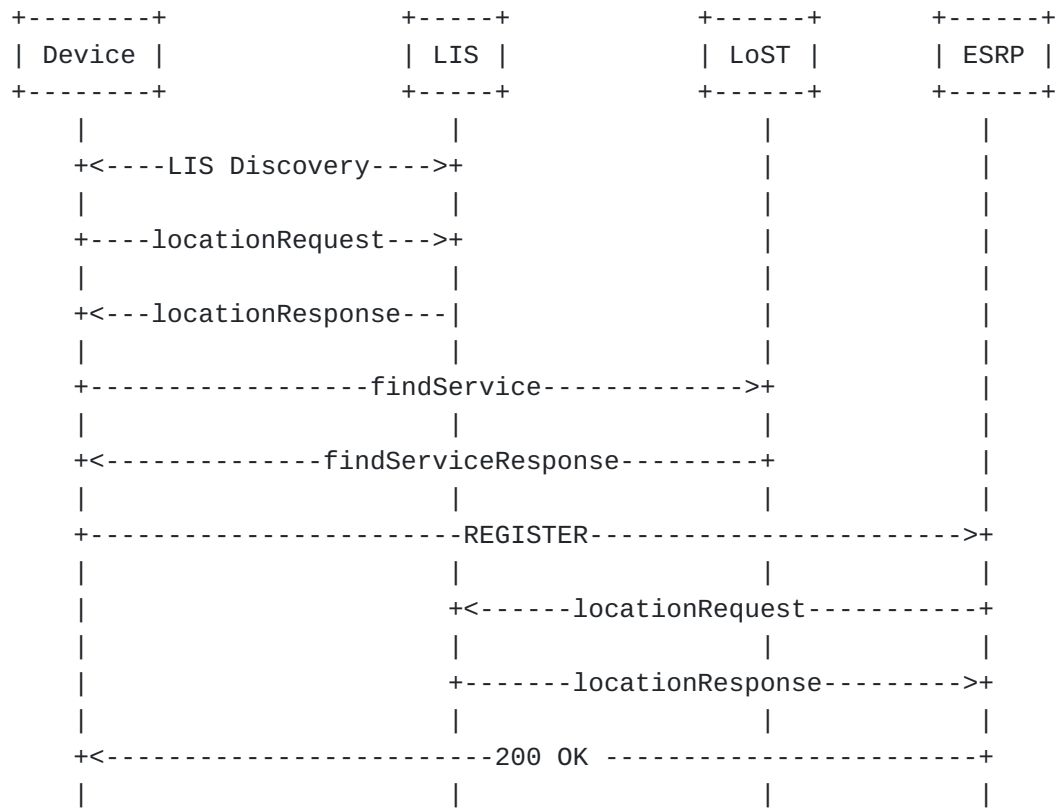    |                        |                    |                 |
```

Figure 3: Example Registration Message Flow

```
REGISTER sip:sos.example.com SIP/2.0
Via: SIP/2.0/TCP 192.0.2.2;branch=z9hG4bKnashds7
Max-Forwards: 70
From: anon <sip:anon@sos.example.com>;tag=7F94778B653B
To: anon <sip:anon@sos.example.com>
Call-ID: 16CB75F21C70
CSeq: 1 REGISTER
Geolocation: <https://lis.access.example.com:9192/suXweu838737d72>
  ;inserted-by="anon@192.0.2.2"
  ;routing-allowed=yes
Geolocation: <cid:target123@192.0.2.2>
  ;inserted-by="anon@192.0.2.2"
  ;routing-allowed=no
Require: gruu, geolocation
Supported: outbound, gruu
   Contact: <sip:anon@192.0.2.2;transport=tcp>
 ;+sip.instance="<urn:uuid:00000000-0000-1000-8000-AABBCCDDEEFF>"
Content-Type: multipart/mixed; boundary=boundary1
Content-Length: ...
```

Figure 4: Sample REGISTER message

Since the emergency client does not have a domain, it MUST register in
the same domain as the ESRP. This is illustrated in the example
REGISTER message show in [Figure 4 (Sample REGISTER message)](#).

---

6. Emergency Client Call Intitiation

Immediately subsequent to the registration a SIP INVITE request is sent
to the ESRP in the following form:

1. The Request URI MUST be the service URN [RFC5031] (Schulzrinne,
   H., "A Uniform Resource Name (URN) for Emergency and Other
   Well-Known Services," January 2008.) in the "sos" tree.

2. The To header MUST be a service URN in the "sos" tree.

3. The From header MUST be present and MUST be the public GRUU
   returned from the registration with the ESRP-registrar.

4. A Route header MUST be present with an ESRP URI, obtained from
   LoST.

5. A Contact header MUST be present and contain the public GRUU [RFC5627] (Rosenberg, J., "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)," October 2009.), and be valid for several minutes following the termination of the call, provided that the UAC remains registered with the same registrar, to permit an immediate call-back to the specific device which placed the emergency call.

6. A SDP offer MUST be included in the INVITE. If voice is supported the offer MUST include the G.711 codec, see Section 14 of [I-D.ietf-ecrit-phonebcp] (Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling," January 2010.).

7. SIP Caller Preferences [RFC3841] (Rosenberg, J., Schulzrinne, H., and P. Kyzivat, "Caller Preferences for the Session Initiation Protocol (SIP)," August 2004.) SHOULD be used to signal how the PSAP should handle the call. For example, a language preference expressed in an Accept-Language header may be used as a hint to cause the PSAP to route the call to a call taker who speaks the requested language. SIP Caller Preferences may also be used to indicate a need to invoke a relay service for communication with people with disabilities in the call.

---

7. Call Termination Control

The description in [I-D.rosen-ecrit-premature-disconnect-rqmts] (Rosen, B., "Requirements for handling abandoned calls and premature disconnects in emergency calls on the Internet," January 2009.) is relevant for this document.

---

8. SIP Feature Restrictions

The functionality defined in Section 9.3 in [I-D.ietf-ecrit-phonebcp] (Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling," January 2010.) regarding disabling of certain features is relevant for this document and an emergency client MUST NOT implement the the features listed in ED-70, and ED-71.

9. Testing

The description in Section 15 of [I-D.ietf-ecrit-phonebcp] (Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling," January 2010.) regarding emergency call testing is used by this specification. Since this specification mandates a registration with the ESRP-registrar a similar tagging URI to that described in [I-D.patel-ecrit-sos-parameter] (Patel, M., "SOS Uniform Resource Identifier (URI) Parameter for Marking of Session Initiation Protocol (SIP) Requests related to Emergency Services," February 2010.) is used to indicate a test registration. Test registrations SHALL be of short durations, but MUST be long enough to allow completion of a "test call" as described in [I-D.ietf-ecrit-phonebcp] (Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling," January 2010.).

9.1. Test Registration

When the emergency client sends a REGISTER request for emergency test registration, the "sos.test" URI parameter MUST be appended to the URI in the Contact header. This indicates to the ESRP-registrar that the request is for emergency test registration.

```
...
   Contact: <sip:anon@192.0.2.2;transport=tcp;sos.test>
 ;+sip.instance="<urn:uuid:00000000-0000-1000-8000-AABBCCDDEEFF>"
Content-Type: multipart/mixed; boundary=boundary1
Content-Length: ...
```

Figure 5: Test REGISTER Message Fragment

Only one Contact header field SHOULD be included in the emergency REGISTER test request. If more than one Contact header is included then the presence of the "sos.test" URI in any of the Contact fields SHALL result in the ESRP-registrar treating the registration as a test registration.

9.2. Format

The following syntax specification uses the augmented Backus-Naur Form
(BNF) as described in [RFC5234] (Crocker, D. and P. Overell, "Augmented
BNF for Syntax Specifications: ABNF," January 2008.).
The "sos.test" URI parameter is a "uri-parameter", as defined by
[RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A.,
Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session
Initiation Protocol," June 2002.).
uri-parameter =/ sos-param-test
sos-param-test = "sos.test"

---

10. PSAP Callback

PSAP callback occurs as described in
[I-D.schulzrinne-ecrit-psap-callback] (Schulzrinne, H., Tschofenig, H.,
and M. Patel, "Public Safety Answering Point (PSAP) Callbacks,"
March 2010.).

---

11. Security Considerations

TBD

---

12. IANA Considerations

This specification defines one new SIP URI parameter, as per the
registry created by [RFC3969] (Camarillo, G., "The Internet Assigned
Number Authority (IANA) Uniform Resource Identifier (URI) Parameter
Registry for the Session Initiation Protocol (SIP)," December 2004.).
Parameter Name: sos.test
Predefined Values: none
Reference: [RFCXXXX]
[NOTE TO IANA: Please replace XXXX with the RFC number of this
specification.]

---

13. Acknowledgements

Thanks to Elaine Quah for being a sounding board.

14. References

14.1. Normative References

[I-D.ietf-ecrit-phonebcp]	Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling," draft-ietf-ecrit-phonebcp-14 (work in progress), January 2010 (TXT).
[I-D.ietf-geopriv-held-identity-extensions]	Winterbottom, J., Thomson, M., Tschofenig, H., and R. Barnes, "Use of Device Identity in HTTP-Enabled Location Delivery (HELD)," draft-ietf-geopriv-held-identity-extensions-03 (work in progress), February 2010 (TXT).
[I-D.ietf-sip-outbound]	Jennings, C., "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)," draft-ietf-sip-outbound-20 (work in progress), June 2009 (TXT).
[I-D.ietf-sipcore-location-conveyance]	Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol," draft-ietf-sipcore-location-conveyance-02 (work in progress), February 2010 (TXT).
[I-D.schulzrinne-ecrit-psap-callback]	Schulzrinne, H., Tschofenig, H., and M. Patel, "Public Safety Answering Point (PSAP) Callbacks," draft-schulzrinne-ecrit-psap-callback-03 (work in progress), March 2010 (TXT).
[I-D.thomson-geopriv-res-gw-lis-discovery]	Thomson, M. and R. Bellis, "Location Information Server (LIS) Discovery using IP address and Reverse DNS," draft-thomson-geopriv-res-gw-lis-discovery-03 (work in progress), January 2010 (TXT).
[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[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 (TXT).
[RFC3841]	Rosenberg, J., Schulzrinne, H., and P. Kyzivat, "Caller Preferences for the Session Initiation Protocol (SIP)," RFC 3841, August 2004 (TXT).
[RFC3969]	

	Camarillo, G., "The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)," BCP 99, RFC 3969, December 2004 (TXT).
[RFC5031]	Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services," RFC 5031, January 2008 (TXT).
[RFC5222]	Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol," RFC 5222, August 2008 (TXT).
[RFC5234]	Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," STD 68, RFC 5234, January 2008 (TXT).
[RFC5627]	Rosenberg, J., "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)," RFC 5627, October 2009 (TXT).

14.2. Informative References

[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-10 (work in progress), July 2009 (TXT).
[I-D.ietf-ecrit-lost-servicelistboundary]	Wolf, K., "LoST Service List Boundary Extension," draft-ietf-ecrit-lost-servicelistboundary-03 (work in progress), February 2010 (TXT).
[I-D.patel-ecrit-sos-parameter]	Patel, M., "SOS Uniform Resource Identifier (URI) Parameter for Marking of Session Initiation Protocol (SIP) Requests related to Emergency Services," draft-patel-ecrit-sos-parameter-08 (work in progress), February 2010 (TXT).
[I-D.rosen-ecrit-premature-disconnect-rqmts]	Rosen, B., "Requirements for handling abandoned calls and premature disconnects in emergency calls on the Internet," draft-rosen-ecrit-premature-disconnect-rqmts-02 (work in progress), January 2009 (TXT).

Authors' Addresses

	James Winterbottom
	Andrew Corporation
	Andrew Building (39)
	University of Wollongong, NSW 2500
	AU
Email:	james.winterbottom@andrew.com
	Martin Thomson
	Andrew Corporation
	Andrew Building (39)
	University of Wollongong, NSW 2500
	AU
Email:	martin.thomson@andrew.com
	Hannes Tschofenig
	Nokia Siemens Networks
	Linnoitustie 6
	Espoo, 02 600
	Finland
Email:	Hannes.Tschofenig@gmx.net
	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
URI:	http://www.cs.columbia.edu