ecrit	B. Rosen	
Internet-Draft	NeuStar	
Intended status: BCP	J. Polk	
Expires: August 31, 2009	Cisco Systems	
	February 27, 2009	

TOC

Best Current Practice for Communications Services in support of Emergency Calling
draft-ietf-ecrit-phonebcp-08

Status of this Memo

Copyright Notice

Abstract

The IETF and other standards organization have efforts targeted at standardizing various aspects of placing emergency calls on IP networks. This memo describes best current practice on how devices, networks and services should use such standards to make emergency calls.

Table of Contents

1. Terminology
2. Introduction
3. Overview of how emergency calls are placed
4. Which devices and services should support emergency calls
5. Identifying an emergency call
6. Location and its role in an emergency call
    - 6.1. Types of location information
    - 6.2. Location Determination
        - 6.2.1. User-entered location information
        - 6.2.2. Access network "wire database" location information
        - 6.2.3. End-system measured location information
        - 6.2.4. Network-measured location information
    - 6.3. Who adds location, endpoint or proxy
    - 6.4. Location and references to location
    - 6.5. End system location configuration
    - 6.6. When location should be configured
    - 6.7. Conveying location in SIP
    - 6.8. Location updates
    - 6.9. Multiple locations
    - 6.10. Location validation
    - 6.11. Default location
    - 6.12. Other location considerations
7. LIS and LoST Discovery
8. Routing the call to the PSAP
9. Signaling of emergency calls
    - 9.1. Use of TLS
    - 9.2. SIP signaling requirements for User Agents
    - 9.3. SIP signaling requirements for proxy servers
10. Call backs
11. Mid-call behavior
12. Call termination
13. Disabling of features
14. Media
15. Testing
16. Security Considerations
17. IANA Considerations
18. Acknowledgements
19. References
    - 19.1. Normative References
    - 19.2. Informative References

Appendix A. BCP Requirements Sorted by Responsible Party
    - A.1. Requirements of End Devices
    - A.2. Requirements of Service Providers
    - A.3. Requirements of Access Network
    - A.4. Requirements of Intermediate Devices

§ Authors' Addresses

1. Terminology

TOC

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.).

This document uses terms from [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.), [RFC5012] (Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies," January 2008.) and [I-D.ietf-ecrit-framework] (Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet Multimedia," July 2009.).

2. Introduction

TOC

This document describes how access networks, SIP user agents, proxy servers and PSAPs support emergency calling, as outlined in [I-D.ietf-ecrit-framework] (Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet Multimedia," July 2009.), which is designed to complement the present document in section headings, numbering and content. This BCP succinctly describes the requirements of end devices and applications (requirements prefaced by "ED-"), access networks (including enterprise access networks) (requirements prefaced by "AN-", service providers (requirements prefaced by "SP-") and PSAPs to achieve globally interoperable emergency calling on the Internet.

This document also defines requirements for "Intermediate" devices which exist between end devices or applications and the access network. For example, a home router is an "Intermediate" device. Reporting location on an emergency call (see Section 6 (Location and its role in an emergency call)) may depend on the ability of such intermediate devices to meet the requirements prefaced by "INT-".

TOC

3. Overview of how emergency calls are placed

An emergency call can be distinguished (Section 5 (Identifying an emergency call)) from any other call by a unique Service URN [RFC5031] (Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services," January 2008.), which is placed in the call set-up signaling when a home or visited emergency dial string is detected. Because emergency services are local to specific geographic regions, a caller must obtain his location (Section 6 (Location and its role in an emergency call)) prior to making emergency calls. To get this location, either a form of measuring (e.g., GPS) (Section 6.2.3 (End-system measured location information)) device location in the endpoint is deployed, or the endpoint is configured (Section 6.5 (End system location configuration)) with its location from the access network's Location Information Server (LIS). The location is conveyed (Section 6.7 (Conveying location in SIP)) in the SIP signaling with the call. The call is routed (Section 8 (Routing the call to the PSAP)) based on location using the LoST protocol [RFC5222] (Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol," August 2008.), which maps a location to a set of PSAP URIs. Each URI resolves to a PSAP or an Emergency Services Routing Proxy (ESRP), which serves a group of PSAPs. The call arrives at the PSAP with the location included in the SIP INVITE request.

---

4. Which devices and services should support emergency calls

TOC

ED-1 A device or application SHOULD support emergency calling if a user could reasonably expect to be able to place a call for help with the device. Some jurisdictions have regulations governing this.
SP-1 If a device or application expects to be able to place a call for help, the service provider that supports it MUST facilitate emergency calling. Some jurisdictions have regulations governing this.
ED-2 Devices that create media sessions and exchange audio, video and/or text, and have the capability to establish sessions to a wide variety of addresses, and communicate over private IP networks or the Internet, SHOULD support emergency calls. Some jurisdictions have regulations governing this.

---

5. Identifying an emergency call

TOC

ED-3 Endpoints SHOULD recognize dial strings of emergency calls. If the service provider always knows the location of the device, then the service provider could recognize them.

SP-2 Proxy servers SHOULD recognize emergency dial strings if for some reason the endpoint does not recognize them. This cannot be relied upon by the device if the service provider cannot always determine the location of the device.
ED-4/SP-3 Emergency calls MUST be marked with a Service URN in the Request-URI of the INVITE.
ED-5/SP-4 Local dial strings MUST be recognized.
ED-6/SP-5 deleted
ED-7/SP-6 Emergency dial strings SHOULD be determined from LoST [RFC5222] (Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol," August 2008.). Dial Strings MAY be configured directly in the device.
AN-1 LoST servers MUST return dial strings for emergency services
ED-8 Endpoints which do not recognize emergency dial strings SHOULD send dial strings as per [RFC4967] (Rosen, B., "Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier," July 2007.).
SP-7 If a proxy server recognizes dial strings on behalf of its clients it MUST recognize emergency dial strings represented by [RFC4967] (Rosen, B., "Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier," July 2007.) and SHOULD recognize emergency dial strings represented by a tel URI [RFC3966] (Schulzrinne, H., "The tel URI for Telephone Numbers," December 2004.).
ED-9 Endpoints SHOULD be able to have home dial strings provisioned.
SP-8 Service providers MAY provision home dial strings in devices.
ED-10 Devices SHOULD NOT have one button emergency calling initiation.
ED-11/SP-9 All emergency services specified in [RFC5031] (Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services," January 2008.) MUST be recognized.

---

6. Location and its role in an emergency call

TOC

Handling location for emergency calling usually involves several steps to process and multiple elements are involved. In Internet emergency calling, where the endpoint is located is "determined" using a variety of measurement or wiretracing methods. Endpoints may be "configured" with their own location by the access network. In some circumstances, a proxy server may insert location into the signaling on behalf of the endpoint. The location is "mapped" to the URI to send the call to, and the location is "conveyed" to the PSAP (and other elements) in the signaling. Likewise, we employ Location Configuration Protocols, the Location-to-Service Mapping Protocol, and Location Conveyance Protocols for these functions. The Location-to-Service Translation protocol [RFC5222] (Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol," August 2008.) is the Location Mapping Protocol defined by the IETF.

6.1. Types of location information

TOC

There are several forms of location. In IETF location configuration and location conveyance protocols, civic and geospatial (geo) forms are both supported. The civic forms include both postal and jurisdictional fields. A cell tower/sector can be represented as a point (geo or civic) or polygon. Other forms of location representation must be mapped into either a geo or civic for use in emergency calls.
ED-12/INT-1/SP-10 Endpoints, Intermediate Devices and Service Providers MUST be prepared to handle location represented in either civic or geo form.
ED-13/INT-2/SP-11/AN-2 Elements MUST NOT convert (civic to geo or geo to civic) from the form of location the determination mechanism supplied.

6.2. Location Determination

TOC

ED-14/INT-3/AN-3 Any suitable location determination mechanism MAY be used.

6.2.1. User-entered location information

TOC

ED-15/INT-4/AN-4 Devices, intermediate Devices and/or access networks SHOULD support a manual method to "override" the location the access network determines. Where a civic form of location is provided, all fields in the PIDF-LO [RFC4119] (Peterson, J., “A Presence-based GEOPRIV Location Object Format,” December 2005.) and [RFC5139] (Thomson, M. and J. Winterbottom, “Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO),” February 2008.) MUST be able to be specified.

6.2.2. Access network "wire database" location information

TOC

AN-5 Access networks supporting copper, fiber or other hard wired IP packet service SHOULD support location configuration. If the network does not support location configuration, it MUST require every device that connects to the network to support end system measured location.

AN-6/INT-5 Access networks and intermediate devices providing wire database location information SHOULD provide interior location data (building, floor, room, cubicle) where possible. It is RECOMMENDED that interior location be provided when spaces exceed approximately 650 square meters.
AN-7/INT-6 Access networks and intermediate devices (including enterprise networks) which support intermediate range wireless connections (typically 100m or less of range) and which do not support a more accurate location determination mechanism such as triangulation, MUST support location configuration where the location of the access point is reflected as the location of the clients of that access point. Where the access network provides location configuration, intermediate devices MUST either be transparent to it, or provide an interconnected client for the supported configuration mechanism and a server for a configuration protocol supported by end devices downstream of the intermediate device

---

6.2.3. End-system measured location information

TOC

ED-16/INT-7 Devices MAY support end-system measured location. Uncertainty of less than 100 m with 95% confidence SHOULD be available for dispatch.
ED-17/INT-8/AN-8 Devices that support endpoint measuring of location MUST have at least a coarse location capability (typically <1km accuracy when not location hiding) for routing of calls. The location mechanism MAY be a service provided by the access network.

6.2.4. Network-measured location information

TOC

AN-9 Access networks MAY provide network-measured location determination. Wireless access network which do not support network measured location MUST require that all devices connected to the network have end-system measured location. Uncertainty of less than 100 m with 95% confidence SHOULD be available for dispatch.
AN-10 Access networks that provide network measured location MUST have at least a coarse location (typically <1km when not location hiding) capability at all times for routing of calls.
AN-11 Access networks with range of <10 meters (e.g. personal area networks such as Bluetooth MUST provide a location to mobile devices connected to them. The location provided SHOULD be that of the access point location unless a more accurate mechanism is provided.

6.3. Who adds location, endpoint or proxy

TOC

ED-18/INT-9 Endpoints SHOULD attempt to configure their own location using the LCPs listed in ED-21.
SP-12 Proxies MAY provide location on behalf of devices if:

- The proxy has a relationship with all access networks the device could connect to, and the relationship allows it to obtain location.

- The proxy has an identifier, such as an IP address, that can be used by the access network to determine the location of the endpoint, even in the presence of NAT and VPN tunnels that may obscure the identifier between the access network and the service provider.

ED-19/INT-10/SP-13 Where proxies provide location on behalf of endpoints, the service provider MUST ensure that either the end device is provided with the local dial strings for its current location (where the end device recognizes dial strings), or the service provider proxy MUST detect the appropriate local dial strings at the time of the call.

6.4. Location and references to location

TOC

ED-20/INT-11 Devices SHOULD be able to accept and forward location by value or by reference. An end device that receives location by reference (and does not also get the corresponding value) MUST be able to perform a dereference operation to obtain a value.

6.5. End system location configuration

TOC

ED-21/INT-12 Devices MUST support both the DHCP location options [RFC4776] (Schulzrinne, H., “Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information,” November 2006.), [RFC3825] (Polk, J., Schnizlein, J., and M. Linsner, “Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information,” July 2004.) and HELD [I-D.ietf-geopriv-http-location-delivery] (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, “HTTP Enabled Location Delivery (HELD),” August 2009.). When devices deploy a specific access network interface in which that access network supports location discovery such as LLDP-MED or 802.11v, the device SHOULD support the additional respective access network specific location discovery mechanism.

AN-12/INT-13 The access network MUST support either DHCP location options or HELD. The access network SHOULD support other location technologies that are specific to the type of access network.
AN-13/INT-14 Where a router is employed between a LAN and WAN in a small (less than approximately 650 square meters) area, the router MUST be transparent to the location provided by the WAN to the LAN. This may mean the router must obtain location as a client from the WAN, and supply an LCP server to the LAN with the location it obtains. Where the area is larger, the LAN MUST have a location configuration mechanism meeting this BCP.
ED-22/INT-15 Endpoints SHOULD try all LCPs supported by the device in any order or in parallel. The first one that succeeds in supplying location can be used.
AN-14/INT-16 Access networks that support more than one LCP MUST reply with the same location information (within the limits of the data format for the specific LCP) for all LCPs it supports.
ED-23/INT-17/SP-14 When HELD is the LCP, the request MUST specify a value of "emergencyRouting" for the "responseTime" parameter and use the resulting location for routing. If a value for dispatch location will be sent, another request with the "responseTime" parameter set to "emergencyDispatch" must be completed, with the result sent for dispatch purposes.
ED-24 Where the operating system supporting application programs which need location for emergency calls does not allow access to Layer 2 and Layer 3 functions necessary for a client application to use DHCP location options and/or LLDP-MED, the operating system MUST provide a published API conforming to ED-12 through ED-21 and ED-21 through ED-31. It is RECOMMENDED that all operating systems provide such an API.

6.6. When location should be configured

TOC

ED-25/INT-18 Endpoints SHOULD obtain location immediately after obtaining local network configuration information. When HELD is the LCP the client MUST support a random back-off period (between 30 seconds and 300 seconds) for re-trying the HELD query, when no response is received, and no other LCP provided location information.
ED-26/INT-19 If the device is configured to use DHCP for bootstrapping, it MUST include both options for location acquisition (civic and geodetic), the option for LIS discovery, and the option for LoST discovery as defined in [RFC4776] (Schulzrinne, H., “Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information,” November 2006.), [RFC3825] (Polk, J., Schnizlein, J., and M. Linsner, “Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information,” July 2004.), [I-D.ietf-geopriv-lis-discovery] (Thomson, M. and J.

Winterbottom, “Discovering the Local Location Information Server (LIS),” March 2010.) and [RFC5223] (Schulzrinne, H., Polk, J., and H. Tschofenig, “Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP),” August 2008.).

ED-27/INT-20 If the device sends a DHCPINFORM message, it MUST include both options for location acquisition (civic and geodetic), the option for LIS discovery, and the option for LoST discovery as defined in [RFC4776] (Schulzrinne, H., “Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information,” November 2006.), [RFC3825] (Polk, J., Schnizlein, J., and M. Linsner, “Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information,” July 2004.), [I-D.ietf-geopriv-lis-discovery] (Thomson, M. and J. Winterbottom, “Discovering the Local Location Information Server (LIS),” March 2010.) and [RFC5223] (Schulzrinne, H., Polk, J., and H. Tschofenig, “Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP),” August 2008.).

ED-28/INT-21 To minimize the effects of VPNs that do not allow packets to be sent via the native hardware interface rather than via the VPN tunnel, location configuration SHOULD be attempted before such tunnels are established.

ED-29/INT-22 Software which uses LCPs SHOULD locate and use the actual hardware network interface rather than a VPN tunnel interface to direct LCP requests to the LIS in the actual access network.

AN-15 Network administrators MUST take care in assigning IP addresses such that VPN address assignments can be distinguished from local devices (by subnet choice, for example), and LISs SHOULD NOT attempt to provide location to addresses that arrive via VPN connections unless it can accurately determine the location for such addresses.

AN-16 Placement of NAT devices where an LCP uses IP address for an identifier SHOULD consider the effect of the NAT on the LCP. The address used to query the LIS MUST be able to correctly identify the record in the LIS representing the location of the querying device

ED-30/INT-23 For devices which are not expected to roam, refreshing location on the order of once per day is RECOMMENDED.

ED-31/INT-24 For devices which roam, refresh of location information SHOULD be more frequent, with the frequency related to the mobility of the device and the ability of the access network to support the refresh operation. If the device can detect that it has moved, for example when it changes access points, the device SHOULD refresh its location.

ED-32/INT-25/AN-17 It is RECOMMENDED that location determination not take longer than 250 ms to obtain routing location and systems SHOULD be designed such that the typical response is under 100 ms. However, as much as 3 seconds to obtain routing location MAY be tolerated if location accuracy can be substantially improved over what can be obtained in 250 ms.

6.7. Conveying location in SIP

TOC

ED-33/SP-15 Location sent between SIP elements MUST be conveyed using [I-D.ietf-sip-location-conveyance] (Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol," March 2009.).

6.8. Location updates

TOC

ED-34/AN-18 Where the absolute location or the accuracy of location of the endpoint may change between the time the call is received at the PSAP and the time dispatch is completed, location update mechanisms MUST be provided.
ED-35/AN-19 Mobile devices MUST be provided with a mechanism to get repeated location updates to track the motion of the device during the complete processing of the call.
ED-36/AN-20 The LIS SHOULD provide a location reference which permits a subscription with appropriate filtering.
ED-37/AN-21 For calls sent with location-by-reference, with a SIP or SIPS scheme, the server resolving the reference MUST support a SUBSCRIBE [RFC3265] (Roach, A., "Session Initiation Protocol (SIP)-Specific Event Notification," June 2002.) to the presence event [RFC3856] (Rosenberg, J., "A Presence Event Package for the Session Initiation Protocol (SIP)," August 2004.). For other location-by-reference schemes that do not support subscription, the PSAP will have to repeatedly dereference the URI to determine if the device moved.
ED-38 If location was sent by value, and the endpoint gets updated location, it MUST send the updated location to the PSAP via a SIP re-INVITE or UPDATE request. Such updates SHOULD be limited to no more than one update every 10 seconds.

6.9. Multiple locations

TOC

ED-39/SP-16 If the LIS has more than one location for an endpoint it MUST use the procedures in [I-D.ietf-geopriv-pdif-lo-profile] (Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations," November 2008.)
ED-40 If a UA has more than one location available to it, it MUST choose one location to route the call towards the PSAP. If multiple locations are in a single PIDF, the procedures in [I-D.ietf-geopriv-pdif-lo-profile] (Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations," November 2008.) MUST be followed. If the UA has

multiple PIDFs, and has no reasonable basis to choose from among them, a random choice is acceptable.
SP-17 If a proxy inserts location on behalf of an endpoint, and it has multiple locations available for the endpoint it MUST choose one location to use to route the call towards the PSAP.
SP-18 If a proxy is attempting to insert location but the UA conveyed a location to it, the proxy MUST use the UA's location for routing and MUST convey that location towards the PSAP. It MAY also include what it believes the location to be in a separate Geolocation header.
SP-19 All location objects received by a proxy MUST be delivered to the PSAP.
ED-41/SP-20 Location objects MUST contain information about the method by which the location was determined, such as GPS, manually entered, or based on access network topology included in a PIDF- LO "method" element. In addition, the source of the location information MUST be included in a PIDF-LO "provided-by" element.
ED-??/SP-?? A location with a method of "derived" MUST NOT be used unless no other location is available.
ED-42/SP-21 The "used-for-routing" parameter MUST be set to the location that was chosen for routing.

6.10. Location validation

TOC

AN-22 A LIS should perform location validation of civic locations via LoST before entering a location in its database.
ED-43 Endpoints SHOULD validate civic locations when they receive them from their LCP. Validation SHOULD be performed in conjunction with the LoST route query to minimize load on the LoST server.

6.11. Default location

TOC

AN-23 When the access network cannot determine the actual location of the caller, it MUST supply a default location. The default SHOULD be chosen to be as close to the probable location of the device as the network can determine. See [I-D.ietf-ecrit-framework] (Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, “Framework for Emergency Calling using Internet Multimedia,” July 2009.)
SP-22 Proxies handling emergency calls MUST insert a default location if the call does not contain a location and the proxy does not have a method for obtaining a better location.
AN-24/SP-23 Default locations MUST be marked with method=Default and the proxy MUST be identified in provided-by element of the PIDF-LO.

6.12. Other location considerations

TOC

ED-44 If the LCP does not return location in the form of a PIDF-LO [RFC4119] (Peterson, J., “A Presence-based GEOPRIV Location Object Format,” December 2005.), the endpoint MUST map the location information it receives from the configuration protocol to a PIDF-LO.
ED-45/AN-25 To prevent against spoofing of the DHCP server, elements implementing DHCP for location configuration SHOULD use [RFC3118] (Droms, R. and W. Arbaugh, “Authentication for DHCP Messages,” June 2001.) although the difficulty in providing appropriate credentials is significant.
ED-46 S/MIME MUST NOT be used to encrypt the SIP Geolocation header or bodies.
ED-47/SP-24 TLS MUST be used to protect location (but see Section 9.1 (Use of TLS)). IPSEC [RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” January 2005.) is an acceptable alternative.

---

7. LIS and LoST Discovery

TOC

ED-48 Endpoints MUST support one or more mechanisms that allow them to determine their public IP address. Examples include STUN [RFC3489] (Rosenberg, J., Weinberger, J., Huitema, C., and R. Mahy, “STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs),” March 2003.) and HTTP get.
ED-49 Endpoints MUST support LIS discovery as described in [I-D.ietf-geopriv-lis-discovery] (Thomson, M. and J. Winterbottom, “Discovering the Local Location Information Server (LIS),” March 2010.), and the LoST discovery as described in [RFC5223] (Schulzrinne, H., Polk, J., and H. Tschofenig, “Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP),” August 2008.).
ED-50 The device MUST have a configurable default LoST server parameter. If the device is provided by or managed by a service provider, it is expected that the service provider will configure this option.
ED-51 DHCP LoST discovery MUST be used, if available, in preference to configured LoST servers. If neither DHCP nor configuration leads to an available LoST server, the device MUST query DNS using it's SIP domain for an SRV record for a LoST service and use that server.
AN-26 Access networks which support DHCP MUST implement the LoST discovery option
SP-25 Service Providers MUST provide an SRV entry in their DNS server which leads to a LoST server

AN-27 Access Networks that use HELD and that have a DHCP server SHOULD support DHCP options for providing LIS and LoST servers.
ED-52 When an endpoint has obtained a LoST server via an discovery mechanism (e.g., via the DNS or DHCP), it MUST prefer the discovered LoST server over LoST servers configured by other means. That is, the endpoint MUST send queries to this LoST server first, using other LoST servers only if these queries fail.

---

8. Routing the call to the PSAP

TOC

ED-53 Endpoints who obtain their own location SHOULD perform LoST mapping to the PSAP URI.
ED-54 Mapping SHOULD be performed at boot time and whenever location changes beyond the service boundary obtained from a prior LoST mapping operation or the time-to-live value of that response has expired. The value MUST be cached for possible later use.
ED-55 The endpoint MUST attempt to update its location at the time of an emergency call. If it cannot obtain a new location quickly (see Section 6 (Location and its role in an emergency call)), it MUST use the cached value.
ED-56 The endpoint SHOULD attempt to update the LoST mapping at the time of an emergency call. If it cannot obtain a new mapping quickly, it MUST use the cached value. If the device cannot update the LoST mapping and does not have a cached value, it MUST signal an emergency call without a Route header containing a PSAP URI.
SP-26 Networks MUST be designed so that at least one proxy in the outbound path will recognize emergency calls with a Request URI of the service URN in the "sos" tree. An endpoint places a service URN in the Request URI to indicate that the endpoint understood the call was an emergency call. A proxy that processes such a call looks for the presence of a SIP Route header field with a URI of a PSAP. Absence of such a Route header indicates the UAC was unable to invoke LoST and the proxy MUST perform the LoST mapping and insert a Route header field with the URI obtained.
SP-27 To deal with old user agents that predate this specification and with UAs that do not have access to their own location data, a proxy that recognizes a call as an emergency call that is not marked as such (see Section 5 (Identifying an emergency call)) MUST also perform this mapping, with the best location it has available for the endpoint. The resulting PSAP URI would be placed in a Route header with the service URN in the Request URI.
SP-28 Proxy servers performing mapping SHOULD use location obtained from the access network for the mapping. If no location is available, a default location (see Section 6.11 (Default location)) MUST be supplied.

SP-29 A proxy server which attempts mapping and fails to get a mapping MUST provide a default mapping. A suitable default mapping would be the mapping obtained previously for the default location appropriate for the caller.
ED-57/SP-30 [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.) and [RFC3263] (Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers," June 2002.) procedures MUST be used to route an emergency call towards the PSAP's URI.
ED-58 Initial INVITES MUST provide an Offer [RFC3264] (Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)," June 2002.).

---

9. Signaling of emergency calls

TOC

ED-59 deleted

9.1. Use of TLS

TOC

ED-60/SP-31 TLS MUST be specified when attempting to signal an emergency call with SIP per Section 3.1 of [I-D.ietf-sip-sips] (Audet, F., "The use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)," November 2008.). IPSEC [RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," January 2005.) is an acceptable alternative.
ED-61/SP-32 If TLS session establishment fails, the call MUST be retried without TLS.
ED-62/SP-33 [I-D.ietf-sip-outbound] (Jennings, C., "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)," June 2009.) is RECOMMENDED to maintain persistent TLS connections between elements.
ED-63/AN-28 TLS MUST be specified when attempting to retrieve location (configuration or dereferencing) with HELD. The use of [RFC5077] (Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State," January 2008.) is RECOMMENDED to minimize the time to establish TLS sessions without keeping server-side state.
ED-64/AN-29 If TLS session establishment fails, the location retrieval MUST be retried without TLS.

TOC

9.2. SIP signaling requirements for User Agents

ED-65 The initial SIP signaling method is an INVITE request:

1. The Request URI SHOULD be the service URN in the "sos" tree, If the device cannot interpret local dial strings, the Request-URI SHOULD be a dial string URI [RFC4967] (Rosen, B., “Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier,” July 2007.) with the dialed digits.

2. The To header SHOULD be a service URN in the "sos" tree. If the device cannot interpret local dial strings, the To: SHOULD be a dial string URI with the dialed digits.

3. The From header MUST be present and SHOULD be the AoR of the caller.

4. A Via header MUST be present.

5. A Route header SHOULD be present with a PSAP URI obtained from LoST (see Section 8 (Routing the call to the PSAP)) and the loose route parameter. If the device does not interpret dial plans, or was unable to obtain a route from a LoST server, no Route header will be present.

6. A Contact header MUST be present which MUST be globally routable, for example a GRUU [I-D.ietf-sip-gruu] (Rosenberg, J., “Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP),” October 2007.), and be valid for several minutes following the termination of the call to permit an immediate call-back to the specific device which placed the emergency call.

7. Other headers MAY be included as per normal SIP behavior.

8. A Supported header MUST be included with the 'geolocation' option tag [I-D.ietf-sip-location-conveyance] (Polk, J. and B. Rosen, “Location Conveyance for the Session Initiation Protocol,” March 2009.), unless the device does not understand the concept of SIP location.

9. If a device understands the SIP location conveyance [I-D.ietf-sip-location-conveyance] (Polk, J. and B. Rosen, “Location Conveyance for the Session Initiation Protocol,” March 2009.) extension and has its location available, it MUST include location either by-value, by-reference or both.

10. If a device understands the SIP Location Conveyance extension and has its location unavailable or unknown to that device, it MUST include a Supported header with a "geolocation" option

tag, and MUST NOT include a Geolocation header, and not include a PIDF-LO message body.

11. If a device understands the SIP Location Conveyance extension and supports LoST [RFC5222] (Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol," August 2008.), the Geolocation "used-for-routing" header parameter MUST be added to the corresponding URI in the Geolocation header. If the device is unable to obtain a PSAP URI for any reason it MUST NOT include "used-for-routing" on a Geolocation URI, so that downstream entities know that LoST routing has not been completed.

12. A SDP offer MUST be included in the INVITE. If voice is supported the offer MUST include the G.711 codec, see Section 14 (Media).

13. If the device includes location-by-value, the UA MUST support multipart message bodies, since SDP will likely be also in the INVITE.

14. A UAC SHOULD include a "inserted-by=endpoint" header parameter on all Geolocation headers. This informs downstream elements which device entered the location at this URI (either cid-URL or location-by-reference URI).

15. SIP Caller Preferences [RFC3841] (Rosenberg, J., Schulzrinne, H., and P. Kyzivat, "Caller Preferences for the Session Initiation Protocol (SIP)," August 2004.) MAY 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.

9.3. SIP signaling requirements for proxy servers

TOC

SP-34 SIP Proxy servers processing emergency calls:

1. If the proxy interprets dial plans on behalf of user agents, the proxy MUST look for the local emergency dial string at the

location of the end device and MAY look for the home dial string. If it finds it, the proxy MUST:

- *Insert a Geolocation header as above. Location-by-reference MUST be used because proxies must not insert bodies.
- *Include the Geolocation "inserted-by=server" and "used-for-routing" parameters.
- *Map the location to a PSAP URI using LoST.
- *Add a Route header with the PSAP URI.
- *Replace the Request-URI (which was the dial string) with the service URN appropriate for the emergency dial string.
- *Route the call using normal SIP routing mechanisms.

2. If the proxy recognizes the service URN in the Request URI, and does not find a a Route header, it MUST query a LoST server. If multiple locations were provided, the proxy uses the location that has the "used-for-routing" marker set. If a location was provided (which should be the case), the proxy uses that location to query LoST. The proxy may have to dereference a location by reference to get a value. If a location is not present, and the proxy can query a LIS which has the location of the UA it MUST do so. If no location is present, and the proxy does not have access to a LIS which could provide location, the proxy MUST supply a default location (See Section 6.11 (Default location)). The location (in the signaling, obtained from a LIS, or default) MUST be used in a query to LoST with the service URN received with the call. The resulting URI MUST be placed in a Route header added to the call.

3. The "inserted-by=" parameter in any Geolocation: header received on the call MUST NOT be modified or deleted in transit.

4. The proxy SHOULD NOT modify any parameters in Geolocation headers received in the call. It MAY add a Geolocation header. Such an additional location SHOULD NOT be used for routing; the location provided by the UA should be used.

5. Either a P-Asserted-Identity [RFC3325] (Jennings, C., Peterson, J., and M. Watson, “Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks,” November 2002.) or an Identity header [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),”

August 2006.), or both, SHOULD be included to identify the sender. For services which must support emergency calls from unauthenticated devices, valid identity may not be available.

---

10. Call backs

TOC

ED-66/SP-35 Devices device SHOULD have a globally routable URI in a Contact: header which remains valid for 30 minutes past the time the original call containing the URI completes unless the device registration expires and is not renewed.
SP-36 Call backs to the Contact: header URI recieved within 30 minutes of an emergency call must reach the device regardless of call features or services that would normally cause the call to be routed to some other entity.
SP-37 Devices MUST have a persistent AOR URI either in a P-Asserted-Identity: header or From: protected by an Identity header suitable for returning a call some time after the original call. Such a call back would not necessarily reach the device that originally placed the call.

---

11. Mid-call behavior

TOC

ED-67/SP-38 During the course of an emergency call, devices and proxies MUST support REFER transactions and the Referred-by: header [RFC3515] (Sparks, R., "The Session Initiation Protocol (SIP) Refer Method," April 2003.).

---

12. Call termination

TOC

ED-68 deleted
ED-69 There can be a case where the session signaling path is lost, and the user agent does not receive the BYE. If the call is hung up, and the session timer (if implemented) expires, the call MAY be declared lost. If in the interval, an incoming call is received from the domain of the PSAP, the device MUST drop the old call and alert for the (new) incoming call. Dropping of the old call MUST only occur if the user is attempting to hang up; the domain of an incoming call can only be determined from the From header, which is not reliable, and could be spoofed. Dropping an active call by a new call with a spoofed From: would be a DoS attack.

---

13. Disabling of features

TOC

ED-70/SP-39 User Agents and proxies MUST disable outgoing call features such as

- *Call Waiting
- *Call Transfer
- *Three Way Call
- *Hold, including Flash hold
- *Outbound Call Blocking

when an emergency call is established. Also see ED-77 in Section 14 (Media).
ED-71/SP-40 The emergency dial strings SHOULD NOT be permitted in Call Forward numbers or speed dial lists.
ED-72/SP-41 The User Agent and Proxies SHOULD disable the following incoming call features on call backs from the PSAP:

- *Call Waiting
- *Do Not Disturb
- *Call Forward (all kinds)

ED-73 Call backs SHOULD be determined by retaining the domain of the PSAP which answers an outgoing emergency call and instantiating a timer which starts when the call is terminated. If a call is received from the same domain and within the timer period, sent to the Contact: or AoR used in the emergency call, it should be assumed to be a call back. The suggested timer period is 5 minutes.

---

14. Media

TOC

ED-74 Endpoints MUST send and receive media streams on RTP [RFC3550] (Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications,” July 2003.).
ED-75 Normal SIP offer/answer [RFC3264] (Rosenberg, J. and H. Schulzrinne, “An Offer/Answer Model with Session Description Protocol (SDP),” June 2002.) negotiations MUST be used to agree on the media streams to be used.
ED-76 Endpoints supporting voice MUST support G.711 A law (and mu Law if they are intended be used in North America) encoded voice as

described in [RFC3551] (Schulzrinne, H. and S. Casner, “RTP Profile for Audio and Video Conferences with Minimal Control,” July 2003.). It is desirable to include wideband codecs such as AMR-WB in the offer.
ED-77 Silence suppression (Voice Activity Detection methods) MUST NOT be used on emergency calls. PSAP call takers sometimes get information on what is happening in the background to determine how to process the call.
ED-78 Endpoints supporting Instant Messaging (IM) MUST support both [RFC3428] (Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, “Session Initiation Protocol (SIP) Extension for Instant Messaging,” December 2002.) and [RFC4975] (Campbell, B., Mahy, R., and C. Jennings, “The Message Session Relay Protocol (MSRP),” September 2007.).
ED-79 Endpoints supporting real-time text MUST use [RFC4103] (Hellstrom, G. and P. Jones, “RTP Payload for Text Conversation,” June 2005.). The expectations for emergency service support for the real-time text medium, described in [RFC5194] (van Wijk, A. and G. Gybels, “Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP),” June 2008.), Section 7.1 SHOULD be fulfilled.
ED-80 Endpoints supporting video MUST support H.264 per [RFC3984] (Wenger, S., Hannuksela, M., Stockhammer, T., Westerlund, M., and D. Singer, “RTP Payload Format for H.264 Video,” February 2005.).

---

15. Testing

TOC

ED-81 INVITE requests to a service URN ending in ".test" indicates a request for an automated test. For example, "urn:service.sos.fire.test". As in standard SIP, a 200 (OK) response indicates that the address was recognized and a 404 (Not found) that it was not. A 486 (Busy Here) MUST be returned if the test service is busy, and a 404 (Not found) MUST be returned if the PSAP does not support the test mechanism.
ED-82 In its response to the test, the PSAP MAY include a text body (text/plain) indicating the identity of the PSAP, the requested service, and the location reported with the call. For the latter, the PSAP SHOULD return location-by-value even if the original location delivered with the test was by-reference. If the location-by-reference was supplied, and the dereference requires credentials, the PSAP SHOULD use credentials supplied by the LIS for test purposes. This alerts the LIS that the dereference is not for an actual emergency call and location hiding techniques, if they are being used, may be employed for this dereference. The test response SHOULD be protected with TLS. If the body cannot be protected, the location SHOULD NOT be included in the response..

ED-83 A PSAP accepting a test call SHOULD accept a media loopback test [I-D.ietf-mmusic-media-loopback] (Sivachelvan, C., Venna, N., Jones, P., Stratton, N., Roychowdhury, A., and K. Hedayat, “An Extension to the Session Description Protocol (SDP) for Media Loopback,” April 2010.) and SHOULD support the "rtp-pkt-loopback" and "rtp-start-loopback" options. The user agent would specify a loopback attribute of "loopback-source", the PSAP being the mirror. User Agents should expect the PSAP to loop back no more than 3 packets of each media type accepted (which limits the duration of the test), after which the PSAP would normally send BYE.
ED-84 User agents SHOULD perform a full call test, including media loopback, after a disconnect and subsequent change in IP address not due to a reboot. After an initial test, a full test SHOULD be repeated approximately every 30 days with a random interval.
ED-85 User agents MUST NOT place a test call immediately after booting. If the IP address changes after booting, the UA should wait a random amount of time (in perhaps a 30 minute period, sufficient for any avalanche restart to complete) and then test.
ED-86 PSAPs MAY refuse repeated requests for test from the same device in a short period of time. Any refusal is signaled with a 486 or 488 response.

---

16. Security Considerations

TOC

Security considerations for emergency calling have been documented in [RFC5069] (Taylor, T., Tschofenig, H., Schulzrinne, H., and M. Shanmugam, “Security Threats and Requirements for Emergency Call Marking and Mapping,” January 2008.), and [I-D.barnes-geopriv-lo-sec] (Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, “An Architecture for Location and Location Privacy in Internet Applications,” March 2009.).

---

17. IANA Considerations

TOC

This document has no actions for IANA.

---

18. Acknowledgements

TOC

Work group members participating in the creation and review of this document include include Hannes Tschofenig, Ted Hardie, Marc Linsner,

Roger Marshall, Stu Goldman, Shida Schubert, James Winterbottom, Barbara Stark, Richard Barnes and Peter Blatherwick.

---

19. References

TOC

19.1. Normative References

TOC

[I-D.ietf-geopriv-http-location-delivery]	Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)," draft-ietf-geopriv-http-location-delivery-16 (work in progress), August 2009 (TXT).
[I-D.ietf-geopriv-lis-discovery]	Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)," draft-ietf-geopriv-lis-discovery-15 (work in progress), March 2010 (TXT).
[I-D.ietf-geopriv-pdif-lo-profile]	Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations," draft-ietf-geopriv-pdif-lo-profile-14 (work in progress), November 2008 (TXT).
[I-D.ietf-mmusic-media-loopback]	Sivachelvan, C., Venna, N., Jones, P., Stratton, N., Roychowdhury, A., and K. Hedayat, "An Extension to the Session Description Protocol (SDP) for Media Loopback," draft-ietf-mmusic-media-loopback-13 (work in progress), April 2010 (TXT).
[I-D.ietf-sip-gruu]	Rosenberg, J., "Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)," draft-ietf-sip-gruu-15 (work in progress), October 2007 (TXT).
[I-D.ietf-sip-location-conveyance]	Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol," draft-ietf-sip-location-conveyance-13 (work in progress), March 2009 (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).
[LLDP]	IEEE, "IEEE802.1ab Station and Media Access Control," Dec 2004.
[LLDP-MED]	TIA, "ANSI/TIA-1057 Link Layer Discovery Protocol - Media Endpoint Discovery."
[RFC2119]	

	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3118]	Droms, R. and W. Arbaugh, “Authentication for DHCP Messages,” RFC 3118, June 2001 (TXT).
[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).
[RFC3263]	Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” RFC 3263, June 2002 (TXT).
[RFC3264]	Rosenberg, J. and H. Schulzrinne, “An Offer/Answer Model with Session Description Protocol (SDP),” RFC 3264, June 2002 (TXT).
[RFC3265]	Roach, A., “Session Initiation Protocol (SIP)-Specific Event Notification,” RFC 3265, June 2002 (TXT).
[RFC3428]	Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, “Session Initiation Protocol (SIP) Extension for Instant Messaging,” RFC 3428, December 2002 (TXT).
[RFC3489]	Rosenberg, J., Weinberger, J., Huitema, C., and R. Mahy, “STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs),” RFC 3489, March 2003 (TXT).
[RFC3515]	Sparks, R., “The Session Initiation Protocol (SIP) Refer Method,” RFC 3515, April 2003 (TXT).
[RFC3550]	Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications,” STD 64, RFC 3550, July 2003 (TXT, PS, PDF).
[RFC3551]	Schulzrinne, H. and S. Casner, “RTP Profile for Audio and Video Conferences with Minimal Control,” STD 65, RFC 3551, July 2003 (TXT, PS, PDF).
[RFC3825]	Polk, J., Schnizlein, J., and M. Linsner, “Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information,” RFC 3825, July 2004 (TXT).
[RFC3841]	Rosenberg, J., Schulzrinne, H., and P. Kyzivat, “Caller Preferences for the Session Initiation Protocol (SIP),” RFC 3841, August 2004 (TXT).
[RFC3856]	Rosenberg, J., “A Presence Event Package for the Session Initiation Protocol (SIP),” RFC 3856, August 2004 (TXT).
[RFC3966]	Schulzrinne, H., “The tel URI for Telephone Numbers,” RFC 3966, December 2004 (TXT).
[RFC3984]	

	Wenger, S., Hannuksela, M., Stockhammer, T., Westerlund, M., and D. Singer, “RTP Payload Format for H.264 Video,” RFC 3984, February 2005 (TXT).
[RFC3986]	Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” STD 66, RFC 3986, January 2005 (TXT, HTML, XML).
[RFC4103]	Hellstrom, G. and P. Jones, “RTP Payload for Text Conversation,” RFC 4103, June 2005 (TXT).
[RFC4119]	Peterson, J., “A Presence-based GEOPRIV Location Object Format,” RFC 4119, December 2005 (TXT).
[RFC4474]	Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” RFC 4474, August 2006 (TXT).
[RFC4776]	Schulzrinne, H., “Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information,” RFC 4776, November 2006 (TXT).
[RFC4967]	Rosen, B., “Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier,” RFC 4967, July 2007 (TXT).
[RFC4975]	Campbell, B., Mahy, R., and C. Jennings, “The Message Session Relay Protocol (MSRP),” RFC 4975, September 2007 (TXT).
[RFC5031]	Schulzrinne, H., “A Uniform Resource Name (URN) for Emergency and Other Well-Known Services,” RFC 5031, January 2008 (TXT).
[RFC5139]	Thomson, M. and J. Winterbottom, “Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO),” RFC 5139, February 2008 (TXT).
[RFC5222]	Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, “LoST: A Location-to-Service Translation Protocol,” RFC 5222, August 2008 (TXT).
[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 (TXT).

19.2. Informative References

TOC

[I-D.barnes-geopriv-lo-sec]	Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications," draft-barnes-geopriv-lo-sec-05 (work in progress), March 2009 (TXT).
[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-sip-sips]	Audet, F., "The use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)," draft-ietf-sip-sips-09 (work in progress), November 2008 (TXT).
[RFC3325]	Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," RFC 3325, November 2002 (TXT).
[RFC5012]	Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies," RFC 5012, January 2008 (TXT).
[RFC5069]	Taylor, T., Tschofenig, H., Schulzrinne, H., and M. Shanmugam, "Security Threats and Requirements for Emergency Call Marking and Mapping," RFC 5069, January 2008 (TXT).
[RFC5077]	Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State," RFC 5077, January 2008 (TXT).
[RFC5194]	van Wijk, A. and G. Gybels, "Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP)," RFC 5194, June 2008 (TXT).

Appendix A. BCP Requirements Sorted by Responsible Party

TOC

A.1. Requirements of End Devices

TOC

ED-1 A device or application SHOULD support emergency calling if a user could reasonably expect to be able to place a call for help with the device. Some jurisdictions have regulations governing this.

ED-2 Devices that create media sessions and exchange audio, video and/or text, and have the capability to establish sessions to a wide variety of addresses, and communicate over private IP networks or the Internet, SHOULD support emergency calls. Some jurisdictions have regulations governing this.
ED-3 Endpoints SHOULD recognize dial strings of emergency calls. If the service provider always knows the location of the device, then the service provider could recognize them.
ED-4 Emergency calls MUST be marked with a Service URN in the Request-URI of the INVITE.
ED-5 Local dial strings MUST be recognized.
ED-7 Emergency dial strings SHOULD be determined from LoST [RFC5222] (Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, “LoST: A Location-to-Service Translation Protocol,” August 2008.). Dial Strings MAY be configured directly in the device.
ED-8 Endpoints which do not recognize emergency dial strings SHOULD send dial strings as per [RFC4967] (Rosen, B., “Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier,” July 2007.).
ED-9 Endpoints SHOULD be able to have home dial strings provisioned by configuration.
ED-10 Devices SHOULD NOT have one button emergency calling initiation.
ED-11 All emergency services specified in [RFC5031] (Schulzrinne, H., “A Uniform Resource Name (URN) for Emergency and Other Well-Known Services,” January 2008.) MUST be recognized.
ED-12 Endpoints, Intermediate Devices and Service Providers MUST be prepared to handle location represented in either civic or geo form.
ED-13 Elements MUST NOT convert (civic to geo or geo to civic) from the form of location the determination mechanism supplied.
ED-14 Any suitable location determination mechanism MAY be used.
ED-15 Devices, intermediate Devices and/or access networks SHOULD support a manual method to "override" the location the access network determines. Where a civic form of location is provided, all fields in the PIDF-LO [RFC4119] (Peterson, J., “A Presence-based GEOPRIV Location Object Format,” December 2005.) and [RFC5139] (Thomson, M. and J. Winterbottom, “Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO),” February 2008.) MUST be able to be specified.
ED-16 Devices MAY support end-system measured location. Uncertainty of less than 100 m with 95% confidence SHOULD be available for dispatch.
ED-17 Devices that support endpoint measuring of location MUST have at least a coarse location capability (typically <1km accuracy when not location hiding) for routing of calls. The location mechanism MAY be a service provided by the access network.
ED-18 Endpoints SHOULD attempt to configure their own location using the LCPs listed in ED-21.
ED-19 Where proxies provide location on behalf of endpoints, the service provider MUST ensure that either the end device is provided with the local dial strings for its current location (where the end

device recognizes dial strings), or the service provider proxy MUST detect the appropriate local dial strings at the time of the call.

ED-20 Devices SHOULD be able to accept and forward location by value or by reference. An end device that receives location by reference (and does not also get the corresponding value) MUST be able to perform a dereference operation to obtain a value.

ED-21 Devices MUST support both the DHCP location options [RFC4776] (Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information," November 2006.), [RFC3825] (Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information," July 2004.) and HELD [I-D.ietf-geopriv-http-location-delivery] (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)," August 2009.). When devices deploy a specific access network interface in which that access network supports location discovery such as LLDP-MED or 802.11v, the device SHOULD support the additional respective access network specific location discovery mechanism.

ED-22 Endpoints SHOULD try all LCPs supported by the device in any order or in parallel. The first one that succeeds in supplying location can be used.

ED-23 When HELD is the LCP, the request MUST specify a value of "emergencyRouting" for the "responseTime" parameter and use the resulting location for routing. If a value for dispatch location will be sent, another request with the "responseTime" parameter set to "emergencyDispatch" must be completed, with the result sent for dispatch purposes.

ED-24 Where the operating system supporting application programs which need location for emergency calls does not allow access to Layer 2 and Layer 3 functions necessary for a client application to use DHCP location options and/or LLDP-MED, the operating system MUST provide a published API conforming to ED-12 through ED-21 and ED-21 through ED-31. It is RECOMMENDED that all operating systems provide such an API.

ED-25 Endpoints SHOULD obtain location immediately after obtaining local network configuration information. When HELD is the LCP the client MUST support a random back-off period (between 30 seconds and 300 seconds) for re-trying the HELD query, when no response is received, and no other LCP provided location information.

ED-26 If the device is configured to use DHCP for bootstrapping, it MUST include both options for location acquisition (civic and geodetic), the option for LIS discovery, and the option for LoST discovery as defined in [RFC4776] (Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information," November 2006.), [RFC3825] (Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information," July 2004.), [I-D.ietf-geopriv-lis-discovery] (Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server

(LIS)," March 2010.) and [RFC5223] (Schulzrinne, H., Polk, J., and H. Tschofenig, "Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)," August 2008.).

ED-27 If the device sends a DHCPINFORM message, it MUST include both options for location acquisition (civic and geodetic), the option for LIS discovery, and the option for LoST discovery as defined in [RFC4776] (Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information," November 2006.), [RFC3825] (Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information," July 2004.), [I-D.ietf-geopriv-lis-discovery] (Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)," March 2010.) and [RFC5223] (Schulzrinne, H., Polk, J., and H. Tschofenig, "Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)," August 2008.).

ED-28 To minimize the effects of VPNs that do not allow packets to be sent via the native hardware interface rather than via the VPN tunnel, location configuration SHOULD be attempted before such tunnels are established.

ED-29 Software which uses LCPs SHOULD locate and use the actual hardware network interface rather than a VPN tunnel interface to direct LCP requests to the LIS in the actual access network.

ED-30 For devices which are not expected to roam, refreshing location on the order of once per day is RECOMMENDED.

ED-31 For devices which roam, refresh of location information SHOULD be more frequent, with the frequency related to the mobility of the device and the ability of the access network to support the refresh operation. If the device can detect that it has moved, for example when it changes access points, the device SHOULD refresh its location.

ED-32 It is RECOMMENDED that location determination not take longer than 250 ms to obtain routing location and systems SHOULD be designed such that the typical response is under 100 ms. However, as much as 3 seconds to obtain routing location MAY be tolerated if location accuracy can be substantially improved over what can be obtained in 250 ms.

ED-33 Location sent between SIP elements MUST be conveyed using [I-D.ietf-sip-location-conveyance] (Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol," March 2009.).

ED-34 Where the absolute location or the accuracy of location of the endpoint may change between the time the call is received at the PSAP and the time dispatch is completed, location update mechanisms MUST be provided.

ED-35 Mobile devices MUST be provided with a mechanism to get repeated location updates to track the motion of the device during the complete processing of the call.

ED-36 The LIS SHOULD provide a location reference which permits a subscription with appropriate filtering.

ED-37 For calls sent with location-by-reference, with a SIP or SIPS scheme, the server resolving the reference MUST support a SUBSCRIBE [RFC3265] (Roach, A., “Session Initiation Protocol (SIP)-Specific Event Notification,” June 2002.) to the presence event [RFC3856] (Rosenberg, J., “A Presence Event Package for the Session Initiation Protocol (SIP),” August 2004.). For other location-by-reference schemes that do not support subscription, the PSAP will have to repeatedly dereference the URI to determine if the device moved.

ED-38 If location was sent by value, and the endpoint gets updated location, it MUST send the updated location to the PSAP via a SIP re-INVITE or UPDATE request. Such updates SHOULD be limited to no more than one update every 10 seconds.

ED-39 If the LIS has more than one location for an endpoint it MUST use the procedures in [I-D.ietf-geopriv-pdif-lo-profile] (Winterbottom, J., Thomson, M., and H. Tschofenig, “GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations,” November 2008.)

ED-40 If a UA has more than one location available to it, it MUST choose one location to route the call towards the PSAP. If multiple locations are in a single PIDF, the procedures in [I-D.ietf-geopriv-pdif-lo-profile] (Winterbottom, J., Thomson, M., and H. Tschofenig, “GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations,” November 2008.) MUST be followed. If the UA has multiple PIDFs, and has no reasonable basis to choose from among them, a random choice is acceptable.

ED-41 Location objects MUST contain information about the method by which the location was determined, such as GPS, manually entered, or based on access network topology included in a PIDF- LO "method" element. In addition, the source of the location information MUST be included in a PIDF-LO "provided-by" element.

ED-42 The "used-for-routing" parameter MUST be set to the location that was chosen for routing.

ED-43 Endpoints SHOULD validate civic locations when they receive them from their LCP. Validation SHOULD be performed in conjunction with the LoST route query to minimize load on the LoST server.

ED-44 If the LCP does not return location in the form of a PIDF-LO [RFC4119] (Peterson, J., “A Presence-based GEOPRIV Location Object Format,” December 2005.), the endpoint MUST map the location information it receives from the configuration protocol to a PIDF-LO.

ED-45 To prevent against spoofing of the DHCP server, elements implementing DHCP for location configuration SHOULD use [RFC3118] (Droms, R. and W. Arbaugh, “Authentication for DHCP Messages,” June 2001.) although the difficulty in providing appropriate credentials is significant.

ED-46 S/MIME MUST NOT be used to encrypt the SIP Geolocation header or bodies.

ED-47 TLS MUST be used to protect location (but see Section 9.1 (Use of TLS)). IPSEC [RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” January 2005.) is an acceptable alternative.

ED-48 Endpoints MUST support one or more mechanisms that allow them to determine their public IP address. Examples include STUN [RFC3489] (Rosenberg, J., Weinberger, J., Huitema, C., and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)," March 2003.) and HTTP get.
ED-49 Endpoints MUST support LIS discovery as described in [I-D.ietf-geopriv-lis-discovery] (Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)," March 2010.), and the LoST discovery as described in [RFC5223] (Schulzrinne, H., Polk, J., and H. Tschofenig, "Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)," August 2008.).
ED-50 The device MUST have a configurable default LoST server parameter. If the device is provided by or managed by a service provider, it is expected that the service provider will configure this option.
ED-51 DHCP LoST discovery MUST be used, if available, in preference to configured LoST servers. If neither DHCP nor configuration leads to an available LoST server, the device MUST query DNS using it's SIP domain for an SRV record for a LoST service and use that server.
ED-52 When an endpoint has obtained a LoST server via an discovery mechanism (e.g., via the DNS or DHCP), it MUST prefer the discovered LoST server over LoST servers configured by other means. That is, the endpoint MUST send queries to this LoST server first, using other LoST servers only if these queries fail.
ED-53 Endpoints who obtain their own location SHOULD perform LoST mapping to the PSAP URI.
ED-54 Mapping SHOULD be performed at boot time and whenever location changes beyond the service boundary obtained from a prior LoST mapping operation or the time-to-live value of that response has expired. The value MUST be cached for possible later use.
ED-55 The endpoint MUST attempt to update its location at the time of an emergency call. If it cannot obtain a new location quickly (see Section 6 (Location and its role in an emergency call)), it MUST use the cached value.
ED-56 The endpoint SHOULD attempt to update the LoST mapping at the time of an emergency call. If it cannot obtain a new mapping quickly, it MUST use the cached value. If the device cannot update the LoST mapping and does not have a cached value, it MUST signal an emergency call without a Route header containing a PSAP URI.
ED-57 [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.) and [RFC3263] (Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers," June 2002.) procedures MUST be used to route an emergency call towards the PSAP's URI.
ED-58 Initial INVITES MUST provide an Offer [RFC3264] (Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)," June 2002.).

ED-59 deleted
ED-60 TLS MUST be specified when attempting to signal an emergency call with SIP per Section 3.1 of [I-D.ietf-sip-sips] (Audet, F., "The use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)," November 2008.). IPSEC [RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," January 2005.) is an acceptable alternative.
ED-61 If TLS session establishment fails, the call MUST be retried without TLS.
ED-62 [I-D.ietf-sip-outbound] (Jennings, C., "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)," June 2009.) is RECOMMENDED to maintain persistent TLS connections between elements.
ED-63 TLS MUST be specified when attempting to retrieve location (configuration or dereferencing) with HELD. The use of [RFC5077] (Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State," January 2008.) is RECOMMENDED to minimize the time to establish TLS sessions without keeping server-side state.
ED-64 If TLS session establishment fails, the location retrieval MUST be retried without TLS.
ED-65 The initial SIP signaling method is an INVITE request:

1. The Request URI SHOULD be the service URN in the "sos" tree, If the device cannot interpret local dial strings, the Request-URI SHOULD be a dial string URI [RFC4967] (Rosen, B., "Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier," July 2007.) with the dialed digits.

2. The To header SHOULD be a service URN in the "sos" tree. If the device cannot interpret local dial strings, the To: SHOULD be a dial string URI with the dialed digits.

3. The From header MUST be present and SHOULD be the AoR of the caller.

4. A Via header MUST be present.

5. A Route header SHOULD be present with a PSAP URI obtained from LoST (see Section 8 (Routing the call to the PSAP)) and the loose route parameter. If the device does not interpret dial plans, or was unable to obtain a route from a LoST server, no Route header will be present.

6. A Contact header MUST be present which MUST be globally routable, for example a GRUU [I-D.ietf-sip-gruu] (Rosenberg, J., "Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)," October 2007.), and be valid for several minutes following the

termination of the call to permit an immediate call-back to the specific device which placed the emergency call.

7. Other headers MAY be included as per normal SIP behavior.

8. A Supported header MUST be included with the 'geolocation' option tag [I-D.ietf-sip-location-conveyance] (Polk, J. and B. Rosen, “Location Conveyance for the Session Initiation Protocol,” March 2009.), unless the device does not understand the concept of SIP location.

9. If a device understands the SIP location conveyance [I-D.ietf-sip-location-conveyance] (Polk, J. and B. Rosen, “Location Conveyance for the Session Initiation Protocol,” March 2009.) extension and has its location available, it MUST include location either by-value, by-reference or both.

10. If a device understands the SIP Location Conveyance extension and has its location unavailable or unknown to that device, it MUST include a Supported header with a "geolocation" option tag, and MUST NOT include a Geolocation header, and not include a PIDF-LO message body.

11. If a device understands the SIP Location Conveyance extension and supports LoST [RFC5222] (Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, “LoST: A Location-to-Service Translation Protocol,” August 2008.), the Geolocation "used-for-routing" header parameter MUST be added to the corresponding URI in the Geolocation header. If the device is unable to obtain a PSAP URI for any reason it MUST NOT include "used-for-routing" on a Geolocation URI, so that downstream entities know that LoST routing has not been completed.

12. A SDP offer MUST be included in the INVITE. If voice is supported the offer MUST include the G.711 codec, see Section 14 (Media).

13. If the device includes location-by-value, the UA MUST support multipart message bodies, since SDP will likely be also in the INVITE.

14. A UAC SHOULD include a "inserted-by=endpoint" header parameter on all Geolocation headers. This informs downstream elements which device entered the location at this URI (either cid-URL or location-by-reference URI).

15. SIP Caller Preferences [RFC3841] (Rosenberg, J., Schulzrinne, H., and P. Kyzivat, “Caller Preferences for the Session Initiation Protocol (SIP),” August 2004.) MAY 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.

ED-66 Devices device SHOULD have a globally routable URI in a Contact: header which remains valid for 30 minutes past the time the original call containing the URI completes unless the device registration expires and is not renewed.
ED-67 During the course of an emergency call, devices and proxies MUST support REFER transactions and the Referred-by: header [RFC3515] (Sparks, R., "The Session Initiation Protocol (SIP) Refer Method," April 2003.).
ED-68 deleted
ED-69 There can be a case where the session signaling path is lost, and the user agent does not receive the BYE. If the call is hung up, and the session timer (if implemented) expires, the call MAY be declared lost. If in the interval, an incoming call is received from the domain of the PSAP, the device MUST drop the old call and alert for the (new) incoming call. Dropping of the old call MUST only occur if the user is attempting to hang up; the domain of an incoming call can only be determined from the From header, which is not reliable, and could be spoofed. Dropping an active call by a new call with a spoofed From: would be a DoS attack.
ED-70 User Agents and proxies MUST disable outgoing call features such as

- *Call Waiting
- *Call Transfer
- *Three Way Call
- *Flash hold
- *Outbound Call Blocking

when an emergency call is established. Also see ED-77 in Section 14 (Media).
ED-71 The emergency dial strings SHOULD NOT be permitted in Call Forward numbers or speed dial lists.
ED-72 The User Agent and Proxies SHOULD disable the following incoming call features on call backs from the PSAP:

- *Call Waiting
- *Do Not Disturb
- *Call Forward (all kinds)

ED-73 Call backs SHOULD be determined by retaining the domain of the PSAP which answers an outgoing emergency call and instantiating a timer which starts when the call is terminated. If a call is received from the same domain and within the timer period, sent to the Contact: or AoR used in the emergency call, it should be assumed to be a call back. The suggested timer period is 5 minutes.

ED-74 Endpoints MUST send and receive media streams on RTP [RFC3550] (Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications,” July 2003.).

ED-75 Normal SIP offer/answer [RFC3264] (Rosenberg, J. and H. Schulzrinne, “An Offer/Answer Model with Session Description Protocol (SDP),” June 2002.) negotiations MUST be used to agree on the media streams to be used.

ED-76 Endpoints supporting voice MUST support G.711 A law (and mu Law if they are intended be used in North America) encoded voice as described in [RFC3551] (Schulzrinne, H. and S. Casner, “RTP Profile for Audio and Video Conferences with Minimal Control,” July 2003.). It is desirable to include wideband codecs such as AMR-WB in the offer.

ED-77 Silence suppression (Voice Activity Detection methods) MUST NOT be used on emergency calls. PSAP call takers sometimes get information on what is happening in the background to determine how to process the call.

ED-78 Endpoints supporting Instant Messaging (IM) MUST support both [RFC3428] (Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, “Session Initiation Protocol (SIP) Extension for Instant Messaging,” December 2002.) and [RFC4975] (Campbell, B., Mahy, R., and C. Jennings, “The Message Session Relay Protocol (MSRP),” September 2007.).

ED-79 Endpoints supporting real-time text MUST use [RFC4103] (Hellstrom, G. and P. Jones, “RTP Payload for Text Conversation,” June 2005.). The expectations for emergency service support for the real-time text medium, described in [RFC5194] (van Wijk, A. and G. Gybels, “Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP),” June 2008.), Section 7.1 SHOULD be fulfilled.

ED-80 Endpoints supporting video MUST support H.264 per [RFC3984] (Wenger, S., Hannuksela, M., Stockhammer, T., Westerlund, M., and D. Singer, “RTP Payload Format for H.264 Video,” February 2005.).

ED-81 INVITE requests to a service URN ending in ".test" indicates a request for an automated test. For example, "urn:service.sos.fire.test". As in standard SIP, a 200 (OK) response indicates that the address was recognized and a 404 (Not found) that it was not. A 486 (Busy Here) MUST be returned if the test service is busy, and a 404 (Not Found) MUST be returned if the PSAP does not support the test mechanism.

ED-82 In its response to the test, the PSAP MAY include a text body (text/plain) indicating the identity of the PSAP, the requested service, and the location reported with the call. For the latter, the PSAP SHOULD return location-by-value even if the original location

delivered with the test was by-reference. If the location-by-reference was supplied, and the dereference requires credentials, the PSAP SHOULD use credentials supplied by the LIS for test purposes. This alerts the LIS that the dereference is not for an actual emergency call and location hiding techniques, if they are being used, may be employed for this dereference. The test response SHOULD be protected with TLS. If the body cannot be protected, the location SHOULD NOT be included in the response.

ED-83 A PSAP accepting a test call SHOULD accept a media loopback test [I-D.ietf-mmusic-media-loopback] (Sivachelvan, C., Venna, N., Jones, P., Stratton, N., Roychowdhury, A., and K. Hedayat, “An Extension to the Session Description Protocol (SDP) for Media Loopback,” April 2010.) and SHOULD support the "rtp-pkt-loopback" and "rtp-start-loopback" options. The user agent would specify a loopback attribute of "loopback-source", the PSAP being the mirror. User Agents should expect the PSAP to loop back no more than 3 packets of each media type accepted (which limits the duration of the test), after which the PSAP would normally send BYE.

ED-84 User agents SHOULD perform a full call test, including media loopback, after a disconnect and subsequent change in IP address not due to a reboot. After an initial test, a full test SHOULD be repeated approximately every 30 days with a random interval.

ED-85 User agents MUST NOT place a test call immediately after booting. If the IP address changes after booting, the UA should wait a random amount of time (in perhaps a 30 minute period, sufficient for any avalanche restart to complete) and then test.

ED-86 PSAPs MAY refuse repeated requests for test from the same device in a short period of time. Any refusal is signaled with a 486 or 488 response.

A.2. Requirements of Service Providers

TOC

SP-1 If a device or application expects to be able to place a call for help, the service provider that supports it MUST facilitate emergency calling. Some jurisdictions have regulations governing this.

SP-2 Proxy servers SHOULD recognize emergency dial strings if for some reason the endpoint does not recognize them. This cannot be relied upon by the device if the service provider cannot always determine the location of the device.

SP-3 Emergency calls MUST be marked with a Service URN in the Request-URI of the INVITE.

SP-4 Local dial strings MUST be recognized.

SP-6 Emergency dial strings SHOULD be determined from LoST [RFC5222] (Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, “LoST: A Location-to-Service Translation Protocol,” August 2008.). Dial Strings MAY be configured directly in the device.

SP-7 If a proxy server recognizes dial strings on behalf of its clients it MUST recognize emergency dial strings represented by [RFC4967] (Rosen, B., "Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier," July 2007.) and SHOULD recognize emergency dial strings represented by a tel URI [RFC3966] (Schulzrinne, H., "The tel URI for Telephone Numbers," December 2004.).
SP-8 Service providers MAY provide home dial strings by configuration.
SP-9 All emergency services specified in [RFC5031] (Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services," January 2008.) MUST be recognized.
SP-10 Endpoints, Intermediate Devices and Service Providers MUST be prepared to handle location represented in either civic or geo form.
SP-11 Elements MUST NOT convert (civic to geo or geo to civic) from the form of location the determination mechanism supplied.
SP-12 Proxies MAY provide location on behalf of devices if:

- The proxy has a relationship with all access networks the device could connect to, and the relationship allows it to obtain location.

- The proxy has an identifier, such as an IP address, that can be used by the access network to determine the location of the endpoint, even in the presence of NAT and VPN tunnels that may obscure the identifier between the access network and the service provider.

SP-13 Where proxies provide location on behalf of endpoints, the service provider MUST ensure that either the end device is provided with the local dial strings for its current location (where the end device recognizes dial strings), or the service provider proxy MUST detect the appropriate local dial strings at the time of the call.
SP-14 When HELD is the LCP, the request MUST specify a value of "emergencyRouting" for the "responseTime" parameter and use the resulting location for routing. If a value for dispatch location will be sent, another request with the "responseTime" parameter set to "emergencyDispatch" must be completed, with the result sent for dispatch purposes.
SP-15 Location sent between SIP elements MUST be conveyed using [I-D.ietf-sip-location-conveyance] (Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol," March 2009.).
SP-16 If the LIS has more than one location for an endpoint it MUST use the procedures in [I-D.ietf-geopriv-pdif-lo-profile] (Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations," November 2008.)
SP-17 If a proxy inserts location on behalf of an endpoint, and it has multiple locations available for the endpoint it MUST choose one location to use to route the call towards the PSAP.
SP-18 If a proxy is attempting to insert location but the UA conveyed a location to it, the proxy MUST use the UA's location for routing and

MUST convey that location towards the PSAP. It MAY also include what it believes the location to be in a separate Geolocation header.
SP-19 All location objects received by a proxy MUST be delivered to the PSAP.
SP-20 Location objects MUST contain information about the method by which the location was determined, such as GPS, manually entered, or based on access network topology included in a PIDF- LO "method" element. In addition, the source of the location information MUST be included in a PIDF-LO "provided-by" element.
SP-21 The "used-for-routing" parameter MUST be set to the location that was chosen for routing.
SP-22 Proxies handling emergency calls MUST insert a default location if the call does not contain a location and the proxy does not have a method for obtaining a better location.
SP-23 Default locations MUST be marked with method=Default and the proxy MUST be identified in provided-by element of the PIDF-LO.
SP-24 TLS MUST be used to protect location (but see Section 9.1 (Use of TLS)). IPSEC [RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," January 2005.) is an acceptable alternative.
SP-25 Service Providers MUST provide an SRV entry in their DNS server which leads to a LoST server
SP-26 Networks MUST be designed so that at least one proxy in the outbound path will recognize emergency calls with a Request URI of the service URN in the "sos" tree. An endpoint places a service URN in the Request URI to indicate that the endpoint understood the call was an emergency call. A proxy that processes such a call looks for the presence of a SIP Route header field with a URI of a PSAP. Absence of such a Route header indicates the UAC was unable to invoke LoST and the proxy MUST perform the LoST mapping and insert a Route header field with the URI obtained.
SP-27 To deal with old user agents that predate this specification and with UAs that do not have access to their own location data, a proxy that recognizes a call as an emergency call that is not marked as such (see Section 5 (Identifying an emergency call)) MUST also perform this mapping, with the best location it has available for the endpoint. The resulting PSAP URI would be placed in a Route header with the service URN in the Request URI.
SP-28 Proxy servers performing mapping SHOULD use location obtained from the access network for the mapping. If no location is available, a default location (see Section 6.11 (Default location)) MUST be supplied.
SP-29 A proxy server which attempts mapping and fails to get a mapping MUST provide a default mapping. A suitable default mapping would be the mapping obtained previously for the default location appropriate for the caller.
SP-30 [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.) and [RFC3263]

(Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” June 2002.) procedures MUST be used to route an emergency call towards the PSAP's URI.
SP-31 TLS MUST be specified when attempting to signal an emergency call with SIP per Section 3.1 of [I-D.ietf-sip-sips] (Audet, F., “The use of the SIPS URI Scheme in the Session Initiation Protocol (SIP),” November 2008.). IPSEC [RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” January 2005.) is an acceptable alternative.
SP-32 If TLS session establishment fails, the call MUST be retried without TLS.
SP-33 [I-D.ietf-sip-outbound] (Jennings, C., “Managing Client Initiated Connections in the Session Initiation Protocol (SIP),” June 2009.) is RECOMMENDED to maintain persistent TLS connections between elements.
SP-34 SIP Proxy servers processing emergency calls:

1. If the proxy interprets dial plans on behalf of user agents, the proxy MUST look for the local emergency dial string at the location of the end device and MAY look for the home dial string. If it finds it, the proxy MUST:

   *Insert a Geolocation header as above. Location-by-reference MUST be used because proxies must not insert bodies.

   *Include the Geolocation "inserted-by=server" and "used-for-routing" parameters.

   *Map the location to a PSAP URI using LoST.

   *Add a Route header with the PSAP URI.

   *Replace the Request-URI (which was the dial string) with the service URN appropriate for the emergency dial string.

   *Route the call using normal SIP routing mechanisms.

2. If the proxy recognizes the service URN in the Request URI, and does not find a a Route header, it MUST query a LoST server. If multiple locations were provided, the proxy uses the location that has the "used-for-routing" marker set. If a location was provided (which should be the case), the proxy uses that location to query LoST. The proxy may have to dereference a location by reference to get a value. If a location is not present, and the proxy can query a LIS which has the location of the UA it MUST do so. If no location is present, and the proxy does not have access to a LIS which could provide location, the proxy MUST supply a default location (See Section 6.11 (Default location)). The location (in the signaling, obtained from a LIS, or default) MUST be used in a query to LoST with the service URN received with the call. The

resulting URI MUST be placed in a Route header added to the call.

3. The "inserted-by=" parameter in any Geolocation: header received on the call MUST NOT be modified or deleted in transit.

4. The proxy SHOULD NOT modify any parameters in Geolocation headers received in the call. It MAY add a Geolocation header. Such an additional location SHOULD NOT be used for routing; the location provided by the UA should be used.

5. Either a P-Asserted-Identity [RFC3325] (Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," November 2002.) or an Identity header [RFC4474] (Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," August 2006.), or both, SHOULD be included to identify the sender. For services which must support emergency calls from unauthenticated devices, valid identity may not be available.

SP-35 Devices device SHOULD have a globally routable URI in a Contact: header which remains valid for 30 minutes past the time the original call containing the URI completes unless the device registration expires and is not renewed.
SP-36 Call backs to the Contact: header URI recieved within 30 minutes of an emergency call must reach the device regardless of call features or services that would normally cause the call to be routed to some other entity.
SP-37 Devices MUST have a persistent AOR URI either in a P-Asserted-Identity: header or From: protected by an Identity header suitable for returning a call some time after the original call. Such a call back would not necessarily reach the device that originally placed the call.
SP-38 During the course of an emergency call, devices and proxies MUST support REFER transactions and the Referred-by: header [RFC3515] (Sparks, R., "The Session Initiation Protocol (SIP) Refer Method," April 2003.).
SP-39 User Agents and proxies MUST disable outgoing call features such as

*Call Waiting

*Call Transfer

*Three Way Call

*Flash hold

*Outbound Call Blocking

when an emergency call is established. Also see ED-77 in Section 14 (Media).
SP-40 The emergency dial strings SHOULD NOT be permitted in Call Forward numbers or speed dial lists.
SP-41 The User Agent and Proxies SHOULD disable the following incoming call features on call backs from the PSAP:

*Call Waiting

*Do Not Disturb

*Call Forward (all kinds)

A.3. Requirements of Access Network

TOC

AN-1 LoST servers MUST return dial strings for emergency services
AN-2 Elements MUST NOT convert (civic to geo or geo to civic) from the form of location the determination mechanism supplied.
AN-3 Any suitable location determination mechanism MAY be used.
AN-4 Devices, intermediate Devices and/or access networks SHOULD support a manual method to "override" the location the access network determines. Where a civic form of location is provided, all fields in the PIDF-LO [RFC4119] (Peterson, J., “A Presence-based GEOPRIV Location Object Format,” December 2005.) and [RFC5139] (Thomson, M. and J. Winterbottom, “Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO),” February 2008.) MUST be able to be specified.
AN-5 Access networks supporting copper, fiber or other hard wired IP packet service SHOULD support location configuration. If the network does not support location configuration, it MUST require every device that connects to the network to support end system measured location.
AN-6 Access networks and intermediate devices providing wire database location information SHOULD provide interior location data (building, floor, room, cubicle) where possible. It is RECOMMENDED that interior location be provided when spaces exceed approximately 650 square meters.
AN-7 Access networks and intermediate devices (including enterprise networks) which support intermediate range wireless connections (typically 100m or less of range) and which do not support a more accurate location determination mechanism such as triangulation, MUST support location configuration where the location of the access point is reflected as the location of the clients of that access point. Where the access network provides location configuration, intermediate devices MUST either be transparent to it, or provide an interconnected client for the supported configuration mechanism and a server for a

configuration protocol supported by end devices downstream of the intermediate device

AN-8 Devices that support endpoint measuring of location MUST have at least a coarse location capability (typically <1km accuracy when not location hiding) for routing of calls. The location mechanism MAY be a service provided by the access network.

AN-9 Access networks MAY provide network-measured location determination. Wireless access network which do not support network measured location MUST require that all devices connected to the network have end-system measured location. Uncertainty of less than 100 m with 95% confidence SHOULD be available for dispatch.

AN-10 Access networks that provide network measured location MUST have at least a coarse location (typically <1km when not location hiding) capability at all times for routing of calls.

AN-11 Access networks with range of <10 meters (e.g. personnal area networks such as Bluetooth MUST provide a location to mobile devices connected to them. The location provided SHOULD be that of the access point location unless a more accurate mechanism is provided.

AN-12 The access network MUST support either DHCP location options or HELD. The access network SHOULD support other location technologies that are specific to the type of access network.

AN-13 Where a router is employed between a LAN and WAN in a small (less than approximately 650 square meters) area, the router MUST be transparent to the location provided by the WAN to the LAN. This may mean the router must obtain location as a client from the WAN, and supply an LCP server to the LAN with the location it obtains. Where the area is larger, the LAN MUST have a location configuration mechanism meeting this BCP.

AN-14 Access networks that support more than one LCP MUST reply with the same location information (within the limits of the data format for the specific LCP) for all LCPs it supports.

AN-15 Network administrators MUST take care in assigning IP addresses such that VPN address assignments can be distinguished from local devices (by subnet choice, for example), and LISs SHOULD NOT attempt to provide location to addresses that arrive via VPN connections unless it can accurately determine the location for such addresses.

AN-16 Placement of NAT devices where an LCP uses IP address for an identifier SHOULD consider the effect of the NAT on the LCP. The address used to query the LIS MUST be able to correctly identify the record in the LIS representing the location of the querying device

AN-17 It is RECOMMENDED that location determination not take longer than 250 ms to obtain routing location and systems SHOULD be designed such that the typical response is under 100 ms. However, as much as 3 seconds to obtain routing location MAY be tolerated if location accuracy can be substantially improved over what can be obtained in 250 ms.

AN-18 Where the absolute location or the accuracy of location of the endpoint may change between the time the call is received at the PSAP

and the time dispatch is completed, location update mechanisms MUST be provided.

AN-19 Mobile devices MUST be provided with a mechanism to get repeated location updates to track the motion of the device during the complete processing of the call.

AN-20 The LIS SHOULD provide a location reference which permits a subscription with appropriate filtering.

AN-21 For calls sent with location-by-reference, with a SIP or SIPS scheme, the server resolving the reference MUST support a SUBSCRIBE [RFC3265] (Roach, A., "Session Initiation Protocol (SIP)-Specific Event Notification," June 2002.) to the presence event [RFC3856] (Rosenberg, J., "A Presence Event Package for the Session Initiation Protocol (SIP)," August 2004.). For other location-by-reference schemes that do not support subscription, the PSAP will have to repeatedly dereference the URI to determine if the device moved.

AN-22 A LIS should perform location validation of civic locations via LoST before entering a location in its database.

AN-23 When the access network cannot determine the actual location of the caller, it MUST supply a default location. The default SHOULD be chosen to be as close to the probable location of the device as the network can determine. See [I-D.ietf-ecrit-framework] (Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet Multimedia," July 2009.)

AN-24 Default locations MUST be marked with method=Default and the proxy MUST be identified in provided-by element of the PIDF-LO.

AN-25 To prevent against spoofing of the DHCP server, elements implementing DHCP for location configuration SHOULD use [RFC3118] (Droms, R. and W. Arbaugh, "Authentication for DHCP Messages," June 2001.) although the difficulty in providing appropriate credentials is significant.

AN-26 Access networks which support DHCP MUST implement the LoST discovery option

AN-27 Access Networks that use HELD and that have a DHCP server SHOULD support DHCP options for providing LIS and LoST servers.

AN-28 TLS MUST be specified when attempting to retrieve location (configuration or dereferencing) with HELD. The use of [RFC5077] (Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State," January 2008.) is RECOMMENDED to minimize the time to establish TLS sessions without keeping server-side state.

AN-29 If TLS session establishment fails, the location retrieval MUST be retried without TLS.

TOC

A.4. Requirements of Intermediate Devices

INT-1 Endpoints, Intermediate Devices and Service Providers MUST be prepared to handle location represented in either civic or geo form.
INT-2 Elements MUST NOT convert (civic to geo or geo to civic) from the form of location the determination mechanism supplied.
INT-3 Any suitable location determination mechanism MAY be used.
INT-4 Devices, intermediate Devices and/or access networks SHOULD support a manual method to "override" the location the access network determines. Where a civic form of location is provided, all fields in the PIDF-LO [RFC4119] (Peterson, J., “A Presence-based GEOPRIV Location Object Format,” December 2005.) and [RFC5139] (Thomson, M. and J. Winterbottom, “Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO),” February 2008.) MUST be able to be specified.
INT-5 Access networks and intermediate devices providing wire database location information SHOULD provide interior location data (building, floor, room, cubicle) where possible. It is RECOMMENDED that interior location be provided when spaces exceed approximately 650 square meters.
INT-6 Access networks and intermediate devices (including enterprise networks) which support intermediate range wireless connections (typically 100m or less of range) and which do not support a more accurate location determination mechanism such as triangulation, MUST support location configuration where the location of the access point is reflected as the location of the clients of that access point. Where the access network provides location configuration, intermediate devices MUST either be transparent to it, or provide an interconnected client for the supported configuration mechanism and a server for a configuration protocol supported by end devices downstream of the intermediate device
INT-7 Devices MAY support end-system measured location. Uncertainty of less than 100 m with 95% confidence SHOULD be available for dispatch.
INT-8 Devices that support endpoint measuring of location MUST have at least a coarse location capability (typically <1km accuracy when not location hiding) for routing of calls. The location mechanism MAY be a service provided by the access network.
INT-9 Endpoints SHOULD attempt to configure their own location using the LCPs listed in ED-21.
INT-10 Where proxies provide location on behalf of endpoints, the service provider MUST ensure that either the end device is provided with the local dial strings for its current location (where the end device recognizes dial strings), or the service provider proxy MUST detect the appropriate local dial strings at the time of the call.
INT-11 Devices SHOULD be able to accept and forward location by value or by reference. An end device that receives location by reference (and does not also get the corresponding value) MUST be able to perform a dereference operation to obtain a value.

INT-12 Devices MUST support both the DHCP location options [RFC4776] (Schulzrinne, H., “Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information,” November 2006.), [RFC3825] (Polk, J., Schnizlein, J., and M. Linsner, “Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information,” July 2004.) and HELD [I-D.ietf-geopriv-http-location-delivery] (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, “HTTP Enabled Location Delivery (HELD),” August 2009.). When devices deploy a specific access network interface in which that access network supports location discovery such as LLDP-MED or 802.11v, the device SHOULD support the additional respective access network specific location discovery mechanism.
INT-13 The access network MUST support either DHCP location options or HELD. The access network SHOULD support other location technologies that are specific to the type of access network.
INT-14 Where a router is employed between a LAN and WAN in a small (less than approximately 650 square meters) area, the router MUST be transparent to the location provided by the WAN to the LAN. This may mean the router must obtain location as a client from the WAN, and supply an LCP server to the LAN with the location it obtains. Where the area is larger, the LAN MUST have a location configuration mechanism meeting this BCP.
INT-15 Endpoints SHOULD try all LCPs supported by the device in any order or in parallel. The first one that succeeds in supplying location can be used.
INT-16 Access networks that support more than one LCP MUST reply with the same location information (within the limits of the data format for the specific LCP) for all LCPs it supports.
INT-17 When HELD is the LCP, the request MUST specify a value of "emergencyRouting" for the "responseTime" parameter and use the resulting location for routing. If a value for dispatch location will be sent, another request with the "responseTime" parameter set to "emergencyDispatch" must be completed, with the result sent for dispatch purposes.
INT-18 Endpoints SHOULD obtain location immediately after obtaining local network configuration information. When HELD is the LCP the client MUST support a random back-off period (between 30 seconds and 300 seconds) for re-trying the HELD query, when no response is received, and no other LCP provided location information.
INT-19 If the device is configured to use DHCP for bootstrapping, it MUST include both options for location acquisition (civic and geodetic), the option for LIS discovery, and the option for LoST discovery as defined in [RFC4776] (Schulzrinne, H., “Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information,” November 2006.), [RFC3825] (Polk, J., Schnizlein, J., and M. Linsner, “Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information,” July 2004.), [I-D.ietf-geopriv-lis-discovery] (Thomson, M. and J. Winterbottom, “Discovering the Local Location Information Server

(LIS)," March 2010.) and [RFC5223] (Schulzrinne, H., Polk, J., and H. Tschofenig, "Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)," August 2008.).

INT-20 If the device sends a DHCPINFORM message, it MUST include both options for location acquisition (civic and geodetic), the option for LIS discovery, and the option for LoST discovery as defined in [RFC4776] (Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information," November 2006.), [RFC3825] (Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information," July 2004.), [I-D.ietf-geopriv-lis-discovery] (Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)," March 2010.) and [RFC5223] (Schulzrinne, H., Polk, J., and H. Tschofenig, "Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)," August 2008.).

INT-21 To minimize the effects of VPNs that do not allow packets to be sent via the native hardware interface rather than via the VPN tunnel, location configuration SHOULD be attempted before such tunnels are established.

INT-22 Software which uses LCPs SHOULD locate and use the actual hardware network interface rather than a VPN tunnel interface to direct LCP requests to the LIS in the actual access network.

INT-23 For devices which are not expected to roam, refreshing location on the order of once per day is RECOMMENDED.

INT-24 For devices which roam, refresh of location information SHOULD be more frequent, with the frequency related to the mobility of the device and the ability of the access network to support the refresh operation. If the device can detect that it has moved, for example when it changes access points, the device SHOULD refresh its location.

INT-25 It is RECOMMENDED that location determination not take longer than 250 ms to obtain routing location and systems SHOULD be designed such that the typical response is under 100 ms. However, as much as 3 seconds to obtain routing location MAY be tolerated if location accuracy can be substantially improved over what can be obtained in 250 ms.

Authors' Addresses

TOC

	Brian Rosen
	NeuStar
	470 Conrad Dr.
	Mars, PA 16046
	US
Phone:	+1 724 382 1051
Email:	br@brianrosen.net

	James Polk
	Cisco Systems
	3913 Treemont Circle
	Colleyville, TX 76034
	US
Phone:	+1-817-271-3552
Email:	jmpolk@cisco.com