ECRIT	H. Schulzrinne	
Internet-Draft	Columbia University	
Intended status: Standards Track	S. McCann	
Expires: April 28, 2011	Research in Motion UK Ltd	
	G. Bajko	
	Nokia	
	H. Tschofenig	
	D. Kroeselberg	
	Nokia Siemens Networks	
	October 25, 2010	

TOC

Extensions to the Emergency Services Architecture for dealing with Unauthenticated and Unauthorized Devices
draft-ietf-ecrit-unauthenticated-access-01.txt

Abstract

The IETF emergency services architecture assumes that the calling device has acquired rights to use the access network or that no authentication is required for the access network, such as for public wireless access points. Subsequent protocol interactions, such as obtaining location information, learning the address of the Public Safety Answering Point (PSAP) and the emergency call itself are largely decoupled from the underlying network access procedures.
In some cases, however, the device does not have these credentials for network access, does not have a VoIP service provider, or the credentials have become invalid, e.g., because the user has exhausted their prepaid balance or the account has expired.
This document provides a problem statement, introduces terminology and describes an extension for the base IETF emergency services architecture to address these scenarios.

Status of this Memo

Copyright Notice

Table of Contents

---

1. Introduction

TOC

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

Roughly speaking, the IETF emergency services architecture (see [I-D.ietf-ecrit-phonebcp] (Rosen, B. and J. Polk, “Best Current Practice for Communications Services in support of Emergency Calling,” July 2010.) and [I-D.ietf-ecrit-framework] (Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, “Framework for Emergency Calling using Internet Multimedia,” July 2010.)) divides responsibility for handling emergency calls between the access network (ISP), the application service provider (ASP) that may be a VoIP service provider and the provider of emergency signaling services, the emergency service network (ESN). The access network may provide location information to end systems, but does not have to provide any ASP signaling functionality. The emergency caller can reach the ESN either directly or through the ASP's outbound proxy. Any of the three parties can provide the mapping from location to PSAP URI by offering LoST [RFC5222] (Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, “LoST: A Location-to-Service Translation Protocol,” August 2008.) services.

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

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

We distinguish between three conditions:

No Access Authentication (NAA):
In the NAA case, the emergency caller does not posses valid credentials for the access network. This includes the case where the access network allows pay-per-use, as is common for wireless hotspots, but there is insufficient time to enter credit card details and other registration information required for access. It also covers all cases where either no credentials are available at all, or the available credentials do not work for the given IAP/ISP. As a result, the NAA case basically combines the below NASP and ZBP cases, but at the IAP/ISP level. Support for emergency call handling in the NAA case is subject to the local policy of the ISP. Such policy may vary substantially between ISPs and typically depends on external factors that are not under the ISP control.

No ASP (NASP): The caller does not have an ASP at the time of the call. This can occur either in case the caller does not possess any valid subscription for a reachable ASP, or in case none of the ASPs where the caller owns a valid subscription is reachable through the ISP.
Note: The interoperability need is increased with this scenario since the client software used by the emergency caller must be compatible with the protocols and extensions deployed by the ESN.

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

These three cases are not mutually exclusive. A caller in need for help may find himself/herself in, for example, a NAA and NASP situation, as explained in more details in Figure 1 (Flow Diagram). Depending on local policy and regulations, it may not be possible to place emergency calls in the NAA case. Unless local regulations require user identification, it should always be possible to place calls in the NASP case, with minimal impact on the ISP. Unless the ESN requires that all calls traverse a known set of VSPs, it is technically possible to let a caller place an emergency call in the ZBP case. We discuss each case in more details in Section 3 (Use Case Categories).
Note: At the time of writing there is no regulation in place that demands the functionality described in this memo. SDOs have started their work on this subject in a proactive fashion in the anticipation that national regulation will demand it for a subset of network environments.
There are also indications that the functionality of unauthenticated emergency calls (called SIM-less calls) in today's cellular system in certain countries leads to a fair amount of hoax or test calls. This

causes overload situations at PSAPs which is considered harmful to the overall availability and reliability of emergency services.
As an example, Federal Office of Communications (OFCOM, Switzerland) provided statistics about emergency (112) calls in Switzerland from Jan. 1997 to Nov. 2001. Switzerland did not offer SIM-less emergency calls except for almost a month in July 2000 where a significant increase in hoax and test calls was reported. As a consequence, the functionality was disabled again. More details can be found in the panel presentations of the 3rd SDO Emergency Services Workshop [esw07] (, "3rd SDO Emergency Services Workshop, http://www.emergency-services-coordination.info/2007Nov/," October 30th - November 1st 2007.).

---

2. Terminology

TOC

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [RFC2119] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.).
This document reuses terminology from [RFC5687] (Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol: Problem Statement and Requirements," March 2010.) and [RFC5012] (Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies," January 2008.), namely Internet Access Provider (IAP), Internet Service Provider (ISP), Application Service Provider (ASP), Voice Service Provider (VSP), Emergency Service Routing Proxy (ESRP), Public Safety Answering Point (PSAP), Location Configuration Server (LCS), (emergency) service dial string, and (emergency) service identifier.

---

3. Use Case Categories

TOC

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

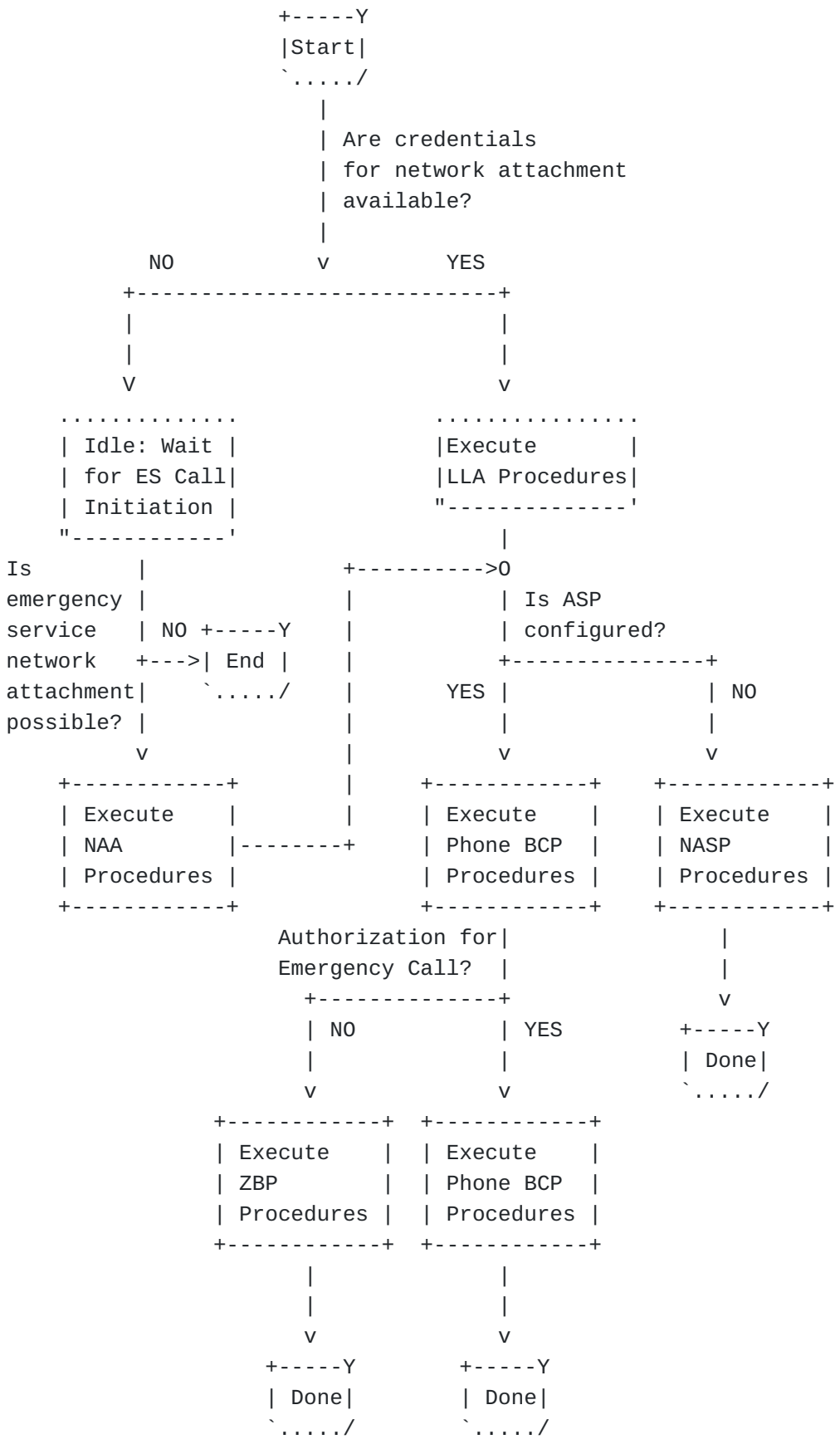
Link Layer Attachment: Some radio networks have added support for unauthenticated emergency access, some other type of networks advertise these capabilities using layer beacons. The end host learns about these unauthenticated emergency services capabilities either from the link layer type or from advertisement.
The end host uses the link layer specific network attachment procedures defined for unauthenticated network access in order to

get access to the network.

Pre-Emergency Service Configuration: When the link layer network attachment procedure is completed the end host learns basic configuration information using DHCP from the ISP, including the address of the LoST server. The end host uses a Location Configuration Protocol (LCP) to retrieve location information. Subsequently, the LoST protocol [RFC5222] (Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol," August 2008.) is used to learn the relevant emergency numbers, and to obtain the PSAP URI applicable for that location.

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

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


+-----Y
|Start|
`...../
Are credentials
for network attachment
available?
NO
YES
Idle: Wait
for ES Call
Initiation
Execute
LLA Procedures
Is
emergency
service
network
attachment
possible?
NO
End
Is ASP
configured?
YES
NO
Execute
NAA
Procedures
Execute
Phone BCP
Procedures
Execute
NASP
Procedures
Authorization for
Emergency Call?
NO
YES
Done
Execute
ZBP
Procedures
Execute
Phone BCP
Procedures
Done
Done

```
Abbreviations:
  LLA: Link Layer Attachment
  ES: Emergency Services
```

Figure 1: Flow Diagram

4. ZBP Considerations

TOC

Although subject to local regulatory mandates, it is expected that for most ASPs even with a lack of authorization for regular service an otherwise authenticated and known subscriber must be granted access to emergency services. Naturally, without an obligation to support emergency services in ZBP cases an ASP can simply disallow access by such customers. As a result, all such subscribers may fall back into a NASP situation as described above.

If ASPs desire or are required by regulation to provide emergency services to subscribers with valid credentials that only fail authorization, the emergency services nature of a call can easily be determined by inspecting the call setup procedure for the presence of the emergency service URNs. This example shows that in the context of this document no specific considerations apply to the ZBP case due to the fact that the ASP will be able to relate the service request to an existing subscription or user and will be in control of adjusting any authorization decision based on its deployemnt specific policy. It is, however, noted that specific security considerations apply due to the fact that emergency service access will likely be granted with limited authorization only, see Section 7 (Security Considerations).

ZBP cases in the context of this document cover all cases where an otherwise valid subscription lacks authorization to access or regular ASP services, i.e., a lack of authorization that would block the subscriber from using the service for emergency purpose. Example ZBP cases include empty prepaid accounts, barred accounts, or certain roaming or mobility restrictions. The exact list of cases where emergency services need to be supported by the ASP is local to the ASP policy and deployment, and is therefore beyond the scope of this document.

TOC

5. NASP Considerations

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

*As an initial step the devices attaches to the network as shown in step (1). This step is outside the scope of this section.

*When the link layer network attachment procedure is completed the end host learns basic configuration information using DHCP from the ISP, including the address of the ESRP, as shown in step (2).

*When the IP address configuration is completed then the SIP UA initiates a SIP INVITE towards the indicated ESRP, as shown in (3). The INVITE message contains all the necessary parameters required by Section 5.1.5 (SIP Emergency Call Signaling).

*The ESRP receives the INVITE and processes it according to the description in Section 5.3.3 (SIP Emergency Call Signaling). The location of the end host may need to be determined using a protocol interaction shown in (4).

*Potentially, an interaction between the LCS of the ISP and the LCS of the IAP may be necessary, see (5).

*Finally, the correct PSAP for the location of the end host has to be evaluated, see (6).

*The ESRP routes the call to the PSAP, as shown in (7).

*The PSAP evaluates the initial INVITE and aims to complete the call setup.

*Finally, when the call setup is completed media traffic can be exchanged between the PSAP and the emergency caller.

For editorial reasons the end-to-end SIP and media exchange between the PSAP and SIP UA are not shown in Figure 2 (Architectural Overview). Two important aspects are worth to highlight:

*The IAP/ISP needs to understand the concept of emergency calls or other emergency applicationsand the SIP profile described in this document. No other VoIP protocol profile, such as XMPP, Skype, etc., are supported for emergency calls in this particular architecture. Other profiles may be added in the future, but the deployment effort is enormous since they have to be universally deployed.

*The end host has no obligation to determine location information. It may attach location information if it has location available (e.g., from a GPS receiver).

Figure 2 (Architectural Overview) shows that the ISP needs to deploy SIP-based emergency services functionality. It is important to note that the ISP itself may outsource the functionality by simply providing access to them (e.g., it puts the IP address of an ESRP or a LoST server into an allow-list). For editorial reasons this outsourcing is not shown.

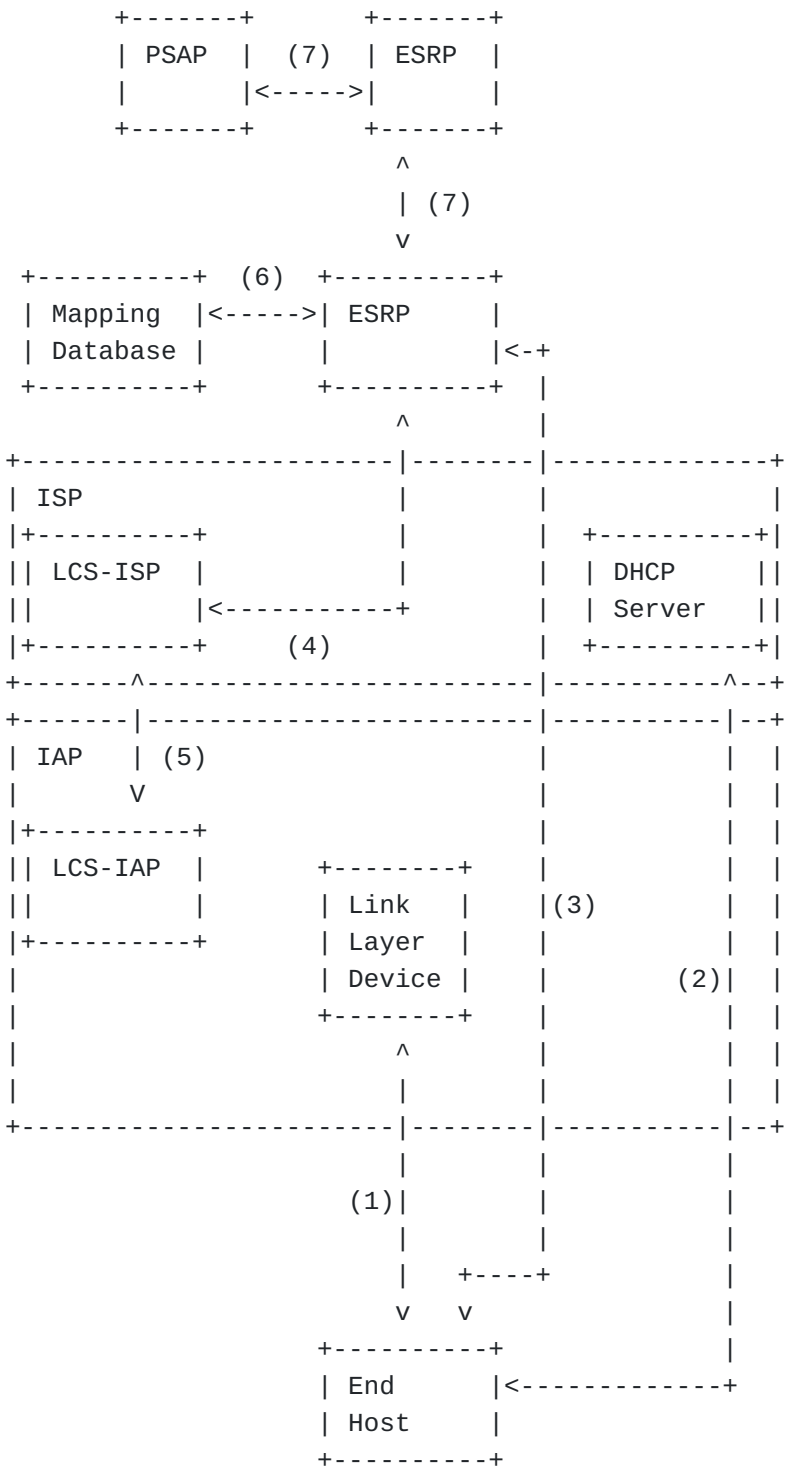


Figure 2: Architectural Overview

Note: Figure 2 (Architectural Overview) does not indicate who runs the ESRP or the mapping database. There are different options available.

5.1. End Host Profile

TOC

5.1.1. LoST Server Discovery

TOC

The end host MAY attempt to use [RFC5222] (Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, “LoST: A Location-to-Service Translation Protocol,” August 2008.) to discover a LoST server. If that attempt fails, the end host SHOULD attempt to discover the address of an ESRP.

5.1.2. ESRP Discovery

TOC

The end host only needs an ESRP when location configuration or LoST server discovery fails. If that is the case, then the end host MUST use the "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers" [RFC3361] (Schulzrinne, H., “Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers,” August 2002.) (for IPv6) and / or the "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers" [RFC3319] (Schulzrinne, H. and B. Volz, “Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers,” July 2003.) to discover the address of an ESRP. This SIP proxy located in the ISP network will be used as the ESRP for routing emergency calls. There is no need to discovery a separate SIP proxy with specific emergency call functionality since the internal procedure for emergency call processing is subject of ISP internal operation.

5.1.3. Location Determination and Location Configuration

TOC

The end host SHOULD attempt to use the supported LCPs to configure its location. If no LCP is supported in the end host or the location configuration is not successful, then the end host MUST attempt to discover an ESRP, which would assist the end host in providing the location to the PSAP.
The SIP UA in the end host MUST attach available location information in a PIDF-LO [RFC4119] (Peterson, J., “A Presence-based GEOPRIV Location Object Format,” December 2005.) when making an emergency call. When constructing the PIDF-LO the guidelines in PIDF-LO profile

[RFC5491] (Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations," March 2009.) MUST be followed. For civic location information the format defined in [RFC5139] (Thomson, M. and J. Winterbottom, "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)," February 2008.) MUST be supported.

5.1.4. Emergency Call Identification

TOC

To determine which calls are emergency calls, some entity needs to map a user entered dialstring into this URN scheme. A user may "dial" 1-1-2, but the call would be sent to urn:service:sos. This mapping SHOULD be performed at the endpoint device.
End hosts MUST use the Service URN mechanism [RFC5031] (Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services," January 2008.) to mark calls as emergency calls for their home emergency dial string (if known). For visited emergency dial string the translation into the Service URN mechanism is not mandatory since the ESRP in the ISPs network knows the visited emergency dial strings.

5.1.5. SIP Emergency Call Signaling

TOC

SIP signaling capabilities [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.) are mandated for end hosts.
The initial SIP signaling method is an INVITE. The SIP INVITE request MUST be constructed according to the requirements in Section 9.2 [I-D.ietf-ecrit-phonebcp] (Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling," July 2010.).
Regarding callback behavior SIP UAs MUST have a globally routable URI in a Contact: header.

5.1.6. Media

TOC

End points MUST comply with the media requirements for end points placing an emergency call found in Section 14 of [I-D.ietf-ecrit-phonebcp] (Rosen, B. and J. Polk, "Best Current

Practice for Communications Services in support of Emergency Calling," July 2010.).

5.1.7. Testing

TOC

The description in Section 15 of [I-D.ietf-ecrit-phonebcp] (Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling," July 2010.) is fully applicable to this document.

5.2. IAP/ISP Profile

TOC

5.2.1. ESRP Discovery

TOC

An ISP hosting an ESRP MUST implement the server side part of "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers" [RFC3361] (Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers," August 2002.) (for IPv4) and / or the "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers" [RFC3319] (Schulzrinne, H. and B. Volz, "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers," July 2003.).

5.2.2. Location Determination and Location Configuration

TOC

When receiving an INVITE message the following steps are done:

1. If the INVITE message does not include location information the ESRP-registrar MUST use HELD identity [I-D.ietf-geopriv-held-identity-extensions] (Winterbottom, J., Thomson, M., Tschofenig, H., and R. Barnes, "Use of Device Identity in HTTP-Enabled Location Delivery (HELD)," October 2010.) to obtain the location of the device as both a location value and reference. In order to contact the LIS the ESRP-registrar SHOULD determine the LIS address using the mechanism described in [I-D.thomson-geopriv-res-gw-lis-discovery] (Thomson, M. and R.

Bellis, “Location Information Server (LIS) Discovery using IP address and Reverse DNS,” September 2010.). The ESRP-registrar MAY use other methods for LIS determination where available.

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

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

5.3. ESRP Profile

TOC

5.3.1. Emergency Call Routing

TOC

The ESRP must route the emergency call to the PSAP responsible for the physical location of the end host. However, a standardized approach for determining the correct PSAP based on a given location is useful but not mandatory.
For cases where a standardized protocol is used LoST [RFC5222] (Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, “LoST: A Location-to-Service Translation Protocol,” August 2008.) is a suitable mechanism.

5.3.2. Emergency Call Identification

TOC

The ESRP MUST understand the Service URN mechanism [RFC5031] (Schulzrinne, H., “A Uniform Resource Name (URN) for Emergency and Other Well-Known Services,” January 2008.) (i.e., the 'urn:service:sos' tree) and additionally the national emergency dial strings. The ESRP SHOULD perform a mapping of national emergency dial strings to Service URNs to simplify processing at PSAPs.

5.3.3. SIP Emergency Call Signaling

TOC

SIP signaling capabilities [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.) are mandated for the ESRP. The ESRP MUST process the messages sent by the client, according to Section 5.1.5 (SIP Emergency Call Signaling). Furthermore, the ESRP MUST be able to add a reference to location information, as described in SIP Location Conveyance [I-D.ietf-sipcore-location-conveyance] (Polk, J., Rosen, B., and J. Peterson, "Location Conveyance for the Session Initiation Protocol," July 2010.), before forwarding the call to the PSAP. The ISP MUST be prepared to receive incoming dereferencing requests to resolve the reference to the location information.

5.3.4. Location Retrieval

TOC

The ESRP acts a location recipient and the usage of HELD [RFC5985] (Barnes, M., "HTTP-Enabled Location Delivery (HELD)," September 2010.) with the identity extensions [I-D.ietf-geopriv-held-identity-extensions] (Winterbottom, J., Thomson, M., Tschofenig, H., and R. Barnes, "Use of Device Identity in HTTP-Enabled Location Delivery (HELD)," October 2010.) may be a possible choice. The ESRP would thereby act as a HELD client and the corresponding LIS at the ISP as the HELD server.
The ESRP needs to obtain enough information to route the call. The ESRP itself, however, does not necessarily need to process location information obtained via HELD since it may be used as input to LoST to obtain the PSAP URI.

---

6. Lower Layer Considerations for NAA Case

TOC

Some radio networks have added support for unauthenticated emergency access, some other type of networks advertise these capabilities using layer beacons. The end host learns about these unauthenticated emergency services capabilities either from the link layer type or from advertisement.
This section discusses different methods to indicate an emergency service request as part of network attachment. It provides some general considerations and recommendations that are not specific to the access technology.
To perform network attachment and get access to the resources provided by an IAP/ISP, the end host uses access technology specific network

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

Link layer emergency indication: The end host provides an indication, e.g. an emergency parameter or flag, as part of the link layer signaling for initial network attachment. Examples include an emergency bit signalled in the IEEE 802.16-2009 wireless link. signalling allows an IEEE 802.1X to occur without exchanging cryptogrpahic keys.

Higher-layer emergency indication: Typically emergency indication in access authentication. The emergency caller's end host provides an indication as part of the access authentication exchanges. EAP based authentication is of particular relevance here. [nwgstg3] (, "WiMAX Forum WMF-T33-001-R015V01, WiMAX Network Architecture Stage-3 http://www.wimaxforum.org/sites/wimaxforum.org/files/ technical_document/2009/09/DRAFT-T33-001-R015v01-O_Network-Stage3-Base.pdf," September 2009.).

6.1. Link Layer Emergency Indication

TOC

In general, link layer emergency indications provide good integration into the actual network access procedure regarding the enabling of means to recognize and prioritize an emergency service request from an end host at a very early stage of the network attachment procedure. However, support in end hosts for such methods cannot be considered to be commonly available.
No general recommendations are given in the scope of this memo due to the following reasons:

*Dependency on the specific access technology.

*Dependency on the specific access network architecture. Access authorization and policy decisions typically happen at a different layers of the protocol stack and in different entities than those terminating the link-layer signaling. As a result, link layer indications need to be distributed and translated between the different involved protocol layers and entities. Appropriate methods are specific to the actual architecture of the IAP/ISP network.

6.2. Higher-Layer Emergency Indication

TOC

This section focuses on emergency indications based on authentication and authorization in EAP-based network access.
An advantage of combining emergency indications with the actual network attachment procedure performing authentication and authorization is the fact that the emergency indication can directly be taken into account in the authentication and authorization server that owns the policy for granting access to the network resources. As a result, there is no direct dependency on the access network architecture that otherwise would need to take care of merging link-layer indications into the AA and policy decision process.
EAP signaling happens at a relatively early stage of network attachment, so it is likely to match most requirements for prioritization of emergency signaling. However, it does not cover early stages of link layer activity in the network attachment process. Possible conflicts may arise e.g. in case of MAC-based filtering in entities terminating the link-layer signaling in the network (like a base station). In normal operation, EAP related information will only be recognized in the NAS. Any entity residing between end host and NAS should not be expected to understand/parse EAP messages.
The following potential methods to provide emergency indications in combination with EAP-based network attachment, are recognized:

1. NAI-based emergency indication:

   An emergency indication can be given by forming a specific NAI that is used as the identity in EAP based authentication for network entry. Methods include:

2. **1.a) NAI Decoration:**
   NAI decoration is commonly used in routing EAP responses within the IAP/ISP AAA infrastructure. Additional decoration can be used to add an indication that the network attachment attempt is meant for accessing emergency services. Potential advantages of such approach include that it requires only minimal realization effort compared to link-layer indications with good integration into the authentication and authorization procedures. The same procedure can be used for all NAA cases (both unauthenticated and unauthorized) as well as for normal attachment with a valid subscription. A potential disadvantage is that such EAP decoration is not globally defined across all different access technologies.

   1.b) Emergency NAI:
   The NAI comes with a realm or username

part indicating emergency (e.g. 'emergency@emergency.com'). An advantage of this method for NAA cases is that no new requirements are put on the involved signaling procedures. Only the identity used for network entry is impacted. Potential disadvantages include that different methods to indicate emergency for NAA cases and standard emergency network attachments may be required. Also, modifying the NAI itself (the username@realm part) may conflict with network selection and network entry procedures, depending on the actual access network.

3. Emergency EAP method

An emergency indication can be given by using a dedicated EAP method that is reserved for emergency network attachment only.

2.a) Existing EAP method with New Method Type: An existing EAP method may be used. EAP methods themselves typically do not support emergency indication. One option would be to pick a common EAP method like EAP-TLS and allocate a new method type for the same method that is exclusively reserved to emergency use. Such EAP method should be chosen in a way that the same method can support NAA cases as well as standard emergency network attachment.

2.b) Existing EAP Method: Same as 2a), but without assigning a new EAP method type for emergency. In this case some implicit indication must be used. For example, in cases where EAP-TLS is used in network attachment in combination with client certificates, the absence of a client certificate could be interpreted by the network as a request for emergency network attachment.

2.c) Emergency EAP Method: A new EAP method could be defined that is specifically designed for emergency network entry in NAA cases. Most likely, such EAP method would not be usable for standard emergency network attachment with an existing subscription. Such dedicated emergency EAP method should be key-generating in compliance with RFC3748 to enable the regular air interface security methods even in unauthenticated operation.

6.3. Securing Network Attachment in NAA Cases

TOC

For network attachment in NAA cases, it may make sense to secure the link-layer connection between the device and the IAP/ISP. This especially holds for wireless access with examples being based access. The latter even mandates secured communication across the wireless link for all IAP/ISP networks based on [nwgstg3] (, “WiMAX Forum WMF-T33-001-R015V01, WiMAX Network Architecture Stage-3 http://www.wimaxforum.org/sites/wimaxforum.org/files/ technical_document/2009/09/DRAFT-T33-001-R015v01-O_Network-Stage3-Base.pdf,” September 2009.).
Therefore, for network attachment that is by default based on EAP authentication it is desirable also for NAA network attachment to use a key-generating EAP method (that provides an MSK key to the authenticator to bootstrap further key derivation for protecting the wireless link).
The following approaches to match the above can be identified:

1) Server-only Authentication:
The device of the emergency service requester performs an EAP method with the IAP/ISP EAP server that performs server authentication only. An example for this is EAP-TLS. This provides a certain level of assurance about the IAP/ISP to the device user. It requires the device to be provisioned with appropriate trusted root certificates to be able to verify the server certificate of the EAP server (unless this step is explicitly skipped in the device in case of an emergency service request).

2) Null Authentication:
an EAP method is performed. However, no credentials specific to either the server or the device or subscription are used as part of the authentication exchange. An example for this would be an EAP-TLS exchange with using the TLS_DH_anon (anonymous) ciphersuite. Alternatively, a publicly available static key for emergency access could be used. In the latter case, the device would need to be provisioned with the appropriate emergency key for the IAP/ISP in advance.

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

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

---

7. Security Considerations

TOC

The security threats discussed in [RFC5069] (Taylor, T., Tschofenig, H., Schulzrinne, H., and M. Shanmugam, “Security Threats and Requirements for Emergency Call Marking and Mapping,” January 2008.) are applicable to this document.

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

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

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

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

Finally, a number of security vulnerabilities discussed in [I-D.ietf-geopriv-arch] (Barnes, R., Lepinski, M., Cooper, A., Morris,

J., Tschofenig, H., and H. Schulzrinne, “An Architecture for Location and Location Privacy in Internet Applications,” October 2010.) around faked location information are less problematic in the context of unauthenticated emergency since location information does not need to be provided by the end host itself or it can be verified to fall within a specific geographical area.

---

8. Acknowledgments

TOC

Parts of this document are derived from [I-D.ietf-ecrit-phonebcp] (Rosen, B. and J. Polk, “Best Current Practice for Communications Services in support of Emergency Calling,” July 2010.). Participants of the 2nd and 3rd SDO Emergency Services Workshop provided helpful input.

---

9. IANA Considerations

TOC

This document does not require actions by IANA.

---

10. References

TOC

10.1. Normative References

TOC

[I-D.ietf-sipcore-location-conveyance]	Polk, J., Rosen, B., and J. Peterson, "Location Conveyance for the Session Initiation Protocol," draft-ietf-sipcore-location-conveyance-03 (work in progress), July 2010 (TXT).
[RFC5031]	Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services," RFC 5031, January 2008 (TXT).
[RFC4119]	Peterson, J., "A Presence-based GEOPRIV Location Object Format," RFC 4119, December 2005 (TXT).
[RFC5491]	Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations," RFC 5491, March 2009 (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).
[RFC3361]	Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers," RFC 3361, August 2002 (TXT).
[RFC3319]	Schulzrinne, H. and B. Volz, "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers," RFC 3319, July 2003 (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).
[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[I-D.ietf-ecrit-phonebcp]	Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling," draft-ietf-ecrit-phonebcp-15 (work in progress), July 2010 (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).

10.2. Informative References

TOC

[RFC5687]	Tschofenig, H. and H. Schulzrinne, “GEOPRIV Layer 7 Location Configuration Protocol: Problem Statement and Requirements,” RFC 5687, March 2010 (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-11 (work in progress), July 2010 (TXT).
[I-D.thomson-geopriv-res-gw-lis-discovery]	Thomson, M. and R. Bellis, “Location Information Server (LIS) Discovery using IP address and Reverse DNS,” draft-thomson-geopriv-res-gw-lis-discovery-04 (work in progress), September 2010 (TXT).
[RFC5985]	Barnes, M., “HTTP-Enabled Location Delivery (HELD),” RFC 5985, September 2010 (TXT).
[RFC5012]	Schulzrinne, H. and R. Marshall, “Requirements for Emergency Context Resolution with Internet Technologies,” RFC 5012, January 2008 (TXT).
[I-D.ietf-geopriv-held-identity-extensions]	Winterbottom, J., Thomson, M., Tschofenig, H., and R. Barnes, “Use of Device Identity in HTTP-Enabled Location Delivery (HELD),” draft-ietf-geopriv-held-identity-extensions-05 (work in progress), October 2010 (TXT).
[I-D.winterbottom-geopriv-lis2lis-req]	Winterbottom, J. and S. Norreys, “LIS to LIS Protocol Requirements,” draft-winterbottom-geopriv-lis2lis-req-01 (work in progress), November 2007 (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).
[I-D.ietf-geopriv-arch]	Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, “An Architecture for Location and Location Privacy in Internet Applications,” draft-ietf-geopriv-arch-03 (work in progress), October 2010 (TXT).
[esw07]	“3rd SDO Emergency Services Workshop, http://www.emergency-services-coordination.info/2007Nov/,” October 30th - November 1st 2007.
[nwgstg3]	“WiMAX Forum WMF-T33-001-R015V01, WiMAX Network Architecture Stage-3 http://www.wimaxforum.org/sites/wimaxforum.org/files/ technical_document/2009/09/DRAFT-T33-001-R015v01-O_Network-Stage3-Base.pdf,” September 2009.

Authors' Addresses

TOC

	Henning Schulzrinne
	Columbia University
	Department of Computer Science
	450 Computer Science Building
	New York, NY 10027
	US
Phone:	+1 212 939 7004
Email:	hgs+ecrit@cs.columbia.edu
URI:	http://www.cs.columbia.edu
	Stephen McCann
	Research in Motion UK Ltd
	200 Bath Road
	Slough, Berks SL1 3XE
	UK
Phone:	+44 1753 667099
Email:	smccann@rim.com
URI:	http://www.rim.com
	Gabor Bajko
	Nokia
Email:	Gabor.Bajko@nokia.com
	Hannes Tschofenig
	Nokia Siemens Networks
	Linnoitustie 6
	Espoo 02600
	Finland
Phone:	+358 (50) 4871445
Email:	Hannes.Tschofenig@gmx.net
URI:	http://www.tschofenig.priv.at
	Dirk Kroeselberg
	Nokia Siemens Networks
	St.-Martin-Str. 76
	Munich 81541
	Germany
Phone:	+49 (89) 515933019
Email:	Dirk.Kroeselberg@nsn.com