ECRIT
Internet-Draft
Intended status: Informational
Expires: January 3, 2008

H. Tschofenig
Nokia Siemens Networks
H. Schulzrinne
Columbia University

July 2, 2007

Emergency Services Architecture Overview: Sharing Responsibilities
draft-tschofenig-ecrit-architecture-overview-00.txt

Status of this Memo

Copyright Notice

Abstract

This document describes the IETF emergency services architectures and illustrates the architectural principles and responsibilities of different parties. For comparison, we also describe the emergency services architecture developed by 3GPP.

Table of Contents

1. Introduction

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

Existing emergency call systems are organized nationally; there are currently no international standards. However, the Internet does not respect national boundaries, and thus international standards are required. To further complicate matters, emergency services support needs to be added to a huge Internet where VoIP endpoints are subject to numerous access technologies and limitations, such as virtual private networks (VPNs), mobility protocols, firewalls, Network Address Translators (NATs), different IP versions including devices that translate from one to another version, different Voice over IP protocols, etc. In addition to these technical obstacles, different business models exist where a Voice Server Provider (VSP) or an Application Server Provider (ASP) are separate from the Internet Service Provider (ISP) and the Internet Attachment Provider (IAP).

This document describes the IETF emergency services architectures and illustrates the architectural principles and the responsibilities of different parties.

The 3GPP emergency services architecture, summarized in Appendix A, splits responsibilities somewhat differently.

2. Terminology

This document reuses terminology from [I-D.ietf-geopriv-l7-lcp-ps] and [I-D.ietf-ecrit-requirements]. To make this document self-contained we copy-and-paste the relevant terms into this section:

Internet Access Provider (IAP):

An organization that provides physical and data link (layer 2) network connectivity to its customers or users, e.g., through digital subscriber lines, cable TV plants, Ethernet, leased lines or radio frequencies. Examples of such organizations include telecommunication carriers, municipal utilities, larger enterprises with their own network infrastructure, and government

organizations such as the military.

Internet Service Provider (ISP):

An organization that provides IP network-layer services to its customers or users. This entity may or may not provide the physical-layer and data link (layer-2) connectivity, such as fiber or Ethernet, i.e., it may or may not play the role of an IAP.

Application Service Provider (ASP):

The organization or entity that provides application-layer services, which may include voice (see "Voice Service Provider"). This entity can be a private individual, an enterprise, a government, or a service provider. An ASP is more general than a Voice Service Provider, since emergency calls may use other media beyond voice, including text and video. For a particular user, the ASP may or may not be the same organization as his IAP or ISP.

Voice Service Provider (VSP):

A specific type of Application Service Provider which provides voice related services based on IP, such as call routing, a SIP URI, or PSTN termination. In this document, unless noted otherwise, any reference to "Voice Service Provider" or "VSP" may be used interchangeably with "Application/ Voice Service Provider" or "ASP/VSP".

Emergency Service Routing Proxy (ESRP):

An ESRP is an emergency call routing support entity that invokes the location-to-PSAP URI mapping function, to return an appropriate PSAP URI, or the URI for another ESRP. Client mapping requests could also be performed by a number of entities, including entities that instantiate the SIP proxy role and the SIP user agent client role.

Public Safety Answering Point (PSAP):

Physical location where emergency calls are received under the responsibility of a public authority. (This terminology is used by both ETSI, in ETSI SR 002 180, and NENA.) In the United Kingdom, PSAPs are called Operator Assistance Centres, in New Zealand, Communications Centres. Within this document, it is assumed, unless stated otherwise, that PSAPs support the receipt of emergency calls over IP, using appropriate application layer protocols such as SIP for call signaling and RTP for media.

Location Configuration Server (LCS):

The term LCS refers to an entity capable of determining the location of an end point and of providing that location information, a reference to it, or both) via the Location Configuration Protocol (LCP) to the requesting party, in most cases to the end point itself or to an entity that acts on behalf of it.

(Emergency) service dial string:

The service dial string identifies the string of digits that a caller must dial to reach a particular (emergency) service. In devices directly connected to the PSTN, the service dial string is the same as the service number and may thus depend on the location of the caller. However, in private phone networks, such as in PBXs, the service dial string consists of a dialing prefix to reach an outside line, followed by the emergency number. For example, in a hotel, the dial string for emergency services in the United States might be 9911. Dial strings may contain indications of pauses or wait-for-secondary- dial-tone indications.

(Emergency) service identifier:

The (emergency) service identifier describes the emergency service, independent of the user interface mechanism, the signaling protocol that is used to reach the service, or the caller's geographic location. It is a protocol constant and used within the mapping and signaling protocols. An example is the service URN [I-D.ietf-ecrit-service-urn].

For the purpose of this document we assume that the ISP and the IAP colaps into a single entity. We use the term ISP only. Furthermore, unless noted otherwise, any reference to "Voice Service Provider" or "VSP" may be used interchangeably with "Application/ Voice Service Provider" or "ASP/VSP".

3. The IETF Emergency Services Architecture

The emergency services architecture developed in the IETF Emergency Context Resolution with Internet Technology (ECRIT) working group, see [I-D.ietf-ecrit-framework], describes an architecture where location information is provided by the IAP/ISP to end points in order to determine the correct dial string and a Uniform Resource Identifier (URI) to route the call to a Public Safety Answering Point (PSAP) via the user's VoIP provider. The Location-to-Service Translation (LoST) protocol [I-D.ietf-ecrit-lost] allows to determine

the PSAP URI for a specific geographical location together with an emergency service identifier, see [I-D.ietf-ecrit-service-urn]. The basic architecture is shown in Figure 1. Detailed message flows are illustrated in Figure 2 of [I-D.ietf-ecrit-framework].

The obligations for the different parties are summarized below. An IETF draft [I-D.ietf-ecrit-phonebcp] describes these in much more detail, including callback capabilities, support for certain codecs, and SIP call handling behavior specific to emergency calls. The distributed mapping database may be operated by the ISP/IAP, the VSP, the PSAP operator, another independent entity or in parts by all these different entities. A description of the mapping architecture can be found in [I-D.ietf-ecrit-mapping-arch].

The obligations for the different parties are as follows:

End Host:

* An end host, through its VoIP applications, has three main responsibilities: it has to obtain its own location, determine the URI of the appropriate PSAP for that location, and recognize when the user places an emergency call by examining the dial string. The end host operating system may assist in determining the device location.

  The protocol interaction is shown as (A) in Figure 1. A number of protocols have been developed to provide this capability, as listed in Section 4.2 of [I-D.ietf-ecrit-phonebcp]. [I-D.ietf-ecrit-phonebcp] mandates support DHCP (see [RFC4776] and [RFC3825]), HELD (see [I-D.ietf-geopriv-http-location-delivery] and LLDP-MED (see [LLDP-MED]).

* A VoIP application needs to support the Location-to-Service Translation (LoST) protocol [I-D.ietf-ecrit-lost] in order to determine the emergency service dial strings and the PSAP URI. Additionally, the service identifiers, defined in [I-D.ietf-ecrit-service-urn], need to be understood by the device.

* In the current architecture, it is assumed that PSAPs can be reached by SIP and RTP, but may support other signaling protocols, either directly or through a protocol translation gateway. The LoST retrieval results indicate whether other VoIP signaling protocols are supported.

IAP/ISP:

* The IAP/ISP has to make location information available to the end point via one or more of the above-mentioned protocols, namely DHCP (see [RFC4776] and [RFC3825]), HELD (see [I-D.ietf-geopriv-http-location-delivery]) and LLDP-MED (see [LLDP-MED]).

Emergency services need location information for two different purposes, first for routing the emergency call to the PSAP that is serving a specific geographical region for the emergency service requested and to dispatch emergency personnel to the scene of the accident, crime or other type of incident. For the latter, the caller may be able to deliver this information orally, but it is generally agreed that emergency services protocols should deliver location information that is automatically generated, to increase accuracy and avoid dispatch delays when the caller is unable to provide location information due to language barriers, lack of familiarity with his or her surroundings or physical or mental impairment.

The accuracy requirements for these two uses differ. For call routing, city or county-level accuracy is often sufficient, while dispatch benefits greatly from having location that identifies a particular building or even room for indoor locations, or a radius of at most a few hundred feet for outdoor locations.

In some cases, Internet Access Providers (IAPs) and/or the Internet Service Providers (ISPs) are afraid that allowing users to access location information for non-emergency purposes or prior to an emergency call will incur additional server load and thus costs. Hence, they do not to disclose precise location information (at the quality suitable for dispatch emergency personnel by the PSAP operator) or not to disclose any location information. The impact for the IETF emergency services architecture to support this type of functionality, referred as 'location hiding', is currently under investigation (see [I-D.schulzrinne-location-hiding-requirements]. It should be noted that the concept of hiding location information refers to call routing only. ISPs have no interest or legal right to hide location information from emergency services personnel.

* The IAP/ISP may additionally operate a (caching) LoST server to improve the robustness and the reliability of the architecture.

* The IAP/ISP must allow signaling and media protocols used for emergency calls to traverse its network.

VSP:

* The IETF emergency services architecture does not require the participation of a VSP as such. However, if a caller uses a VSP, this VSP often forces all calls, emergency or not, to traverse an outbound proxy operated by the VSP. Also, at least initially, customer equipment may not be able to perform LoST lookups and thus needs to rely on the VSP to recognize emergency calls and route them to the correct PSAP.

* If the VSP uses a signaling or media protocol that is not natively supported by the PSAP, it needs to offer protocol translation and gateway services.

* VSPs can assist the PSAP by providing identity assurance for emergency callers that are their customers. Such identity assurance may assist with prosecuting prank callers. However, identity assurance can only be effective if the VSP can authenticate their customers, e.g., by having a verifiable customer postal address. (Verification by credit card usage fails when the credit card number has been stolen.)

PSAP:

* The IETF architecture does not standardize PSAP architecture and only describes those aspects in [I-D.ietf-ecrit-phonebcp] that are necessary for emergency calls to be processed by the PSAP. To make the overall architecture work, PSAPs must accept calls from any VSP/ASP in the world, as shown in protocol interaction (D) in Figure 1. Since calls may come from anywhere, PSAPs must develop mechanisms to reduce the number of prank calls, particularly calls with spoofed location information. [I-D.barnes-geopriv-lo-sec] discusses this problem. The PSAP operator can expect to receive civic or geodetic location information in the format known as PIDF-LO, specified in [RFC4119], revised for civic location information by [I-D.ietf-geopriv-revised-civic-lo]) and profiled for geodetic information in [I-D.ietf-geopriv-pdif-lo-profile]).

The distributed mapping database may be operated by the ISP/IAP, the VSP, the PSAP operator, another independent entity or in parts by all

these different entities. A description of the mapping architecture can be found in [I-D.ietf-ecrit-mapping-arch].

```
                  +---------------------------+
                  |                           |
                  | Emergency Network         |
                  | Infrastructure            |
                  |                           |
                  | +----------+ +----------+ |
                  | | PSAP     | | ESRP     | |
                  | |          | |          | |
                  | +----------+ +----------+ |
                  +-------------^-------------+   (D)
                                +----------------------+
                                                       |
   +--------------+                              +-----+--------+
   |              |              ----            |     |        |
   | ISP/IAP      |          ///-    -\\\        |     | VSP    |
   |              |         /            \\      |     |        |
   | +----------+ |        |  Distributed |      | +---+------+ |
   | | LCS      | |       |   Mapping      |     | | SIP      | |
   | |          | |       |   Database     |     | | Proxy    | |
   | +----------+ |        |              |      | +----------+ |
   |     ^        |         \            //      |     ^        |
   |     |        |          \\\-    -///        |     |        |
   |     |        |              ----            |     |        |
   +-----+--------+    (B)        ^              +-----+--------+
         |  +---------------------+                    |
      (A)|  |                                          |
         |  |  +---------------------------------------+
         |  |  |                    (C)
         v  v  v
     +----------+
     | End      |
     | Host     |
     +----------+
```

Figure 1: Overview of the IETF Emergency Services Architecture

4. Security Considerations

This document does not describe the security aspects of the two architectures. The protocol documents and the ECRIT security requirements [I-D.ietf-ecrit-security-threats] describe potential threats, and make protocol, implementation and operational recommendations to minimize these threats.

5. Acknowledgments

We would like to thank the ECRIT working group their work on the IETF ECRIT emergency services architecture. Additionally, we would like to thank the participants of various emergency services workshops, meetings and phone conferences for sharing their view with us.

The authors would particularly like to thank Alain Van Gaever from the European Commission for pushing us to write such a document.

Dirk Kroeselberg, Leopold Murhammer, Richard Barnes, and James Winterbottom provided us review comments for the pre-00 version.

6. Open Issues

Currently, the IETF emergency services architecture does not describe how to handle calls that are not authorized to access a network due to lack of proper credentials or that are not configured with a particular VSP.

There is currently no mechanism for prioritizing access to network resources for emergency calls, e.g., during mass casualty event.

7. References

7.1. Normative References

[I-D.ietf-ecrit-lost]
Hardie, T., "LoST: A Location-to-Service Translation Protocol", draft-ietf-ecrit-lost-05 (work in progress), March 2007.

[I-D.ietf-sip-location-conveyance]
Polk, J. and B. Rosen, "Session Initiation Protocol Location Conveyance", draft-ietf-sip-location-conveyance-07 (work in progress), February 2007.

[I-D.ietf-ecrit-service-urn]
Schulzrinne, H., "A Uniform Resource Name (URN) for Services", draft-ietf-ecrit-service-urn-06 (work in progress), March 2007.

[RFC4776] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", RFC 4776, November 2006.

[RFC3825] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", RFC 3825, July 2004.

[RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.

[I-D.ietf-geopriv-pdif-lo-profile]
Tschofenig, H., "GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations", draft-ietf-geopriv-pdif-lo-profile-07 (work in progress), April 2007.

[I-D.ietf-geopriv-revised-civic-lo]
Thomson, M. and J. Winterbottom, "Revised Civic Location Format for PIDF-LO", draft-ietf-geopriv-revised-civic-lo-05 (work in progress), February 2007.

[LLDP-MED]
, ., "ANSI/TIA-1057, Link Layer Discovery Protocol for Media Endpoint Devices (aka LLDP-MED)", April 2006.

7.2. Informative References

[I-D.ietf-geopriv-l7-lcp-ps]
Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements", draft-ietf-geopriv-l7-lcp-ps-02 (work in progress), April 2007.

[I-D.ietf-ecrit-framework]
Rosen, B., "Framework for Emergency Calling in Internet Multimedia", draft-ietf-ecrit-framework-01 (work in progress), March 2007.

[I-D.marshall-geopriv-lbyr-requirements]
Marshall, R., "Requirements for a Location-by-Reference Mechanism used in Location Configuration and Conveyance", draft-marshall-geopriv-lbyr-requirements-01 (work in progress), March 2007.

[I-D.ietf-geopriv-http-location-delivery]
Barnes, M., "HTTP Enabled Location Delivery (HELD)", draft-ietf-geopriv-http-location-delivery-00 (work in progress), June 2007.

[I-D.ietf-ecrit-mapping-arch]

Schulzrinne, H., "Location-to-URL Mapping Architecture and Framework", draft-ietf-ecrit-mapping-arch-01 (work in progress), December 2006.

[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-01 (work in progress), March 2007.

[I-D.ietf-ecrit-requirements]
Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", draft-ietf-ecrit-requirements-13 (work in progress), March 2007.

[I-D.ietf-ecrit-security-threats]
Taylor, T., "Security Threats and Requirements for Emergency Call Marking and Mapping", draft-ietf-ecrit-security-threats-04 (work in progress), April 2007.

[I-D.schulzrinne-location-hiding-requirements]
Schulzrinne, H., "Location Hiding: Problem Statement and Requirements", July 2007.

[I-D.barnes-geopriv-lo-sec]
Barnes, R., "GEOPRIV Security Requirements", July 2007.

[TS-24.229]
"TS 24.229, 3rd Generation Partnership Project; Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3, (Release 7)", June 2007.

[TS-23.167]
"TS 23.167, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions (Release 7)", June 2007.

Appendix A. The 3GPP Emergency Services Architecture

The description in this section re-uses terminology introduced in this document rather than using native 3GPP introduced terminology.

The basic idea of the 3GPP emergency services architecture, based on

[TS-24.229]/[TS-23.167], is shown in Figure 2 and is characterized by the difference that emergency services support is provided by the ISP/IAP (or a closely associated entity). This has the following consequences:

- o A SIP-based signaling profile needs to be standardized for interaction between the SIP UA and the SIP proxy in the ISP/IAP/ visited VSP/ASP. For the 3GPP emergency architecture IMS was chosen as the profile, i.e., a flavor of IETF SIP. This exchange is shown in (1).

- o The SIP proxy responsible for emergency call routing needs to determine location information of the end point. Since the SIP proxy and the location server are both located in the ISP/IAP (or in a closely associated entity) local information, such as IP addresses, cell identifiers, MAC addresses or similar identifiers are sufficient. Determining the address of the PSAP is also a local matter since there is a relationship between the ISP/IAP and the PSAP operator responsible for a specific geographic region. This exchange is shown in (2).

- o To provide identity information for the emergency call to the PSAP operator it is necessary to interact with the user's home VSP/ASP (in the roaming case). This is shown with the message interaction in (3).

- o The interaction between the ISP/IAP/visited VSP/ASP and the PSAP operator is a national matter and is currently not specified.

The obligations for the different parties are as follows:
End Host:

  * The end host needs to support the IMS-specific SIP profile. The detailed steps are described in Section 6.1 of [TS-23.167]. End hosts that do not support this specific version of SIP (including the specific authentication mechanisms) cannot be supported.

  * PIDF-LO [RFC4119] may need to be supported to allow the end host to attach GPS available location information. Other location protocols, such as the Secure User Plane Location protocol (SUPL), may be needed in special cases. See Section 7.6 of [TS-23.167] for a detailed considerations on how to retrieve location information.

ISP/IAP/visited VSP/ASP:

* The SIP proxy in the access network needs to understand the IMS-specific SIP profile and the protocols used for (2), (3) and (4), whereby (4) is not specified. The detailed steps are described in Section 6.2.1, Section 6.2.2, 6.2.3 of [TS-23.167]. On a high-level basis, the responsibility is mainly to understand the SIP protocol (and the corresponding extensions), to determine the end host's location information, to perform the necessary interaction for verifying the emergency caller's identity via the interaction with the home VSP and finally to route the emergency call to the correct PSAP.

Home VSP/ASP:

* The home VSP/ASP needs to provide SIP call back functionality and asserts the identity of the emergency caller. A roaming agreement is assumed to be in place between the home and the visted VSP/ASP. Note that the security mechanism used to authenticate the end host to the Home VSP needs to prevent the visited VSP from being able to later impersonate the user. Note that this authentication procedure is likely be done during the network access authentication procedure rather than during the SIP signaling exchange.

PSAP:

* This protocol interaction is not specified but assumed to be based on SIP.

```
              +---------------------------+
              |                           |
              | Emergency Network         |
              | Infrastructure            |
              |                           |
              | +----------+ +----------+ |
              | | PSAP     | | ESRP     | |
              | |          | |          | |
              | +----------+ +----------+ |
              +-------------^-------------+
                            |
                            | (4)
   +------------------------+-------+       +-----------------------+
   | ISP/IAP                |       |       | Home VSP/ASP          |
   | Visited VSP/ASP        |       |       |                       |
   |+----------+            v       |       |    +----------+       |
   || LCS      |  (2)  +----------+ |   (3) |    | Identity |       |
   ||          |<--+-->| ESRP /   |<+-----+-+--->| Provider |       |
   |+----------+   |   | SIP Proxy| |     | |    +----------+       |
   |+----------+   |   +----------+ |     | |    +----------+       |
   || Mapping  |<--+        ^       |     | |    | SIP      |       |
   || Database |            |       |     +-+--->| Proxy    |       |
   |+----------+            |       |       |    +----------+       |
   +------------------------+-------+       +-----------------------+
                            |
                            | (1)
                            |
                            |
                            v
                       +----------+
                       | End      |
                       | Host     |
                       +----------+
```

Figure 2: Overview of the 3GPP Emergency Services Architecture

Authors' Addresses

Hannes Tschofenig
Nokia Siemens Networks
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: Hannes.Tschofenig@nsn.com
URI: http://www.tschofenig.com

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

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).