Deploying IP-based Emergency Services

Internet Architecture Board

Abstract

The IETF ECRIT and GEOPRIV working groups have developed standards for critical components of the next-generation, IP-based 911 system. This whitepaper reviews some of the basic principles of these technologies and explains how to incrementally deploy the architecture to take into account currently deployed emergency services systems.

1 Introduction

The ability to summon the police, the fire department or an ambulance in emergencies is one of the most important functions available when using the telephone. As telephone functionality moves from circuit-switched to Internet telephony, its users rightfully expect that this core feature will continue to be available and work as well as it has in the past. Users also expect to be able to reach emergency assistance using new communication devices and applications, such as instant messaging or SMS, and new media, such as video. In all cases, the basic objective is the same: The person seeking help needs to be connected with the most appropriate public safety answering point (PSAP), where call takers dispatch assistance to the caller's location. PSAPs are responsible for a particular geographic region, which can be as small as a single university campus or as large as a country.

The transition to Internet-based emergency services introduces two major structural challenges. First, while traditional emergency calling imposed no requirements on end systems and was regulated at the national level, Internet-based emergency calling needs global standards, particularly for end systems. In the old public switched telephone network (PSTN), each caller used a single entity, the landline or mobile carrier, to obtain services. For Internet multimedia services, network level transport and application can be separated, with the Internet service provider (ISP) providing IP connectivity service, and a voice service provider (VSP) adding call routing and PSTN termination services. We ignore the potential separation between the Internet access provider, i.e., a carrier that provides physical and data link layer network connectivity to its customers, and the ISP that provides network layer services. We use the term VSP for simplicity, instead of the more generic term Application Server Provider (ASP).

The documents that are being developed within the IETF Emergency Context Resolution with Internet Technology (ECRIT) working group [1] support multimedia-based emergency services, and not just voice. As will be explained in more detail below, emergency calls need to be identified for special call routing and handling services, and they need to carry the location of the caller for routing and dispatch. Only the calling device can reliably recognize emergency calls, while the ISP is a reliable source of location information of the calling device based on its point of attachment to the network. Handling of emergency calls is, however, complicated by the wide variety of access technologies in use, such as virtual private networks (VPNs), other forms of tunneling, firewalls, and Network Address Translators (NATs).

The emergency services architecture developed by the IETF ECRIT working

group is described in [15] and can be summarized as emergency calls are generally handled like regular multimedia calls, except for call routing. The ECRIT architecture assumes that PSAPs are connected to an IP network and support the Session Initiation Protocol (SIP) [16] for call setup and messaging. However, the calling user agent may use any call signaling or instant messaging protocol, which the VSP then translates into SIP.

Non-emergency calls are routed by a VSP, either to another subscriber of the VSP, typically via some SIP session border controller or proxy, or a PSTN gateway. For emergency calls, the VSP keeps its call routing role, routing calls to the emergency service system, to reach a PSAP, instead. However, we also want to allow callers that do not subscribe to a VSP to reach a PSAP, using nothing but a standard SIP [16] user agent (see [22] for a discussion about this topic); the same mechanisms described here apply. Since the Internet is global, it is possible that a caller's VSP resides in a jurisdiction other than where the caller and the PSAP are located. In such circumstances it may be desirable to exclude the VSP and provide a direct signaling path between the caller and the emergency network. This has the advantage of ensuring that all parties included in the call delivery process reside in the same regulatory jurisdiction.

As noted in the introduction, the architecture does not force or assume any type of trust or business relationship between the ISP and the VSP carrying the emergency call. In particular, this design assumption affects how location is derived and transported.

Providing emergency services requires three crucial steps, which we summarize in turn below: recognizing an emergency call, determining the caller's location, and routing the call and location information to the appropriate emergency service system operating a PSAP.

1.1 Recognizing Emergency Calls

Many countries support more than one emergency service number. Consequently, devices have to support a large number of emergency numbers world-wide. Because of this diversity, the ECRIT architecture decided to separate the concept of an emergency dial string, which remains the familiar and regionally-defined emergency number, and a protocol identifier that is used for identifying emergency calls within the signaling system. The calling end system has to recognize the emergency (service) dial string and to translate it into an emergency service identifier, which is an extensible set of Uniform Resource Names (URNs) defined in RFC 5031 [19]. A common example for such a URN, defined to reach the

generic emergency service, is urn:service.sos. The emergency service URN is included in the signaling request as the destination and is used to identify the call as an emergency call. If the end system fails to recognize the emergency dial string, the VSP may also perform this service.

Since mobile devices may be sold and used world wide, we want to avoid manually configuring emergency dial strings. In general, a device should recognize the emergency dial string familiar to the user and the dial strings customarily used in the currently visited country. The Location-to-Service Translation Protocol (LoST) [4], described in more detail later, also delivers this information.

1.2 Obtaining and Conveying Location Information

In the IETF emergency services architecture, location information can be conveyed in SIP either by value ("LbyV") or by reference ("LbyR"). For the former, the XML location object is added as a message body in the SIP message.

When passed as a value then location is encapsulated within the Presence Information Data Format Location Object (PIDF-LO), an XML-based document to encapsulate civic and geodetic location information. The format of PIDF-LO is described in [8] with the civic location format updated in [25] and the geodetic location format profiled in [28]. The latter document uses the Geography Markup Language (GML) developed by the Open Geospatial Consortium (OGC) for describing commonly utilized location shapes. More information about the standardization efforts on location can be found in Chapter **??**.

Location by value is particularly appropriate if the end system has access to the location information, e.g., if it contains a Global Positioning System (GPS) receiver or uses one of the location configuration mechanisms described below. In environments where the end host location changes frequently, the LbyR mechanism might be more appropriate. In this case, the LbyR is an HTTP/HTTPS or SIP/SIPS URI, which the recipient needs to resolve to obtain the current location. Terminology and requirements for the LbyR mechanism are available with [7].

An LbyV and an LbyR can be obtained via location configuration protocols, such as the HELD protocol [2] or DHCP [10, 18, 9]. Once obtained, location information is required for LoST queries, and is added to SIP messages [11].

The ISP is the source of the most accurate and dependable location information. It is, however, not the only source. A calling device may have built-in location capabilities, such as GPS, producing highly accurate location information. For landline Internet connections such as DSL, cable or fiber-to-the-home, the ISP knows the provisioned location for the network termination, for example. The

IETF Geographic Location/Privacy (GEOPRIV) working group has developed protocol mechanisms, called location configuration protocols, so that the end host can request and receive location information from the ISP. The best current practice document for emergency calling [14] enumerates three options that should be universally supported by clients: DHCP civic [18] and geo [10], and HELD [2]. HELD uses XML query and response objects carried in HTTP exchanges. DHCP does not use the PIDF-LO format, but rather more compact binary representations of locations that require the end-point to construct the PIDF-LO.

Particularly for cases where end systems are not location-capable, a VSP may need to obtain location information on behalf of the end host [29].

Obtaining at least rough location information at the time of the call is time-critical, as the LoST query can only be initiated once the calling device or VSP has obtained location information. Also, to speed up response, it is desirable to transmit this location information with the initial call signaling message. In some cases, however, location information at call setup time is imprecise. For example, a mobile device typically needs 15 to 20 seconds to get an accurate GPS location "fix" and the initial location report is based on the cell tower and sector. For such calls, the PSAP should be able to request more accurate location information either from the mobile device directly or the Location Information Server (LIS) operated by the ISP. The SIP event notification extension, defined in RFC 3265 [12], is one such mechanism that allows a PSAP to obtain the location from an LIS. To ensure that the PSAP is only informed of pertinent location changes, and that the number of notifications is kept to a minimum, event filters [6] can be used.

The two-stage location refinement mechanism described above works best when location is provided by reference (LbyR) in the SIP INVITE call setup request. The PSAP subscribes to the LbyR provided in the SIP exchange and the LbyR refers to the LIS in the ISPs network. In addition to a SIP URI, the LbyR message can also contain an HTTP/ HTTPS URI. When such a URI is provided, an HTTP-based protocol can be used to retrieve the current location [30].

1.3 Routing Emergency Calls

In limited scenarios, where the VSP and the ISP role are offered by the same provider routing of IP-based emergency calls can be based on statically pre-configured rules. However, the separation of these two roles to separate companies introduces challenges for emergency call routing. In addition, emergency services authorities are interested to use IP and SIP-based functionality to route calls more dy-

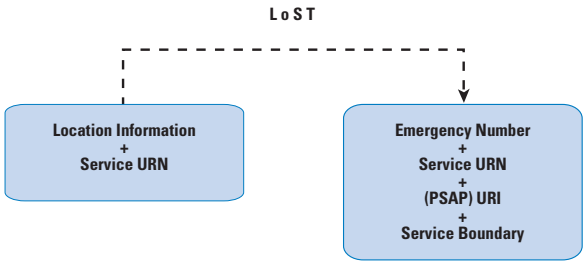

Figure 1: High-Level Functionality of Location-to-Service Translation (LoST).

namically. To decouple the routing enforcement point from the decision point an automated procedure has been standardized. Two mechanisms are available: the service boundary exchange mechanisms [24] and the Location to Service Translation (LoST) protocol [4]. [24] has limited applicability for exchange of service boundaries between trusted entities and LoST may make use of [24] for distributing mappings. LoST is a generic mechanism that maps a location and a service URN to a specific PSAP URI and a service region. LoST, illustrated in Figure 1, is an HTTP-based query/response protocol where a client sends a request containing the location information and service URN to a server and receives a response, containing the service URL, typically a SIP URL, the service region where the same information would be returned and an indication of how long the information is valid. Both request and response are formatted as XML. For efficiency, responses are cached, as otherwise every small movement would trigger a new LoST request. As long as the client remains in the same service region, it does not need to consult the server again until the response returned reaches its expiration date. The response may also indicate that only a more generic emergency service is offered for this region. For example, a request for 'urn:service:sos.marine' in Austria may be replaced by 'urn:service:sos'. Finally, the response also indicates the emergency number / dial string for the respective service.

1.4 Obligations

In this section we discuss the requirements the different entities need to satisfy, based on Figure 2. A more detailed description can be found in [14]. Note that this narration focuses on the final stage of deployment and does not discuss the transition architecture, in which some implementation responsibilities can be rearranged, with an impact on the overall functionality offered by the emergency services architecture. A few variations were introduced to handle the transition

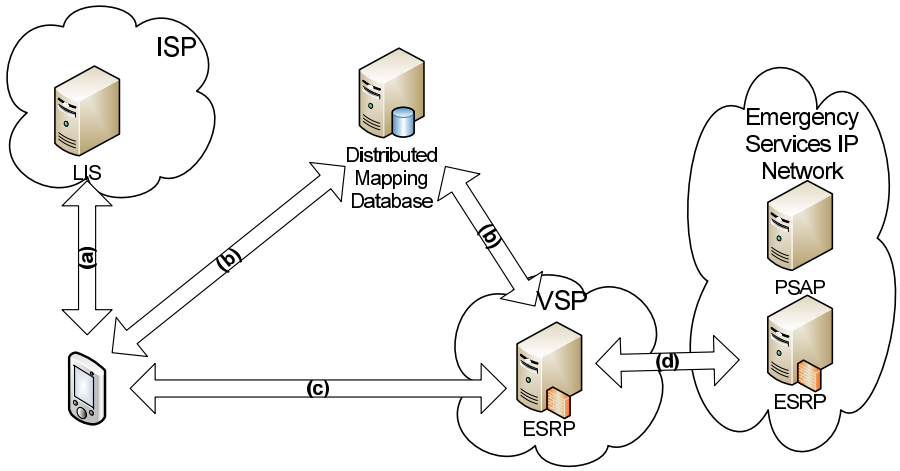

Figure 2: Main Components involved in an Emergency Call.

from the current system to a fully developed ECRIT architecture.

With the work on the IETF emergency architecture we have tried to balance the responsibilities among the participants, as described below.

1.4.1 End Hosts

An end host, through its VoIP application, has three main responsibilities: it has to attempt 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 for location configuration is indicated as interface (a) in Figure 2 and a number of location configuration protocols have been developed to provide this capability.

A VoIP application needs to support the Location-to-Service Translation (LoST) protocol [4] in order to determine the emergency service dial strings and the PSAP URI. Additionally, the service URNs, defined in [19], need to be understood by the device.

As currently defined, it is assumed that PSAPs can be reached by SIP, but may support other signaling protocols, either directly or through a protocol translation gateway. The LoST retrieval results indicate whether other signaling protocols are

supported. To provide support for multi-media different types of codecs may need to be supported; details can be found in [14].

1.4.2 ISP

The ISP has to make location information available to the end point via one or more of the location configuration protocols.

In order to route an emergency call correctly to a PSAP, an ISP may initially disclose the approximate location for routing to the end point and more precise location information later, when emergency personnel is dispatched by the PSAP operator. The functionality required by the IETF emergency services architecture is restricted to the disclosure of a relatively small amount of location information, as discussed in [21] and in [3].

The ISP may also operate a caching LoST server to improve the robustness and the reliability of the architecture. This lowers the roundtrip time for contacting a LoST server, and the caches are most likely to hold the mappings of the area where the emergency caller is currently located.

In the case where ISPs allow Internet traffic to traverse their network, the signaling and media protocols used for emergency calls function without problems. Today, there are no legal requirements to offer prioritization of emergency calls over IP-based networks. While the standardization community has developed a range of Quality of Service signaling protocols, their widespread deployment still remains to happen.

1.4.3 VSP

SIP does not mandate that call setup requests traverse SIP proxies, i.e., SIP messages can be sent directly to the user agent. Thus, even for emergency services, it is possible to use SIP without the involvement of a VSP. However, in terms of deployment, it is highly likely that a VSP will be used. If a caller uses a VSP, this VSP often forces all calls, emergency or not, to traverse an outbound proxy or session border controller (SBC) operated by the VSP. If some end devices are unable to perform a LoST lookup, VSP can provide the necessary functions as a back-up solution.

If the VSP uses a signaling or media protocol that is not supported by the PSAP, it needs to translate the signaling or media flows.

VSPs can assist the PSAP by providing identity assurance for emergency calls, e.g., using SIP Identity (RFC 3325 [5]), thus helping to prosecute prank callers. However, the link between the subscriber information and the real-world person making the call is weak. In many cases, VSPs have, at best, only the credit card data for their customers and some of these customers may use gift cards or other anonymous means of payment.

1.4.4 PSAP

The emergency services best current practice document [14] only discusses the standardization of the interfaces from the VSP and ISP towards PSAPs and some parts of the PSAP-to-PSAP call transfer mechanisms that are necessary for emergency calls to be processed by the PSAP. Many aspects related to the internal communication within a PSAP, between PSAPs as well as between a PSAP and first responders are beyond the scope of the IETF specification.

When emergency calling has been fully converted to Internet protocols, PSAPs must accept calls from any VSP, as shown in interface (d) of Figure 1. Since calls may come from all sources, PSAPs must develop mechanisms to reduce the number of malicious calls, particularly calls containing intentionally false location information. Assuring the reliability of location information remains challenging, particularly as more and more devices are equipped Global Navigation Satellite Systems (GNSS) receivers, such as GPS, allowing them to determine their own location [27]. However, it may be possible in some cases to verify the location information provided by an end-point by comparing it against network-provided location information.

1.5 LoST Mapping Architecture

So far, we have described the LoST protocol as it is described in RFC 5222 [4], namely as a client-server protocol. A single LoST server, however, does not store the mapping elements for all PSAPs worldwide, for both technical and administrative reasons. Thus, there is a need to let LoST servers interact with other LoST servers, each covering a specific geographical region. The LoST protocol already provides the baseline mechanisms for supporting such a communication architecture, as described in RFC 5582 [20], an informational RFC providing terminology (in the form of different roles for LoST servers that distinguish their behavior) and explaining the basic concept of the LoST mapping architecture. RFC

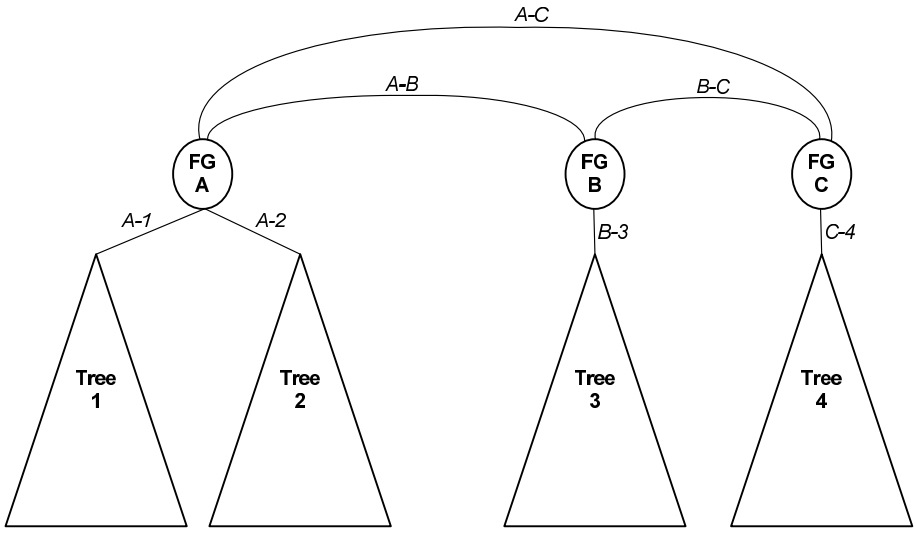

Figure 3: Trees and Forest Guides in the LoST Mapping Architecture.

5582 motivates the basic design decision for LoST to utilize it in a wide variety of architectures, but leaves the detailed instantiation to deployments in different jurisdictions.

The awareness of peering LoST servers determines the structure of the architecture rather than certain physical properties of a network, such as topology of a fiber installation, or the structure of a national emergency services organization. Two types of structures are used in combination, namely a mesh and a hierarchical structure. The mesh topology is envisioned for the top-level LoST entities, whereas the hierarchical structure reflects a parent - child relationship in a tree. Figure 3 shows this structure graphically with the LoST servers acting in their roles of forest guides (FGs) and trees. A tree consists of a self-contained hierarchy of authoritative mapping servers (AMS) for a particular service. An AMS is a LoST server that can provide the authoritative answer to a particular set of queries. The top-most server in a tree is a tree root and this server peers with one or multiple FGs, i.e., the tree root announces its coverage region to FGs. In Figure 3, for example, the root of tree 1 interacts with FG A and makes the coverage area available. FG A also receives the coverage area from the root of tree 2. All tree roots receive information about the coverage area of their children in the tree. On the top level, all FGs (namely FG A, FG B, and FG C) form a mesh and synchronize their coverage areas.

Seekers and resolvers are two additional LoST entities in the LoST mapping

architecture that are not shown in Figure 3. Neither seekers nor resolvers provide authoritative answers themselves but they may cache results. Particularly the use of resolvers to cache mapping elements is expected to be very common.

To best understand the LoST mapping architecture it is important to highlight the main design goals:

Robustness: To ensure the stability of the system even if different people in different places of the LoST architecture make different decisions, the system will still function. It cannot be assumed that everyone has to agree with everyone else. The minimum level of agreement that has to be ensured is that AMSs are able to authoritatively answer mapping queries, i.e., only those LoST servers respond authoritatively if they indeed have the authority of a specific coverage area.

Consistent Responses: Any device (called seeker) can issue a LoST query and it will get a consistent answer regardless of where the query enters the system. In some (rare) cases of territorial disputes, two AMSs may claim authoritative for the same region. In such a case, the answer received by a seeker will vary depending on the entry point into the mapping system.

Scalability: Scalability of the LoST architecture is ensured by the use of caching and the distributed nature of the LoST servers in the architecture. Any LoST entity may support caching of received mapping elements. The mapping elements may be obtained as part of the ordinary operation of LoST (via query and responses) but also via separate replication of the mapping elements. LoST Sync [24] is one such protocol to exchange mappings between LoST servers (and other entities).

Minimal Seeker Configuration: A seeker is a LoST client requesting a mapping. The only information a seeker needs to know is the address of a resolver; it does not need to know the structure of all Forest Guides nor does it need to maintain a global picture of LoST servers. To avoid having end user involvement in the configuration of LoST servers, Section 4 of the LoST specification provides a discovery technique based on DNS, and RFC 5223 [23] offers a DHCP-based discovery procedure. Although LoST servers can be located anywhere, a placement topologically closer to the end host, e.g., in the access network, may be desirable in disaster situations with intermittent network connectivity. RFC 5223 offers this capability.

Even though it is technically possible to let seekers and resolvers enter their queries at any point in the LoST mapping architecture, a deployment choice is to configure resolvers with the addresses of the FGs. A query and response for an emergency caller located in Germany with a service provider in Finland could then be shown as depicted in Figure 4. In our example we assume that the VSP deploys a LoST resolver that is contacted by the their own customers, the seekers. We furthermore assume in this example that no caching takes place to illustrate the message flow (as shown with dotted lines). In message (1) the seeker contacts its pre-configured resolver with a recursive query providing its current location (somewhere in Germany). The resolver at this point in time does not have any information about the PSAP that has to be contacted for the given location in Germany (for the solicited service). Since the resolver knows the address of the forest guide (only one forest guide is shown in our example), it issues an iterative query to it, as marked with message (2). The FG responds with the entry point for the German LoST tree. The resolver then issues another query towards the provided tree root in message (3). For this example we assume that the root of tree 1 knows the address of the PSAP the seeker has to contact. This final response is then forwarded to seeker via the resolver. The resolver would want to cache the intermediate and final results in order to speed-up later lookups for the same geographical area and the same service. Once the seeker knows the final answer, it can proceed with the emergency call setup procedure to contact the PSAP, as shown in message (4) with the double line.

As illustrated, LoST servers form a distributed mapping database, with each server carrying mapping elements. These mapping elements are the main data structure that is communicated in the LoST protocol, synchronized between FGs and LoST servers in the tree, and cached by resolvers and seekers. Figure 5 shows the data elements of this important data structure graphically.

1.6 Steps towards an IETF Emergency Services Architecture

The architecture described so far requires changes both in already-deployed VoIP end systems and in the existing PSAPs. The speed of transition and the path taken varies between different countries depending on funding and business incentives. As such, it is difficult to argue whether upgrading end points will be easier or replacing the emergency service infrastructure. In any case, the transition approaches being investigated consider both directions. We can distinguish roughly four stages of transition; the description below omits many of the details due to space constraints:

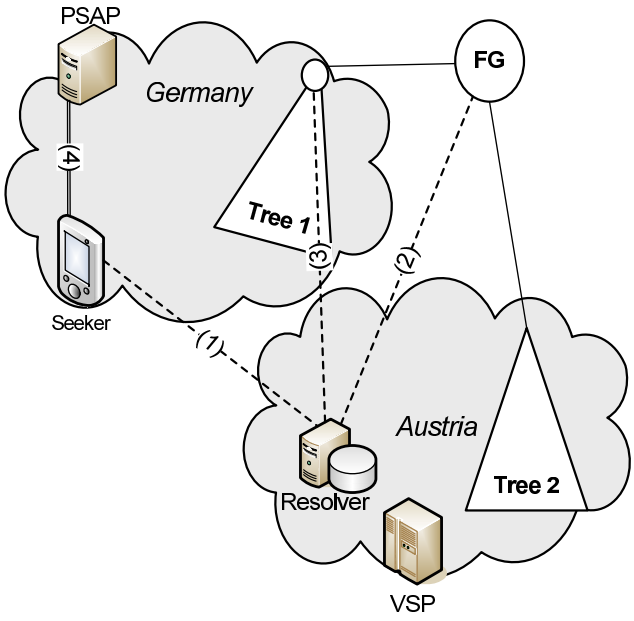

Figure 4: Example Query / Response in the LoST Mapping Architecture.

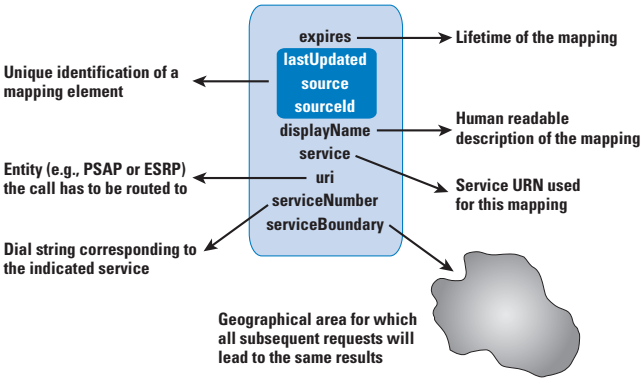

Figure 5: Mapping Element.

- Initially, VoIP end systems cannot place emergency calls at all. This is currently the case for many software clients, such as GoogleTalk.
- In a second stage, VoIP callers manually configure their location, and emergency calls are routed to the appropriate PSAP as circuit-switched calls via PSTN gateways, using technologies similar to mobile calls. This level of service is now offered in some countries for PSTN-replacement VoIP ser-

vices, i.e., VoIP services that are offered as replacement for the home phone. In the United States, this is known as the ”NENA i2” service.

- In a third stage, PSAPs maintain two separate infrastructures, one for calls arriving via an IP network, and the legacy infrastructure.
- In the final stage, all calls, including those from traditional cell phones and analog landline phones, reach the PSAP via IP networks, with the legacy calls converted to the ECRIT requirements by the carriers or the emergency service infrastructure.

1.6.1 Legacy End Points

Figure 5 shows an emergency services architecture with legacy end points. When the emergency caller dials the European-wide emergency number ’112’ (step 0), the device treats it as any other call without recognizing it as an emergency call, i.e., the dial string provided by the end point that may conform to RFC 4967 [13] or RFC 3966 [17] is signaled to the VSP (step 1). Recognition of the dial string is then left to the VSP for processing/sorting; the same is true for location retrieval (step 2) and routing to the nearest (or appropriate) PSAP (step 3). Dial string recognition, location determination and call routing are simpler on a fixed device and voice / application service provided only by the ISP than when they are provided via separate a VSP and ISP.

If devices are used in environments without location services, the VSP’s SIP proxy may need to insert location information based on estimates or subscriber data. We briefly describe these cases below.

There are two main challenges to overcome when dealing with legacy devices: First, the VSP has to discover the LIS that knows the location of the IP-based end host. The VSP is only likely to know the IP address of that device, which is visible in the call signaling that arrives at the VSP. When a LIS is discovered and contacted, and some amount of location information is available, then the second challenge arises, namely how to route the emergency call to the appropriate PSAP. To accomplish the latter task, it is necessary to have some information about the PSAP boundaries.

[14] does not describe a complete solution for interworking with legacy PSAPs but instead offers building blocks to use. The following constraints exist when dealing with legacy end points:

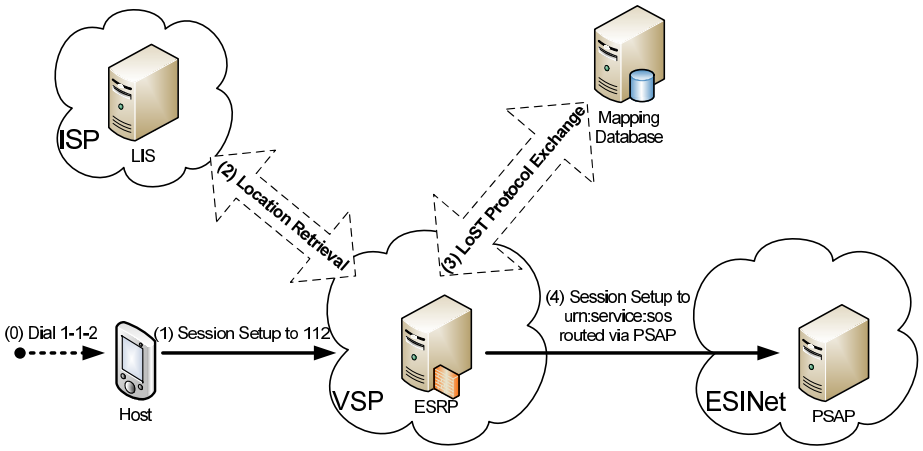

Figure 6: Emergency Services Architecture with Legacy End Points.

- Only the emergency numbers configured at the VSP are understood. This may lead to cases where a dialed emergency number is not recognized or a non-emergency call is routed to a PSAP.
- Using the host's IP address to discover the ISP network to which the host is attached is challenging and may, in case of mobility protocols and VPNs, lead to wrong results.
- Security and privacy concerns may arise when a large number of VSPs/ASPs can retrieve location information from an ISP. It is likely that only authorized VSP/ASPs will be granted access. Hence, it is unlikely that such a solution would work smoothly across national boundaries.
- When the emergency call is not recognized by the User Agent, then functions like call waiting, call transfer, three way call, flash hold, outbound call blocking, etc. cannot be disabled.
- The User Agent software may block callbacks from the PSAP since it does not have ways to recognize those as calls related to an earlier emergency.
- Privacy settings may not be respected and identity information may get disclosed to unauthorized parties. These identity privacy features exist in some jurisdiction even in emergency situations.

- Certain VoIP call features may not be supported, such as a REFER (for conference call and transfer to secondary PSAP) or the Globally Routable User Agent URIs (GRUU) for identifying individual devices issuing the emergency call.
- User Agents will not be able to convey location information to the VSP (even if it is available).

1.6.2 Partially Upgraded End Hosts

A giant step forward in simplifying the handling of IP-based emergency calls is to provide the end host with some information about the ISP so that LIS discovery is possible. The end host may, for example, learn the ISP's domain name, by using LIS discovery [26], or might even obtain a Location by Reference (LbyR) via the DHCP-URI option [9] or via HELD [2]. The VSP is then either able to resolve the LbyR in order to route the call or to use the domain to discover a LIS using DNS.

Additional software upgrades at the end device may allow emergency calls to be recognized based on some pre-configured emergency numbers (e.g., '1-1-2' and '9-1-1') and allow for the implementation of other emergency service-related features, such as disabling silence suppression during emergency calls.

1.7 Outlook

Regulation for IP-based emergency services is still at an early stage in most countries. The ability to obtain location information of IP devices automatically is not a requirements in most networks. Automatically obtaining location information is crucial for reliable emergency service operation to support nomadic[1] and mobile devices.

Regulators have traditionally focused on the national or, at most, the European level, and the international nature of the Internet poses new challenges. For example, mobile devices are now routinely used beyond their country of purchase and, unlike traditional cellular phones, need to support emergency calling functionality. It appears likely that different countries will deploy IP-based emergency

[1]Nomadic devices remain in one place during a communication session, but are moved frequently from place top place. Laptops with WiFi interfaces are currently the most common nomadic device.

services over different time horizons, so that a traveler may be surprised to find that she cannot call for emergency assistance outside their home country.

The separation between Internet access and application providers on the Internet is one of the most important differences to existing circuit switched telephony networks. A side effect of this separation is the increased speed of innovation at the application layer, and the number of new communication mechanisms is steadily increasing. Many emergency service organizations have recognized this trend and advocate for the use of new communication mechanisms, including video, real-time text, and instant messaging, to offer improved emergency calling support for citizens. Again, this requires regulators to re-think the distribution of responsibilities, funding and liability.

For many communication systems in use today it is difficult to trace malicious activities back to the human who caused them since identity proofing requirements are often fairly low when registering with Internet application services. This is not a completely new problem, as pay phones and prepaid cell phones have long offered mischief makers the opportunity to place hoax calls, but the weak user registration procedures, the lack of deployed end-to-end identity mechanisms, and the ease of providing false location information increases the attack surface at PSAPs. Attackers also have become more sophisticated over time, and using botnets to generate a large volume of automated emergency calls to exhaust PSAP resources, including call takers and first responders, is not science fiction.

References

[1] *IETF Emergency Context Resolution with Internet Technologies (ecrit) Working Group*. URL: `http://datatracker.ietf.org/wg/ecrit/charter/`.

[2] M. Barnes. *HTTP-Enabled Location Delivery (HELD)*, September 2010. RFC 5985, Internet Engineering Task Force.

[3] R. Barnes and M. Lepinski. *Using Imprecise Location for Emergency Context Resolution*, July 2012. draft-ietf-ecrit-rough-loc-05 (work in progress), Internet Engineering Task Force.

[4] T. Hardie, A. Newton, H. Schulzrinne, and H. Tschofenig. *LoST: A Location-to-Service Translation Protocol*, August 2008. RFC 5222, Internet Engineering Task Force.

[5] C. Jennings, J. Peterson, and M. Watson. *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*, November 2002. RFC 3325, Internet Engineering Task Force.

[6] R. Mahy, B. Rosen, and H. Tschofenig. *Filtering Location Notifications in the Session Initiation Protocol (SIP)*, January 2012. RFC 6447, Internet Engineering Task Force.

[7] R. Marshall. *Requirements for a Location-by-Reference Mechanism*, May 2010. RFC 5808, Internet Engineering Task Force.

[8] J. Peterson. *A Presence-based GEOPRIV Location Object Format*, December 2005. RFC 4119, Internet Engineering Task Force.

[9] J. Polk. *Dynamic Host Configuration Protocol (DHCP) IPv4 and IPv6 Option for a Location Uniform Resource Identifier (URI)*, May 2012. draft-ietf-geopriv-dhcp-lbyr-uri-option-15 (work in progress), Internet Engineering Task Force.

[10] J. Polk, M. Linsner, M. Thomson, and B. Aboba. *Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information*, July 2011. RFC 6225, Internet Engineering Task Force.

[11] J. Polk and B. Rosen. *Location Conveyance for the Session Initiation Protocol*, December 2011. RFC 6442, Internet Engineering Task Force.

[12] A. Roach. *Session Initiation Protocol (SIP)-Specific Event Notification*, June 2002. RFC 3265, Internet Engineering Task Force.

[13] B. Rosen. *Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier*, July 2007. RFC 4967 (Proposed Standard).

[14] B. Rosen and J. Polk. *Best Current Practice for Communications Services in support of Emergency Calling*, September 2011. draft-ietf-ecrit-phonebcp-20 (work in progress), Internet Engineering Task Force.

[15] B. Rosen, H. Schulzrinne, J. Polk, and A. Newton. *Framework for Emergency Calling Using Internet Multimedia*, December 2011. RFC 6443, Internet Engineering Task Force.

[16] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. *SIP: Session Initiation Protocol*, June 2002. RFC 3261, Internet Engineering Task Force.

[17] H. Schulzrinne. *The tel URI for Telephone Numbers*, December 2004. RFC 3966, Internet Engineering Task Force.

[18] H. Schulzrinne. *Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information*, November 2006. RFC 4776, Internet Engineering Task Force.

[19] H. Schulzrinne. *A Uniform Resource Name (URN) for Emergency and Other Well-Known Services*, January 2008. RFC 5031, Internet Engineering Task Force.

[20] H. Schulzrinne. *Location-to-URL Mapping Architecture and Framework*, September 2009. RFC 5582, Internet Engineering Task Force.

[21] H. Schulzrinne, L. Liess, H. Tschofenig, B. Stark, and A. Kuett. *Location Hiding: Problem Statement and Requirements*, January 2012. RFC 6444, Internet Engineering Task Force.

[22] H. Schulzrinne, S. McCann, G. Bajko, H. Tschofenig, and D. Kroeselberg. *Extensions to the Emergency Services Architecture for dealing with Unauthenticated and Unauthorized Devices*, September 2012. draft-ietf-ecrit-unauthenticated-access-05 (work in progress), Internet Engineering Task Force.

[23] H. Schulzrinne, J. Polk, and H. Tschofenig. *Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)*, August 2008. RFC 5223, Internet Engineering Task Force.

[24] H. Schulzrinne and H. Tschofenig. *Synchronizing Location-to-Service Translation (LoST) Protocol based Service Boundaries and Mapping Elements*, October 2012. RFC 6739, Internet Engineering Task Force.

[25] M. Thomson and J. Winterbottom. *Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)*, February 2008. RFC 5139, Internet Engineering Task Force.

[26] M. Thomson and J. Winterbottom. *Discovering the Local Location Information Server (LIS)*, September 2010. RFC 5986, Internet Engineering Task Force.

[27] H. Tschofenig, H. Schulzrinne, and B. Aboba. *Trustworthy Location Information*, October 2012. draft-ietf-ecrit-trustworthy-location-04.txt (work in progress), Internet Engineering Task Force.

[28] J. Winterbottom, M. Thomson, and H. Tschofenig. *GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations*, March 2009. RFC 5491, Internet Engineering Task Force.

[29] J. Winterbottom, H. Tschofenig, and R. Barnes. *Use of Device Identity in HTTP-Enabled Location Delivery (HELD)*, March 2011. RFC 6155, Internet Engineering Task Force.

[30] J. Winterbottom, H. Tschofenig, H. Schulzrinne, and M. Thomson. *A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)*, October 2012. RFC 6753, Internet Engineering Task Force.