Internet Engineering Task Force
INTERNET-DRAFT
draft-schulzrinne-sipping-sos-03.ps
H. Schulzrinne
Columbia U.
December 6, 2002
Expires: May 2003

Emergency Services for Internet Telephony based on the Session Initiation Protocol (SIP)

Status of this Memo

Copyright Notice

Abstract

This document defines a universal emergency SIP URI, sip:sos@domain, that allows SIP user agents to contact the local emergency number. It also describes how such calls are routed for both PSTN and IP-based emergency call centers.

1 Introduction

Using the PSTN, emergency help can often be summoned at a designated, widely known number, regardless of where the telephone was purchased. However, this number differs between localities, even though it is often the same for a country or region (such as many countries in the European Union). For end systems based on the Session Initiation Protocol (SIP) [2], it is desirable to have a universal identifier, independent of location, to simplify the user experience and to allow the device to perform appropriate processing. Here, we define a common user identifier, "sos", as the contact mechanism for emergency assistance.

We also describe how such calls are routed to the appropriate emergency call center (ECC). (In the United States and Canada, emergency call centers are referred to as Public Safety Answering Points (PSAPs).) Since each emergency call center is generally only responsible for a specific geographic area, it is important that calls are routed to the correct ECC. Regardless of whether the ECC is connected to the PSTN or is directly reachable via SIP, the network location of the caller has little relationship to its physical location. If the call is routed through a PSTN gateway, the originating number is likely either associated with the gateway or is permanently assigned to the IP phone, regardless of where it is currently located. For SIP-based ECCs, the IP address or Contact header information in the call only provides crude approximation as to the geographic location of the caller and may well be completely wrong if virtual private networks are used. Thus, the SIP request needs to convey the location of the caller so that the call can be routed appropriately. Section 5 discusses one possible approach.

1.1 Terminology

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 [1] and indicate requirement levels for compliant SIP implementations.

2 Requirements

A single, global (set of) identifiers for emergency services is highly desirable, as it allows end system and network devices to be built that recognize such services and can act appropriately. Such actions may include restricting the functionality of the end system, providing special features, overriding user service constraints or routing session setup messages. The details of the emergency service and the associated end system and network server policies can be specific to jurisdictions and are beyond the scope of this document.

3 Emergency URI

It is RECOMMENDED that SIP-based [2] end systems and proxy servers support a uniform emergency call identifier, namely the user name "sos" at any domain, e.g.,

```
sip:sos@example.com
```

The host part of the emergency URI SHOULD be the host portion of the address-of-record of the caller.

The domain-of-record was chosen since a SIP user agent may not be able to determine the local domain it is visiting. This also allows each user to test this facility, as the user can ensure that such services are operational in his home domain. An outbound proxy in the visited domain can handle the call if it believes to be in a position to provide appropriate emergency services.

In addition, user agents and proxies SHOULD also recognize the telephone numbers 911 and 112, expressed as a "tel" URI [3, 4] such as

```
tel:911;phone-context=+1
tel:112;phone-context=+1
```

for this purpose. Where feasible, user agents SHOULD recognize additional, local emergency numbers. Outbound proxy servers MUST be configurable to recognize additional local emergency numbers.

There are about 60 service numbers for emergency services in the world; including them all is not practical, as that would interfere with existing local two, three and four-digit dialing plans.

In addition, we define subaddresses of sos for specific emergency services:

sos.fire	fire brigade
sos.rescue	ambulance (rescue)
sos.marine	marine guard
sos.police	police (law enforcement)
sos.mountain	mountain rescue

In some areas, these emergency services use different numbers.

The “sos” user name and user names starting with “sos.” MUST NOT be assigned to any regular user. It is RECOMMENDED that SIP MESSAGE requests are directed to a TTY-for-the-deaf translator or a short-message service (SMS) if the emergency call center cannot handle SIP messaging.

4 Request Handling

A user agent SHOULD direct an “sos” request to an outbound proxy server.

> Using a proxy server that is local to the user agent is more likely to reach a geographically local server, although that is not guaranteed if virtual private networks are being used.

User agent servers and proxy servers MUST NOT require that the user agent client be registered or authenticated in order to place an emergency call.

OPTIONS requests to the user “sos” and the “sos.*” addresses (sos.fire, etc.) can be used to test if the “sos” addresses are valid. As in standard SIP, a 200 (OK) response indicates that the address was recognized and a 404 (Not found) that it was not. Such request cause no further action. It is RECOMMENDED that user agents periodically automatically check for the availability of the “sos” identifier and alert the user if the check fails. The period of such automated checks SHOULD NOT be less than once per day and MUST be randomly placed over the testing interval.

Any proxy, outbound or otherwise, that receives such a request MUST forward (proxy) or redirect the request to the appropriate local emergency number (e.g., 911 in the United States or 112 in Europe). Typically, the proxy server routes the call to an appropriate PSTN gateway, translating the request URI to the local emergency number. Any SIP PSTN gateway shall translate this emergency identifier to the locally supported emergency number. Determining the appropriate number is discussed in Section 5.

If a proxy receives a “sos.*” request (such as sos.fire), the proxy forwards it to the appropriate emergency service. If it does not recognize the suffix (e.g., fire), it MUST forward the request to the appropriate general emergency contact, handling it as if the address was “sos”.

5 Request Routing

Each SIP request directed to the emergency URI SHOULD contain information about the caller’s location. We outline a mechanism below.

1. The SIP UA determines its location, preferably ahead of the emergency call. It MAY use DHCP [5], retrieving the the location either as geospatial coordinates (longitude, latitude and altitude) [6] or as a civil address (street and community) [**?**].

   The UA needs to inform the DHCP server about its network attachment point. There are several possibilities, including use of the RFC 3046 [7] Agent-Circuit-ID or Remote-ID sub-options. This approach will only work if the DHCP relay agent is colocated with the LAN device close to the SIP UA. Another option, not yet fully supported, is to have the UA determine the device and port information and then include this in the DHCP request. There currently is no DHCP option for doing so, however.

2. It then inserts this location into a SIP header field, for example:

```
Location: ;lat=38.89868 ;long=-77.03723 ;alt=15 ;alt-unit=m
```

```
;lares=0.000122 ;lores=0.000122
;hno=600 ;lmk="White House" ;mcn="Washington"
;stn="Pennsylvania" ;sts="Ave" ;sta="DC"
;privacy=dnf
```

Here, we assume that the DHCP option provided a resolution of 22 bits. The example is taken from [8].

(The SIP header field format is fictitious and is defined in TBD.)

Alternatively, the outbound proxy may map the UA's device address to a physical location, e.g., based on a traceback within an Ethernet switched LAN. Such mechanisms are beyond the scope of this document.

3. The outbound proxy or recipient of the SIP request uses the location information to determine the address of the emergency call center. We call this entity the emergency call router (ECR). The ECR needs to make a two-step determination. First, it determines if the caller is local, i.e., guaranteed to be served by the same ECC ("emergency service area"). For example, this may be the case for an ECR located on a corporate or university campus or a DSL provider which precisely knows that a subset of its lines are local to a ECC service area. If the caller is not local, it needs to look up the serving ECC in a database. The protocol for doing this lookup is currently not standardized.

   There are two basic decisions:

   (a) The ECC uses SIP-based technology, regardless of location. In that case, the ECR simply proxies or redirects the request to the SIP-capable ECC. Note that the ECC can also be a front-end for a regional or national call routing service that in turn finds the correct emergency dispatch center.

   (b) The ECC uses traditional technology. Here, we have two sub-cases:

      i. The caller and ECR are known to be served by the same ECC. In that case, the ECR places a normal emergency call.

      ii. The caller and ECR are not in the same emergency service area. In that case, a database lookup determines the PSTN number of the ECC. The ECR then routes the call to an appropriate PSTN gateway that can place the call. Ideally, the gateway may be local to the ECC, but that may not be achievable, as it would require a gateway in every community.

         In the United States, for example, there are about 5,000 primary emergency call centers, called Public Safety Answering Points (PSAPs).

   In both of these cases, the ECR causes the calling number to be a telephone number that is mapped by the ECC to the location of the caller. (The process for creating such mappings is beyond the scope of this document. The process has been demonstrated in some jurisdictions for multi-line telephone systems.) It is not clear whether all circuit-switched trunk technologies allow potentially arbitrary, out-of-area calling numbers.

6 Alternative Identifiers Considered

The scheme proposed here follows the convention of RFC 2142 [9]. One drawback is that it may conflict with locally assigned addresses of the form "sos@somewhere".

There are a number of possible alternatives, each with their own set of advantages and problems:

tel:sos This solution avoids name conflicts, but is not a valid "tel" URI. It also only works if every outbound proxy knows how to route requests to a proxy that can reach emergency services. The SIP URI proposed here only requires a user's home domain to be appropriately configured.

URI parameter: One could create a special URI, such as "aor-domain;user=sos". This avoids the name conflict problem.

Special domain: A special domain, such as "sip:fire@sos.int" could be used to identify emergency calls. This has similar properties as the "tel:sos" URI, except that it is indeed a valid URI.

7 Security Considerations

The SIP specification [2] details a number of security considerations. Security for emergency calls has conflicting goals, namely to make it as easy and reliable as possible to reach emergency services, while discouraging and possibly tracing prank calls. It appears unlikely that classical authentication mechanisms can be required by emergency call centers, but SIP proxy servers may be able to add identifying information.

Allowing the user agent to clearly and unambiguously identify emergency calls makes it possible for the user agent to make appropriate policy decisions. For example, a user agent policy may reveal a different amount of information to the callee when making an emergency call. Local laws may affect what information network servers or service providers may be allowed or be required to release to emergency call centers. They may also base their decision on the user-declared destination of the call.

Normative References

[1] S. Bradner, "Key words for use in RFCs to indicate requirement levels," RFC 2119, Internet Engineering Task Force, Mar. 1997.

[2] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: session initiation protocol," RFC 3261, Internet Engineering Task Force, June 2002.

Informative References

[3] A. Vaha-Sipila, "URLs for telephone calls," RFC 2806, Internet Engineering Task Force, Apr. 2000.

[4] H. Schulzrinne and A. Vaha-Sipila, "The tel URI for telephone calls," Internet Draft, Internet Engineering Task Force, Oct. 2002. Work in progress.

[5] R. Droms, "Dynamic host configuration protocol," RFC 2131, Internet Engineering Task Force, Mar. 1997.

[6] J. Polk *et al.*, "DHCP option for geographic location," Internet Draft, Internet Engineering Task Force, Oct. 2002. Work in progress.

[7] M. Patrick, "DHCP relay agent information option," RFC 3046, Internet Engineering Task Force, Jan. 2001.

[8] J. Polk *et al.*, "Semantics for DHC location object within GEOPRIV," Internet Draft, Internet Engineering Task Force, Oct. 2002. Work in progress.

[9] D. Crocker, "Mailbox names for common services, roles and functions," RFC 2142, Internet Engineering Task Force, May 1997.

8 Acknowledgements

Andrew Allen, James Polk, Brian Rosen and John Schnizlein contributed helpful comments.

9 Authors' Addresses

Henning Schulzrinne
Dept. of Computer Science
Columbia University
1214 Amsterdam Avenue
New York, NY 10027
USA
electronic mail: schulzrinne@cs.columbia.edu

Full Copyright Statement