Internet Engineering Task Force
INTERNET-DRAFT
draft-schulzrinne-sipping-sos-04.ps
H. Schulzrinne
Columbia U.
January 8, 2003
Expires: June 2003

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

Status of this Memo

Copyright Notice

Abstract

This document describes how Session Initiation Protocol (SIP) user agents and proxies can set up emergency calls and, more generally, reach emergency assistance via SIP requests. For that purpose, it defines a universal emergency SIP URI, sip:sos@domain and sips:sos@domain, that allows SIP user agents to contact the local emergency number. It also defines conventions that increase the high probability of reaching the appropriate emergency call center. The document does not define any SIP protocol extensions.

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) [1], 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. This identifier is meant to be used in addition to any local emergency numbers.

We also describe how emergency 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 6 discusses one possible approach.

This document does not introduce any new SIP header fields, request methods, status codes, message bodies, or events. User agents unaware of the recommendations in this draft can place emergency calls, but may not be able to provide the same user interface functionality. The document suggests behavior for proxy servers, in particular outbound proxy servers.

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 BCP 14, RFC 2119 [2] and indicate requirement levels for compliant SIP implementations.

2 Requirements

- SIP-based end systems must be able to reach emergency call centers. These emergency call centers may have SIP capabilities or may be reachable only via a SIP-to-PSTN gateway. Since each ECC serves only a limited geographic area, often defined by jurisdictional boundaries such as state, province or county, SIP-based emergency requests must

- While current emergency call centers are limited to voice and TDD (telecommunication device for the deaf) communications, future SIP-based ECCs should handle all relevant means of interaction, including multimedia and instant messaging [8].

- It should be possible for devices to provide user interfaces that can directly cause an emergency call, without the user having to "dial" or type a specific address.

- Even as each country is likely to operate their emergency calling infrastructure differently, SIP devices should be able to reach emergency help and, if possible, be located in any country.

- While traveling, users must be able to use their familiar "home" emergency identifier. Users should also be able to dial the local emergency number in the country they are visiting.

- Any mechanism must be deployable incrementally and work even if not all SIP entities support emergency calling. User agents conforming to the SIP specification [1], but unaware of this document, must be able to place emergency calls, possibly with restricted functionality.

- Given incremental deployment, emergency call functionality should be testable by the user without causing an emergency response.

- Emergency calling mechanisms must support existing emergency call centers based on circuit-switched technology as well as future ECC that are SIP-capable.

- Emergency call mechanisms should not require a specific technology for determining the location of the caller.

3 Emergency URIs

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.

UAs that determine that a dialog or transaction relates to an emergency MUST use an emergency call identifier in the Request-URI. The Request-URI MUST be either an emergency SIP URI defined in Section 3.1 or an emergency tel URI defined in Section 3.2.

3.1 SIP URIs for Emergency Calls

It is RECOMMENDED that SIP-based [1] end systems and proxy servers support a uniform emergency call identifier, namely the reserved user name "sos" within any domain, e.g.,

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

The reserved name is case-insensitive.

The host part of the emergency URI SHOULD be the host portion of the address-of-record of the caller. The "sips" form SHOULD be used to ensure integrity and confidentiality. All SIP requests with URIs of this form are assumed to be emergency calls.

> 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, we reserve user addresses beginning with the string "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

The sub-addresses are also case-insensitive. Additional subaddresses can be registered with IANA (Section 11).

> In some areas, these emergency services use different numbers.

The SIP URI user name "sos" and user names starting with "sos." MUST NOT be assigned to any regular user.

3.2 Tel URIs for Emergency Calls

User agents SHOULD determine the local emergency numbers, either by consulting their manual configuration for devices that do not move across national borders, by DHCP (Section 9) or some other configuration mechanism. If a user agent has no knowledge of local emergency numbers, it MUST also recognize the digit strings 000, 08, 112, 110, 118, 119, 911 and 999 as emergency numbers.

SIP user agents, such as Ethernet deskphones, that are unlikely to move frequently across national borders can easily implement a local dialing plan that recognizes local emergency numbers. Mobile devices, including PDAs and laptops, may not have a reliable way of determining their current location. Using automatic configuration avoids collisions with extensions that equal one of the eight numbers above. If a local network does not have an outbound proxy server, local dial plans also do not apply, so the problem of number collision does not arise. Collisions with non-emergency service numbers are still possible, albeit less likely. For example, 118 is used for directory assistance in the United Kingdom.

If the user dials any of these digit strings, the UAC SHOULD generate a request with the "sos" URI described in Section 3.1 unless it has discovered a local outbound proxy as described in Section 9. In that case, a UAC MAY use a "tel" URI [3, 4] without phone-context, such as

```
tel:911
tel:112
```

Outbound proxy servers MUST be configurable to recognize additional local emergency numbers in "tel" URIs.

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.

4 Request Handling

Once identified, a user agent SHOULD direct an emergency call request to an outbound proxy server or use the discovery mechanism described in Section 9 to find a local PSTN gateway that can connect the caller to a local emergency call center.

Outbound proxy servers MUST recognize all local emergency numbers as well as the tel URIs enumerated in Section 3.2. The proxy MAY use any additional information contained in the call request, such as Mobile Country Code and the Mobile Network Code for 3GPP devices, to recognize additional numbers as emergency numbers.

It is RECOMMENDED that gateway 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 instant messaging.

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.

5 Determining User Agent Location

Proper handling of emergency calls requires knowledge of the caller location to route the call to the appropriate ECC and to help the ECC in locating the caller when rendering emergency assistance. We describe the routing details in Section 6.

The SIP UA determines its location, preferably ahead of the emergency call. It MAY use DHCP [9], retrieving the the location one or more of: geospatial coordinates (longitude, latitude and altitude) [10], civil address (street and community) [11] or network access information such as the port and switch number or the wireless cell identity.

The UA needs to inform the DHCP server about its network attachment point. There are several possibilities, including use of the RFC 3046 [12] 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.

The UAC inserts this location into a SIP header field. For geographic information, this might look something like the following:

```
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 [13].

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

For 3GPP networks, the P-Access-Network-Info header field [14] can convey the cell information, as defined in 3GPP TS 24.229.

Alternatively, an 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.

6 Request Routing

Any proxy, outbound or otherwise, that receives such a request MUST forward (proxy) or redirect the request to the appropriate emergency number local to the caller, using the location information described in Section 5.

Note that in some limited cases, the proxy may be able to determine that the requestor is in the same local network even without explicit location information. This may be the case, for example, if the IP address of the request indicates a local device and the network offers no VPN services. Even under these restricted circumstances, back-to-back UAs may mislead the proxy in this estimation.

We distinguish two cases, depending on whether the proxy has access to a location-to-ECC mapping service or not. A special, but important, case is that the caller is known to be local to a PSTN gateway.

6.1 Known to be Local

In some cases, the proxy server can reliably determine that the caller and a local PSTN gateway are in the same emergency service area. In that case, the proxy forwards the call request to the gateway, translating the emergency URI into the local emergency number.

6.2 Mapping Service Available

We refer to the location-to-ECC mapping service as a jurisdictional directory service (JDS) since it maps geographic and/or civil locations to emergency response jurisdictions. [TBD: better term?] The JDS can be considered a special kind of SIP location service. The protocol between the proxy and the JDS is beyond the scope of this document.

One plausible solution simply proxies the SIP request itself to the JDS.

Conceptually, the JDS is provided with a geographic location and possibly the type of emergency service requested (for "sip:sos.service" URIs) and returns SIP or tel URIs for one or more ECCs serving the caller. If the JDS does not recognize the service specification, it treats the mapping request like a general emergency service request.

The tel URI returned by the JDS will contain a globally reachable (E.164) number, i.e., a global-number according to [4]. The proxy routes the call accordingly, using a local mechanism to determine the appropriate gateway, e.g., TRIP [5].

Ideally, the chosen gateway should 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).

6.3 No Mapping Service Available

If the proxy does not have access to a JDS, it attempts to pick the closest PSTN gateway, translates the Request-URI to a locally valid emergency number and proxies the call to that gateway.

If a proxy receives a service-specific request of the form "sip:sos.*@domain" (such as "sos.fire@example.com"), the proxy forwards it to the local appropriate specific 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 "sip:sos@domain".

7 Caller Identification

When using a PSTN gateway, the gateway 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.

8 Call Behavior

The user agent SHOULD not issue a REFER during an emergency call.

The user agent SHOULD NOT issue a BYE request during an emergency call. If the user "hangs up", it is RECOMMENDED that the end system generate an alert tone until the user reconnects.

The UA SHOULD automatically accept an incoming call from the same entity that accepted the previous emergency call.

This allows the ECC to call back should the call be interrupted accidentally.

9 Identifying the Local Emergency Numbers and Gateway

There are many ways that a user agent can configure emergency numbers for use in analyzing calls made with telephony-type user input. These include configuration tokens such as SIM cards in mobile devices, or protocol-based solutions. We describe one such protocol-based mechanism, based on DHCP, but this does not imply a requirement for devices.

We propose a new DHCP option that enumerates the valid local emergency identifiers, as a list of "tel", "sip" or "sips" URIs. These identifiers can be used by the UA to trigger special behavior when the user dials those numbers, or they can identify a local PSTN gateway that can provide local emergency service. A DHCP server SHOULD advertise its local emergency number as well as those numbers among the eight digit strings enumerated in Section 3.2 that do not collide with local non-emergency services or extensions.

This DHCP option MUST NOT be used if DHCP does not announce the local SIP server [6].

> Unlike an outbound proxy server, the DHCP server is very likely to be located within the same country as the user agent. However, since the user agent needs to perform the call routing, it makes little sense to have the DHCP information identify a set of numbers that mean nothing special to the outbound proxy server. Thus, server identification and emergency number identification belong together.

If the local network supports the location of gateways via SLP [7], the user agent can discover such gateways. The SLP service description needs to be enhanced with a list of valid emergency numbers.

Details are described in TBD.

[This is for discussion only and, if suitable, will move to a different draft.]

10 Alternative Identifiers Considered

The "sos" SIP URI reserved user name proposed here follows the convention of RFC 2142 [15] and the "postmaster" convention documented in RFC 2822 [16]. 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, but requires mechanism-aware user agents that are capable of emitting this special URI.

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.

11 IANA Considerations

Subaddresses of the "sos" address are registered with IANA This specification establishes the "sos" subaddres sub-registry under http://www.iana.org/assignments/sip-parameters.

Subaddresses are registered by the IANA when they are published in standards track RFCs. The IANA Considerations section of the RFC must include the following information, which appears in the IANA registry along with the RFC number of the publication.

- Name of the subaddress. The name MAY be of any length, but SHOULD be no more than twenty characters long. The name MUST consist of alphanumeric characters only and is case-insensitive.
- Descriptive text that describes the emergency service.

12 Security Considerations

The SIP specification [1] 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.

Given the sensitive nature of many emergency calls, it is desirable to use the "sips" URI to ensure transport-level confidentiality and integrity. However, this may cause the call to fail in some environments.

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.

Outbound proxies may need to adjust their authentication requirements for such emergency calls.

It is desirable to be able to verify that the call is reaching a true emergency call center. The caller is unlikely to know or be able to obtain the public key of the destination ECC since it does not even know the ECC identity. The responding ECC could sign the response, via standard SIP S/MIME mechanisms. However, the principal in the certificate would appear as a random-looking domain name, such as `admin.fayette.co.ga.us`, which cannot be reliably identified as an ECC. Here, an attribute certificate (AC) [17] could be used to associate the attribute "ECC" with the SIP URI. However, it appears unlikely that such an Attribute Authority will emerge anytime soon, particularly across national borders. Alternatively, ICANN could create a new restricted top-level domain, such as .sos, that is open only to accredited emergency response entities. Clearly, this is also not likely in the short term.

The caller has little choice other than to trust the outbound proxy server acting as an ERC or to act as its own ERC. In the former, more likely case, the ERC will obtain the ECC identity from a database source it trusts. The ERC then only has to ensure that the call reaches the appropriate domain, which standard TLS server authentication accomplishes, regardless of the domain name used by the ECC and without the notion of attribute certificates. Since a caller cannot assume that all ECCs will have valid ACs, the absence of such a certificate is unlikely to cause the caller to abandon the call in an emergency. Thus, the transitive trust model, which is easier to implement, appears to be a more pragmatic approach.

Normative References

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

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

[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, Dec. 2002. Work in progress.

[5] J. Rosenberg, H. F. Salama, and M. Squire, “Telephony routing over IP (TRIP),” RFC 3219, Internet Engineering Task Force, Jan. 2002.

[6] H. Schulzrinne, “Dynamic host configuration protocol (dhcp-for-ipv4) option for session initiation protocol (SIP) servers,” RFC 3361, Internet Engineering Task Force, Aug. 2002.

[7] W. Zhao and H. Schulzrinne, “Locating ip-to-public switched telephone network (PSTN) telephony gateways via SLP,” internet draft, Internet Engineering Task Force, Aug. 2002. Work in progress.

Informative References

[8] B. Campbell, J. Rosenberg, and H. Schulzrinne, eds., “Session initiation protocol (SIP) extension for instant messaging,” RFC 3428, Internet Engineering Task Force, Dec. 2002.

[9] R. E. Droms, “Dynamic host configuration protocol,” RFC 2131, Internet Engineering Task Force, Mar. 1997.

[10] J. Polk *et al.*, “DHCP option for geographic location,” internet draft, Internet Engineering Task Force, Oct. 2002. Work in progress.

[11] H. Schulzrinne, “DHCP option for civil location,” internet draft, Internet Engineering Task Force, Dec. 2002. Work in progress.

[12] M. Patrick, “DHCP relay agent information option,” RFC 3046, Internet Engineering Task Force, Jan. 2001.

[13] J. Polk *et al.*, “Semantics for DHC location object within GEOPRIV,” internet draft, Internet Engineering Task Force, Oct. 2002. Work in progress.

[14] M. Garcia, E. Henrikson, and D. L. Mills, “Private extensions (p-header) extensions to the session initiation protocol (SIP) for the 3rd-generation partnership project (3GPP),” internet draft, Internet Engineering Task Force, Nov. 2002. Work in progress.

[15] D. H. Crocker, “Mailbox names for common services, roles and functions,” RFC 2142, Internet Engineering Task Force, May 1997.

[16] P. Resnick, ed., “Internet message format,” RFC 2822, Internet Engineering Task Force, Apr. 2001.

[17] S. Farrell and R. Housley, “An Internet attribute certificate profile for authorization,” RFC 3281, Internet Engineering Task Force, Apr. 2002.

13 Change History

13.1 Changes since -03

- Added description of local discovery mechanism for finding a local gateway.

- Noted that 'sos' is case-insensitive and only applies to SIP URIs, not other URIs.
- Described the ECC verification options available to a caller.
- Added local gateway discovery.
- Added outline of how to use DHCP for configuring additional local emergency numbers.
- Added 3GPP emergency numbers beyond 112 and 911.

14 Acknowledgements

Andrew Allen, Keith Drage, Mike Pierce, James Polk, Brian Rosen and John Schnizlein contributed helpful comments.

15 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