Internet Engineering Task Force
INTERNET-DRAFT
draft-ietf-sip-emergency-00.ps

Schulzrinne
Columbia U.

March 24, 2001
Expires: December 2001

Emergency Call Services for SIP-based Internet Telephony

Status of this Memo

Copyright Notice

Abstract

This document describes how SIP-based Internet telephony systems can provide emergency calling services.

1 Introduction

A companion document [1] outlines some of the issues in providing emergency calling service. This document suggests a set of protocols and operational mechanisms to provide such services. The design is motivated by the desire to keep the overall system as simple as possible and to minimize dependencies on external services, particularly those that are used only or mainly for emergency services.

We abstractly refer to emergency answering services (EAS) as locations where public safety officials answer emergency calls. In the United States and Canada, these are commonly known as Public Safety Answering Points (PSAPs). In Europe, . . .

In this document, we do not distinguish whether the EAS is connected to the legacy PSTN or uses SIP-enabled end systems. For simplicity, we assume that calls are routed to the PSTN gateway that can reach emergency services that correspond to the caller's location. (Note that this has implications for the density of PSTN gateways.) In the future, it may be feasible for gateways to provide guidance to PSTN switches as to which exchange the call originated from, even if the calling Internet terminal does not have an assigned E.164 number that corresponds to a geographic location. (With number portability, E.164 numbers may not be good indicators of geographic origin and thus may not be helpful in selecting an EAS.)

2 Emergency Address

All SIP proxies MUST recognize the user name `sos` in any domain as the emergency address. They SHOULD also recognize the user names `911` and `112` as such, in addition to any local emergency numbers. (These

sip URLs should be recognized as emergency addresses independent of whether they are labeled with the "user=phone" parameter.) In addition, the `tel:911` and `tel:112` URLs, and emergency numbers local to the proxy, should also be recognized.

> 112 is the GSM and European emergency number. 911 is the North American emergency number. Unfortunately, there are far too many different local emergency numbers to include them all.

SIP UAs MUST NOT be able to register for these emergency addresses. However, registrations may be configured such that emergency calls are directed to an appriate proxy.

SIP UAs SHOULD employ an automatic configuration mechanism to learn about local emergency addresses. The precise configuration mechanism is beyond the scope of this document.

> This makes it possible for a UA that is brought into a new environment to be used for emergency calls by users other than the owner.

3 Locating the Emergency Answering Service

For reliability and robustness, any SIP proxy, including outbound proxies and those operating in emergency answering services (EAS), SHOULD attempt to route the call to the best available EAS, based on location information contained in the request. For example, a basic proxy might always route the call to a single EAS, even though the caller's physical location may require routing to another EAS.

> With VPNs, a proxy may not be able to tell whether a call originated within the local campus, for example.

UAs SHOULD include geographic and/or civil location information in their emergency requests. Proxies MAY add additional information to calls they recognize as emergency calls, either to augment the information or to indicate that the proxy has doubts about the location information already included in the request. (This mechanism raises number of security considerations detailed in Section 5.)

Similar to the use of ENUM [2], we propose to use DNS to map location identifiers to SIP or other URLs. (Note: If a particular domain does not want to use this mechanism, they can refer the emergency call to a hard-configured EAS, which can then use any local mechanism to perform further call routing lookups.) For example, postal codes and country identifiers may be used for mappings, so that the United States postal code 07605-1234 gets mapped to a DNS lookup `4.3.2.1.5.0.6.7.0.us.emergency.arpa`. If a locality has multiple address code formats, such as shorter and longer postal codes, the short codes should also have entries, in case the UA or proxy does not have precise location information. The management of this DNS address space is beyond the scope of this document.

> Postal codes are usually assigned geographically, so that resolution is more likely to be geographically close to the querier, increasing reliability. DNS is proposed since it does not require installing and maintaining additional servers and infrastructure, is usually fast and minimizes the additional complexity in proxies. It does have the disadvantage that geographic information has to be entered completely. Does this work for Canadian and UK postal codes that combine letters and numbers?

[THIS REQUIRES DISCUSSION. IS THERE A BETTER SCHEME?]

4 User Location

The UA or proxy handling the emergency call adds information about caller location (civil and/or geographic) to the SIP request, using the Remote-Party-ID header [3].

[THIS IS OBVIOUSLY HAND-WAVING.]

The ability of EAS to request location information from third parties is beyond the scope of this document, as it does not affect SIP signaling.

5 Security Considerations

Emergency call services raise numerous security and privacy issues. Callers need to be authenticated to discourage crank calls that could interfere with true emergency requests. This requires authenticated caller information, but this also raises privacy issues. Generally, expectation of privacy appears to be less than making emergency calls, as location information is considered extremely helpful in providing emergency assistance. It may be desirable, however, to allow end systems to explicitly decline being identified by location or caller, with the answering emergency operator being made aware of this fact.

Address information needs to be protected against spoofing, either within the end system or en route, as such spoofing can be used to deny emergency services.

RFC 1984 [4]

6 Acknowledgements

References

[1] H. Schulzrinne, “Providing emergency call services for sip-based internet telephony,” Internet Draft, Internet Engineering Task Force, July 2000. Work in progress.

[2] P. Faltstrom, “E.164 number and DNS,” Request for Comments 2916, Internet Engineering Task Force, Sept. 2000.

[3] W. Marshall *et al.*, “SIP extensions for caller identity and privacy,” Internet Draft, Internet Engineering Task Force, Nov. 2000. Work in progress.

[4] IAB and IESG, “IAB and IESG statement on cryptographic technology and the internet,” Request for Comments 1984, Internet Engineering Task Force, Aug. 1996.

7 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