Internet Engineering Task Force (IETF)
Request for Comments: 7090
Category: Standards Track
ISSN: 2070-1721

H. Schulzrinne
Columbia University
H. Tschofenig
C. Holmberg
Ericsson
M. Patel
Huawei Technologies (UK) Co., Ltd.

April 2014

Public Safety Answering Point (PSAP) Callback

Abstract

After an emergency call is completed (terminated either prematurely by the emergency caller or normally by the call taker), the call taker may feel the need for further communication. For example, the call may have been dropped by accident without the call taker having sufficient information about the current state of an accident victim. A call taker may trigger a callback to the emergency caller using the contact information provided with the initial emergency call. This callback could, under certain circumstances, be treated like any other call and, as a consequence, it may get blocked by authorization policies or may get forwarded to an answering machine.

The IETF emergency services architecture specification already offers a solution approach for allowing Public Safety Answering Point (PSAP) callbacks to bypass authorization policies in order to reach the caller without unnecessary delays. Unfortunately, the specified mechanism only supports limited scenarios. This document discusses shortcomings of the current mechanisms and illustrates additional scenarios where better-than-normal call treatment behavior would be desirable. We describe a solution based on a new header field value for the SIP Priority header field, called "psap-callback", to mark PSAP callbacks.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7090.

Copyright Notice

Table of Contents

1. Introduction

Summoning police, the fire department, or an ambulance in emergencies is one of the fundamental and most valuable 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 legacy technology. New devices and services are being made available that could be used to make a request for help and that are not traditional telephones. Users are increasingly expecting them to be used to place emergency calls.

An overview of the protocol interactions for emergency calling using the IETF emergency services architecture is described in [RFC6443], and [RFC6881] specifies the technical details. As part of the emergency call setup procedure, two important identifiers are conveyed to the PSAP call taker's user agent, namely the address-of-record (AOR), and if available, the Globally Routable User Agent (UA) URIs (GRUUs). RFC 3261 [RFC3261] defines the AOR as:

An address-of-record (AOR) is a SIP or SIPS URI that points to a domain with a location service that can map the URI to another URI where the user might be available. Typically, the location service is populated through registrations. An AOR is frequently thought of as the "public address" of the user.

In SIP systems, a single user can have a number of user agents (handsets, softphones, voicemail accounts, etc.) that are all referenced by the same AOR. There are a number of cases in which it is desirable to have an identifier that addresses a single user agent rather than the group of user agents indicated by an AOR. The GRUU is such a unique user-agent identifier, and it is also globally routable. [RFC5627] specifies how to obtain and use GRUUs. [RFC6881] also makes use of the GRUU for emergency calls.

Regulatory requirements demand that the emergency call setup procedure itself provides enough information to allow the call taker to initiate a callback to the emergency caller. This is desirable in those cases where the call is dropped prematurely or when further communication needs arise. The AOR and the GRUU serve this purpose.

The communication attempt by the PSAP call taker back to the emergency caller is called a "PSAP callback".

A PSAP callback may, however, be blocked by user-configured authorization policies or may be forwarded to an answering machine since SIP entities (SIP proxies as well as the SIP user equipment itself) cannot differentiate the PSAP callback from any other SIP call. "Call barring", "do not disturb", or "call diversion" (also called call forwarding) are features that prevent delivery of a call. It is important to note that these features may be implemented by SIP intermediaries as well as by the user agent.

Among the emergency services community, there is a desire to treat PSAP callbacks in such a way that the chances of reaching the emergency caller are increased. At the same time, any solution must minimize the chance that other calls bypass call forwarding or other authorization policies. Ideally, the PSAP callback has to relate to an earlier emergency call that was made "not too long ago". An exact time interval is difficult to define in a global IETF standard due to the variety of national regulatory requirements, but [RFC6881] suggests 30 minutes.

Nevertheless, to meet the needs from the emergency services community, a basic mechanism for preferential treatment of PSAP callbacks was defined in Section 13 of [RFC6443]. The specification says:

> A UA may be able to determine a PSAP callback by examining the domain of incoming calls after placing an emergency call and comparing that to the domain of the answering PSAP from the emergency call. Any call from the same domain and directed to the supplied Contact header or AOR after an emergency call should be accepted as a callback from the PSAP if it occurs within a reasonable time after an emergency call was placed.

This approach mimics a stateful packet-filtering firewall and is indeed helpful in a number of cases. It is also relatively simple to implement even though it requires call state to be maintained by the user agent as well as by SIP intermediaries. Unfortunately, the solution does not work in all deployment scenarios. In Section 3 we describe cases where the currently standardized approach is insufficient.

2. Terminology

Emergency-services-related terminology is borrowed from [RFC5012]. This includes terminology like emergency caller, user equipment, call taker, Emergency Service Routing Proxy (ESRP), and Public Safety Answering Point (PSAP).

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Callback Scenarios

This section illustrates a number of scenarios where the currently specified solution, as described in [RFC6881], for preferential treatment of callbacks fails. As explained in Section 1, a SIP entity examines an incoming PSAP callback by comparing the domain of the PSAP with the destination domain of the outbound emergency call placed earlier.

3.1. Routing Asymmetry

In some deployment environments, it is common to have incoming and outgoing SIP messaging routed through different SIP entities. Figure 1 shows this graphically whereby a Voice over IP (VoIP) provider uses different SIP proxies for inbound and for outbound call handling. Unless the two devices are synchronized, the callback

reaching the inbound proxy would get treated like any other call since the emergency call established state information at the outbound proxy only.

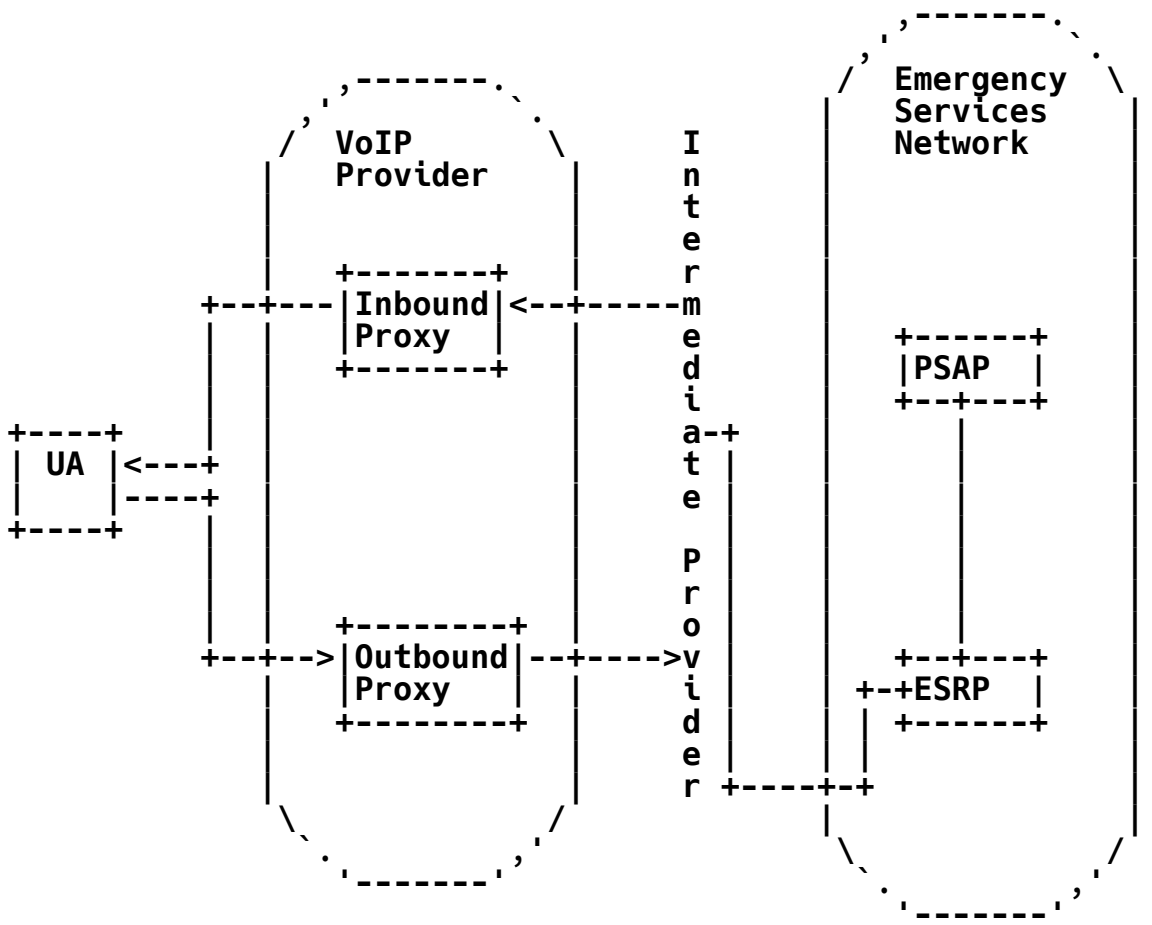

Figure 1: Example for Routing Asymmetry

3.2. Multi-Stage Routing

Consider the emergency call routing scenario shown in Figure 2 where routing towards the PSAP occurs in several stages. In this scenario, we consider a SIP UA that uses the Location-to-Service Translation (LoST) Protocol [RFC5222] to learn the next-hop destination, namely esrp@example.net, to get the call closer to the PSAP. This call is then sent to the proxy of the user's VoIP provider (example.org). The user's VoIP provider receives the emergency call and creates a state based on the destination domain, namely example.net. It then routes the call to the indicated ESRP. When the ESRP receives the call, it needs to decide what the next hop is to get to the final PSAP. In our example, the next hop is the PSAP with the URI psap@example.com.

When a callback is sent from psap@example.com towards the emergency caller, the call will get normal treatment by the proxy of the VoIP provider since the domain of the PSAP does not match the stored state information.

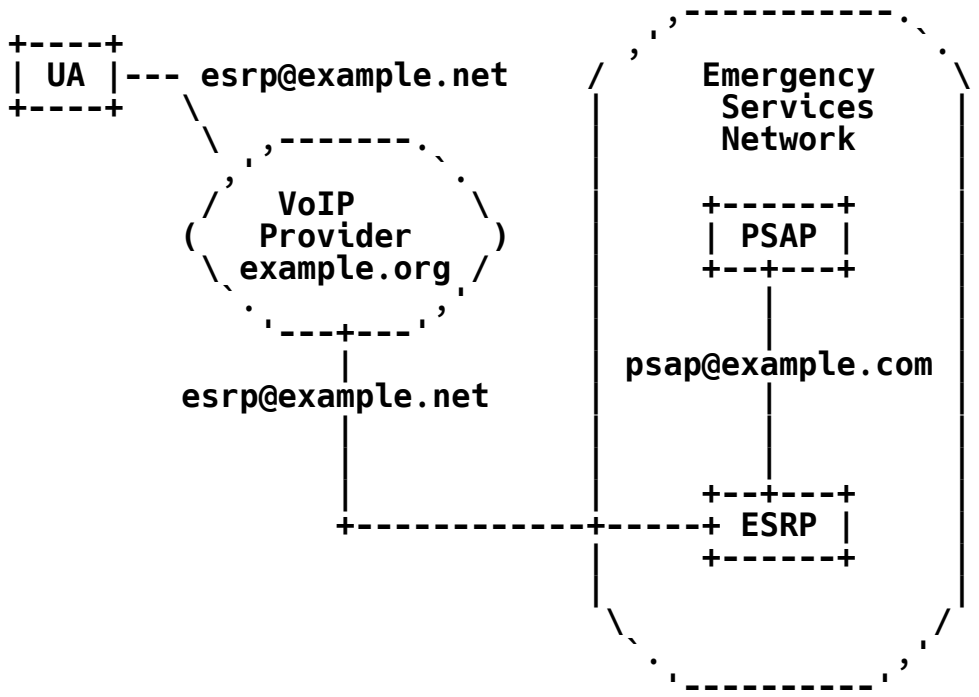

Figure 2: Example for Multi-Stage Routing

3.3. Call Forwarding

Imagine the following case where an emergency call enters an emergency network (state.example) via an ESRP, but then it gets forwarded to a different emergency services network (in our example, to example.net, example.org, or example.com). The same considerations apply when the police, fire and, ambulance networks are part of the state.example subdomains (e.g., police.state.example).

Similar to the previous scenario, the wrong state information is being set up during the emergency call setup procedure. A callback would originate in the example.net, example.org, or example.com domains whereas the emergency caller's SIP UA or the VoIP outbound proxy has stored state.example.

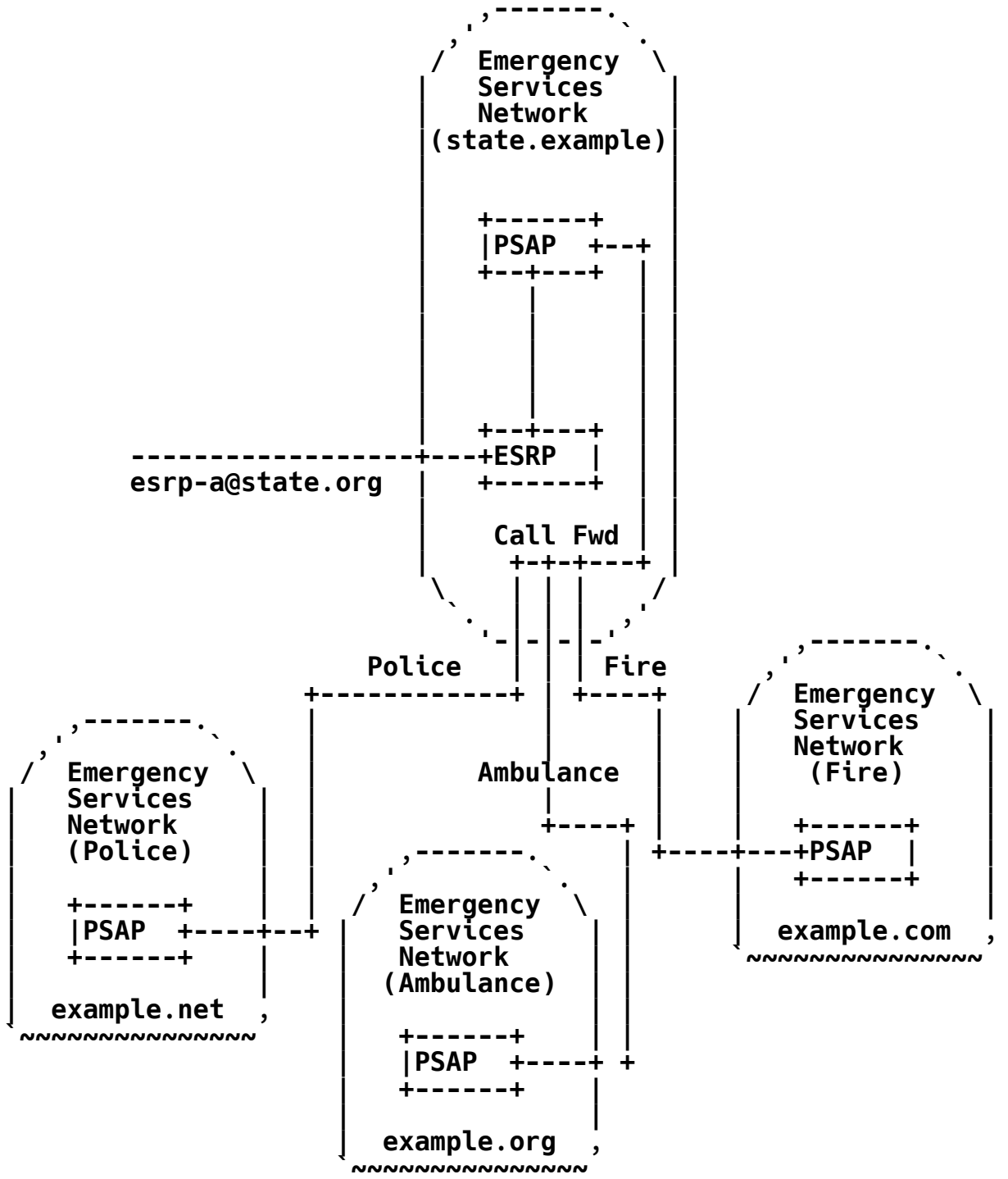

Figure 3: Example for Call Forwarding

3.4. Network-Based Service URN Resolution

The IETF emergency services architecture also considers cases where the resolution from the Service URN to the PSAP URI does not only happen at the SIP UA itself but at intermediate SIP entities, such as the user's VoIP provider.

Figure 4 shows this message exchange of the outgoing emergency call and the incoming PSAP graphically. While the state information stored at the VoIP provider is correct, the state allocated at the SIP UA is not.

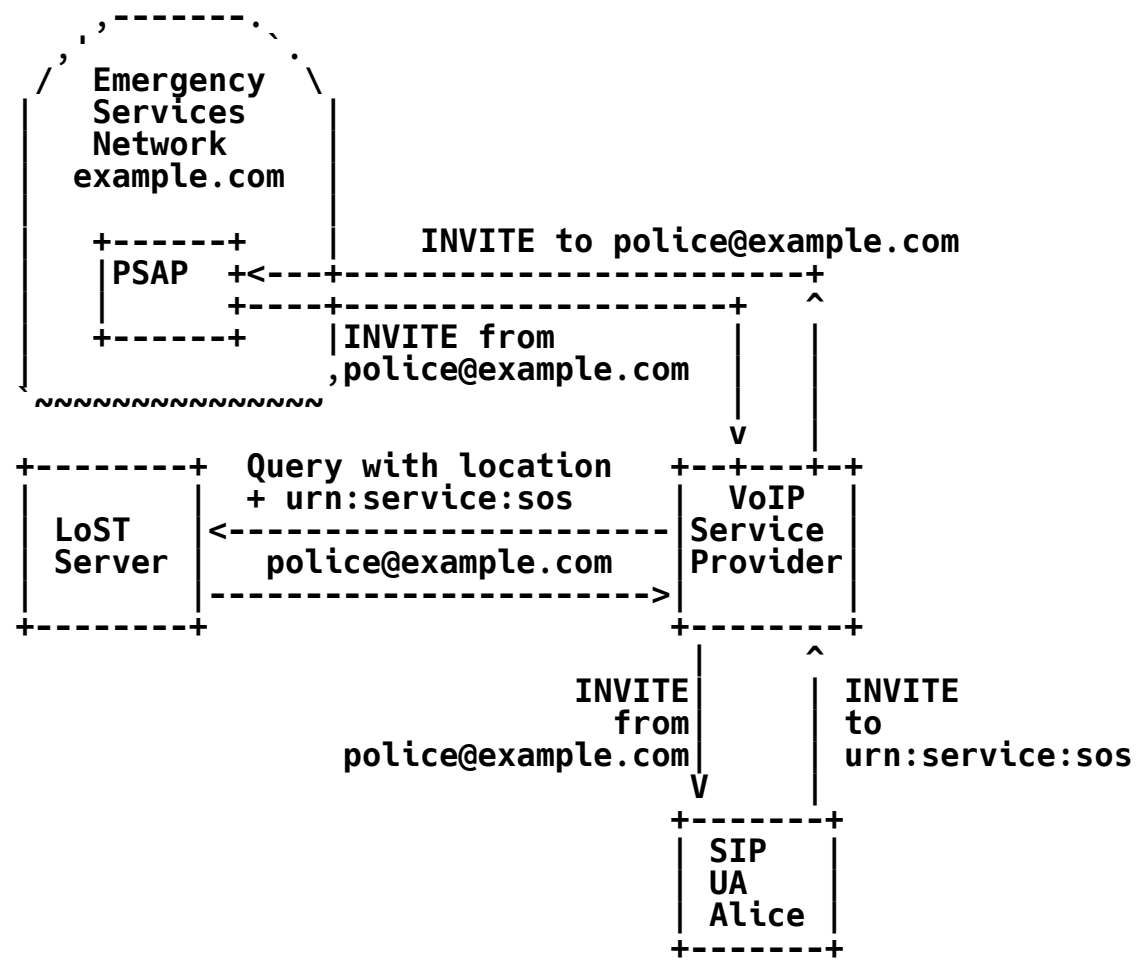

Figure 4: Example for Network-Based Service URN Resolution

3.5. PSTN Interworking

In case an emergency call enters the Public Switched Telephone Network (PSTN), as shown in Figure 5, there is no guarantee that the callback sometime later leaves the same PSTN/VoIP gateway or that the same endpoint identifier is used in the forward as well as in the backward direction making it difficult to reliably detect PSAP callbacks.

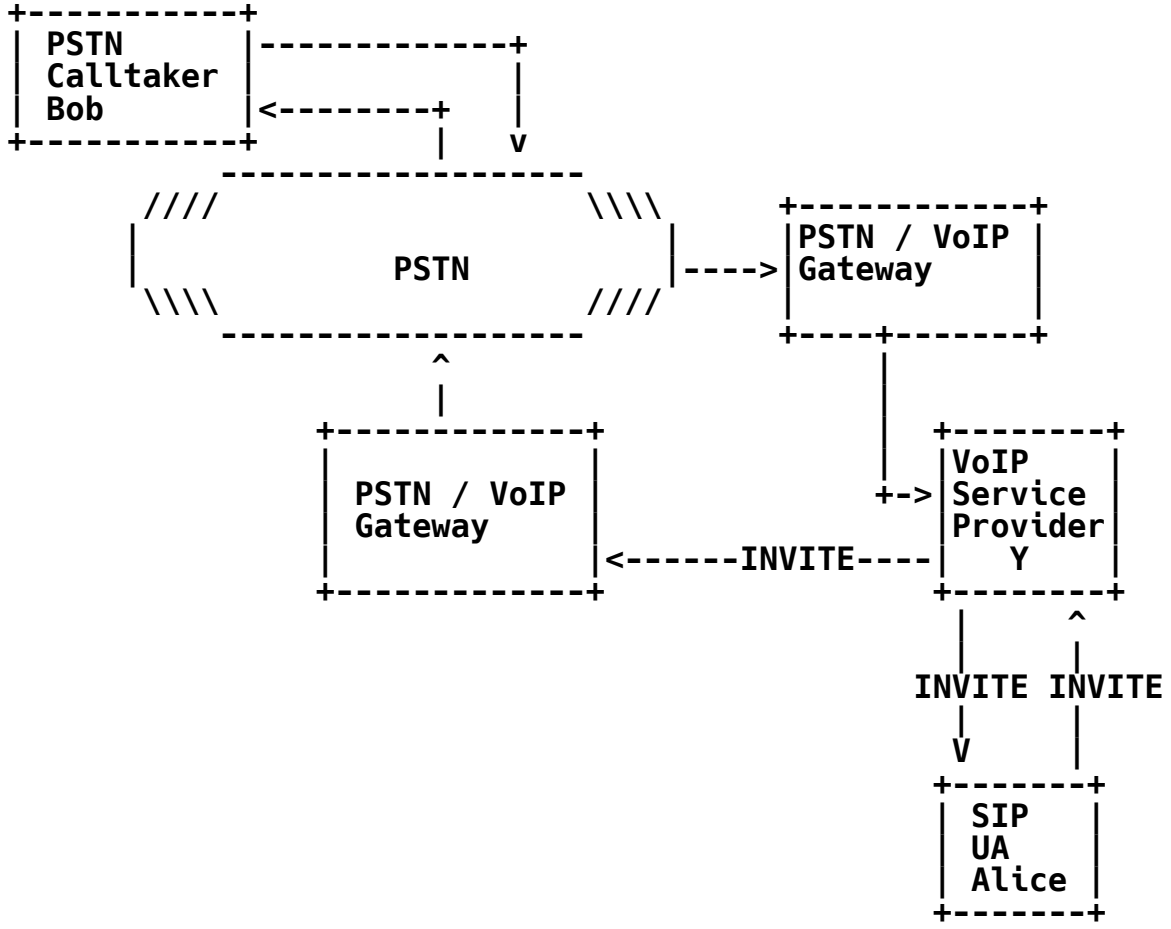

Figure 5: Example for PSTN Interworking

Note: This scenario is considered outside the scope of this document. The specified solution does not support this use case.

4. SIP PSAP Callback Indicator

4.1. General

This section defines a new header field value, called "psap-callback", for the SIP Priority header field defined in [RFC3261]. The value is used to inform SIP entities that the request is associated with a PSAP callback SIP session.

4.2. Usage

SIP entities that receive the header field value within an initial request for a SIP session can, depending on local policies, apply PSAP callback-specific procedures for the session or request.

The PSAP callback-specific procedures may be applied by SIP-based network entities and by the callee. The specific actions taken when receiving a call marked as a PSAP callback marked call, such as bypassing services and barring procedures, are outside the scope of this document.

4.3. Syntax

4.3.1. General

This section defines the ABNF [RFC5234] for the new SIP Priority header field value "psap-callback".

4.3.2. ABNF

```
priority-value  =/  "psap-callback"
```

Figure 6: ABNF

5. Security Considerations

5.1. Security Threat

The PSAP callback functionality described in this document allows marked calls to bypass blacklists and ignore call-forwarding procedures and other similar features used to raise the attention of emergency callers when attempting to contact them. In the case where the SIP Priority header value, "psap-callback", is supported by the SIP UA, it would override user-interface configurations, such as vibrate-only mode, to alert the caller of the incoming call.

5.2. Security Requirements

The security threat discussed in Section 5.1 leads to the requirement to ensure that the mechanisms described in this document cannot be used for malicious purposes, including telemarketing.

Furthermore, if the newly defined extension is not recognized, not verified adequately, or not obeyed by SIP intermediaries or SIP endpoints, then it must not lead to a failure of the call handling procedure. Such a call must be treated like a call that does not have any marking attached.

The indicator described in Section 4 can be inserted by any SIP entity, including attackers. So it is critical that the indicator only lead to preferential call treatment in cases where the recipient has some trust in the caller, as described in the next section.

5.3. Security Solution

The approach for dealing with the implementation of the security requirements described in Section 5.2 can be differentiated between the behavior applied by the UA and by SIP proxies. A UA that has made an emergency call MUST keep state information so that it can recognize and accept a callback from the PSAP if it occurs within a reasonable time after an emergency call was placed, as described in Section 13 of [RFC6443]. Only a timer started at the time when the original emergency call has ended is required; information about the calling party identity is not needed since the callback may use a different calling party identity, as described in Section 3. Since these SIP UA considerations are described already in [RFC6443] as well as in [RFC6881] the rest of this section focuses on the behavior of SIP proxies.

Figure 7 shows the architecture that utilizes the identity of the PSAP to decide whether a preferential treatment of callbacks should be provided. To make this policy decision, the identity of the PSAP (i.e., calling party identity) is compared with a PSAPs white list.

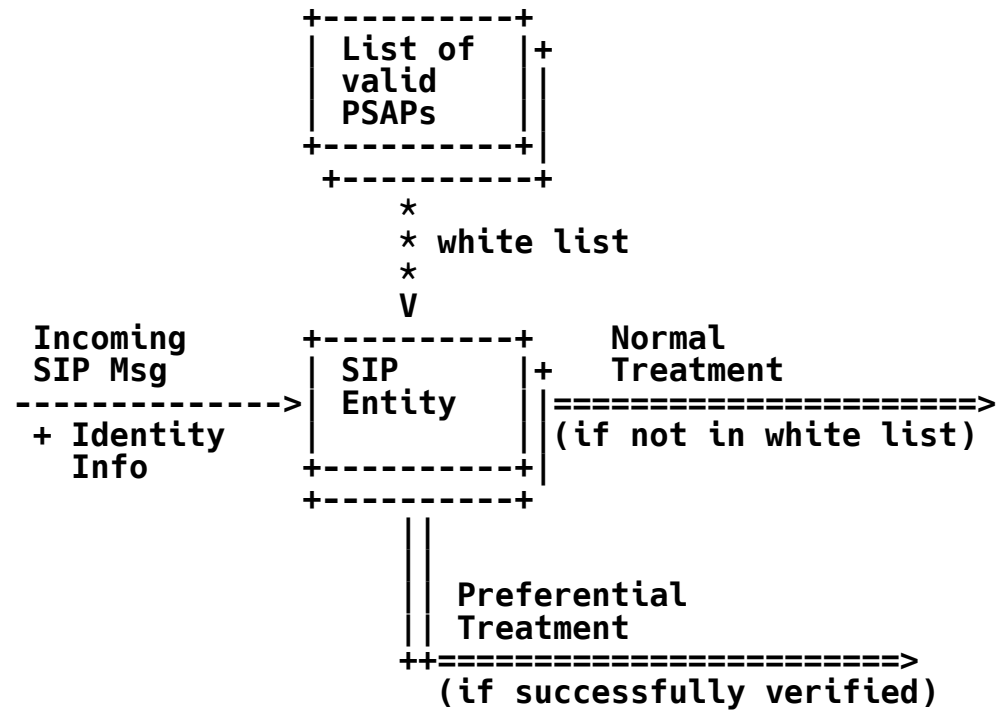

Figure 7: Identity-Based Authorization

The identity assurance in SIP can come in different forms, namely via the SIP Identity [RFC4474] or the P-Asserted-Identity [RFC3325] mechanisms. The former technique relies on a cryptographic assurance and the latter on a chain of trust. Also, the usage of Transport Layer Security (TLS) between neighboring SIP entities may provide useful identity information. At the time of writing, these identity technologies are being revised in the Secure Telephone Identity Revisited (stir) working group [STIR] to offer better support for legacy technologies interworking and SIP intermediaries that modify the content of various SIP headers and the body. Once the work on these specifications has been completed, they will offer a stronger calling party identity mechanism that limits or prevents identity spoofing.

An important aspect from a security point of view is the relationship between the emergency services network (containing the PSAPs) and the VoIP provider, assuming that the emergency call travels via the VoIP provider and not directly between the SIP UA and the PSAP.

The establishment of a white list with PSAP identities may be operationally complex and dependent on the relationship between the emergency services operator and the VoIP provider. If there is a relationship between the VoIP provider and the PSAP operator, for

example, when they are both operating in the same geographical region, then populating the white list is fairly simple and consequently the identification of a PSAP callback is less problematic compared to the case where the two entities have never interacted with each other before. In the end, the VoIP provider has to verify whether the marked callback message indeed came from a legitimate source.

VoIP providers MUST only give PSAP callbacks preferential treatment when the calling party identity of the PSAP was successfully matched against entries in the white list. If it cannot be verified (because there was no match), then the VoIP provider MUST remove the PSAP callback marking. Thereby, the callback reverts to a normal call. As a second step, SIP UAs MUST maintain a timer that is started with the original emergency call and this timer expires within a reasonable amount of time, such as 30 minutes per [RFC6881]. Such a timer also ensures that VoIP providers cannot misuse the PSAP callback mechanism, for example, to ensure that their support calls reach their customers.

Finally, a PSAP callback MUST use the same media as the original emergency call. For example, when an initial emergency call established a real-time text communication session, then the PSAP callback must also attempt to establish a real-time communication interaction. The reason for this is twofold. First, the person seeking help may have disabilities that prevent them from using certain media and hence using the same media for the callback avoids unpleasant surprises and delays. Second, the emergency caller may have intentionally chosen a certain media and does not prefer to communicate in a different way. For example, it would be unfortunate if a hostage tries to seek help using instant messaging to avoid any noise when subsequently the ringtone triggered by a PSAP callback using a voice call gets the attention of the hostage-taker. User-interface designs need to cater to such situations.

6. IANA Considerations

This document adds the "psap-callback" value to the SIP "Priority Header Field Values" registry allocated by [RFC6878]. The semantic of the newly defined "psap-callback" value is defined in Section 4.

7. Acknowledgements

We would like to thank the following persons for their feedback: Bernard Aboba, Andrew Allen, John-Luc Bakker, Kenneth Carlberg, Martin Dolly, Keith Drage, Timothy Dwight, John Elwell, Janet Gunn, Cullen Jennings, Hadriel Kaplan, Paul Kyzivat, John Medland, Atle Monrad, James Polk, Dan Romascanu, Brian Rosen, Robert Sparks, Geoff Thompson, and Martin Thomson.

We would also like to thank the ECRIT working group chairs, Marc Linsner and Roger Marshall, for their support. Roger Marshall was the document shepherd for this document. Vijay Gurbani provided the general area review.

During IESG review, the document received good feedback from Barry Leiba, Spencer Dawkins, Richard Barnes, Joel Jaeggli, Stephen Farrell, and Benoit Claise.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC5234] Crocker, D., Ed., and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[RFC5627] Rosenberg, J., "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)", RFC 5627, October 2009.

[RFC6878] Roach, A., "IANA Registry for the Session Initiation Protocol (SIP) "Priority" Header Field", RFC 6878, March 2013.

8.2. Informative References

[RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

[RFC5012] Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", RFC 5012, January 2008.

[RFC5222] Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol", RFC 5222, August 2008.

[RFC6443] Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling Using Internet Multimedia", RFC 6443, December 2011.

[RFC6881] Rosen, B. and J. Polk, "Best Current Practice for Communications Services in Support of Emergency Calling", BCP 181, RFC 6881, March 2013.

[STIR] IETF, "Secure Telephone Identity Revisited (stir) Working Group", http://datatracker.ietf.org/wg/stir/charter/, October 2013.

Authors' Addresses

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

Hannes Tschofenig

EMail: Hannes.Tschofenig@gmx.net
URI: http://www.tschofenig.priv.at

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

EMail: christer.holmberg@ericsson.com

Milan Patel
Huawei Technologies (UK) Co., Ltd.
300 South Oak Way, Green Park
Reading, Berkshire RG2 6UF
U.K.

EMail: Milan.Patel@huawei.com