

ECRIT
Internet-Draft
Intended status: Standards Track
Expires: June 21, 2013

H. Schulzrinne
Columbia University
H. Tschofenig
Nokia Siemens Networks
C. Holmberg
Ericsson
M. Patel
InterDigital Communications
December 18, 2012

Public Safety Answering Point (PSAP) Callback
draft-ietf-ecrit-psap-callback-07.txt

Abstract

After an emergency call is completed (either prematurely terminated by the emergency caller or normally by the call taker) it is possible that the call taker feels 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 situation of a wounded person. A call taker may trigger a callback towards 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 PSAP callbacks to bypass authorization policies 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.

Note that this version of the document does not yet specify a solution due to the lack of the working group participants agreeing on the requirements.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-

Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on June 21, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	4
2.	Terminology	6
3.	Callback Scenarios	7
3.1.	Routing Asymmetry	7
3.2.	Multi-Stage Routing	8
3.3.	Call Forwarding	9
3.4.	Network-based Service URN Resolution	11
3.5.	PSTN Interworking	12
4.	SIP PSAP Callback Indicator	13
4.1.	General	13
4.2.	Usage	13
4.3.	Syntax	13
4.3.1.	General	13
4.3.2.	ABNF	13
5.	Security Considerations	14
5.1.	Security Threat	14
5.2.	Security Requirements	14
5.3.	Security Solution	14
6.	IANA Considerations	16
7.	Acknowledgements	17
8.	References	18
8.1.	Normative References	18
8.2.	Informative References	19

1. Introduction

Summoning police, the fire department or an ambulance in emergencies is one of the fundamental and most-valued 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, which are not traditional telephones, and 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 are described in [\[RFC6444\]](#) and [\[I-D.ietf-ecrit-phonebcp\]](#) 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 (GRUU). [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.) which are all referenced by the same AOR. There are a number of cases in which it is desirable to have an identifier which 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, which is still globally routable. [RFC 5627](#) [\[RFC5627\]](#) specifies how to obtain and use GRUUs. [\[I-D.ietf-ecrit-phonebcp\]](#) 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 call back to the emergency caller. This is desirable in those cases where the call got dropped prematurely or when further communication need arises. The AoR and the GRUU serve this purpose.

The communication attempt by the PSAP call taker back to the emergency caller is called '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"(aka 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 the desire to offer PSAP callbacks a treatment such that chances are increased that it reaches the emergency caller. At the same time a design must deal with the negative side-effects of allowing certain calls to 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.

To nevertheless meet the needs from the emergency services community a basic mechanism for preferential treatment of PSAP callbacks was defined in [Section 13 of \[RFC6444\]](#). The specification says:

'A UA may be able to determine a PSAP call back 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 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

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 [[RFC2119](#)].

Emergency services related terminology is borrowed from [[RFC5012](#)]. This includes terminology like emergency caller, user equipment, and call taker.

3. Callback Scenarios

This section illustrates a number of scenarios where the currently specified solution, as specified in [[I-D.ietf-ecrit-phonebcp](#)], for preferential treatment of callbacks fails. As explained in [Section 1](#) a SIP entity examines an incoming PSAP call back by comparing the domain of the PSAP with the destination domain of the emergency call.

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 VoIP provider uses different SIP proxies for inbound and for outbound call handling. Unless they two devices are state synchronized the callback hitting the inbound proxy would get treated like any other call since the emergency call established state information at the outbound proxy only.

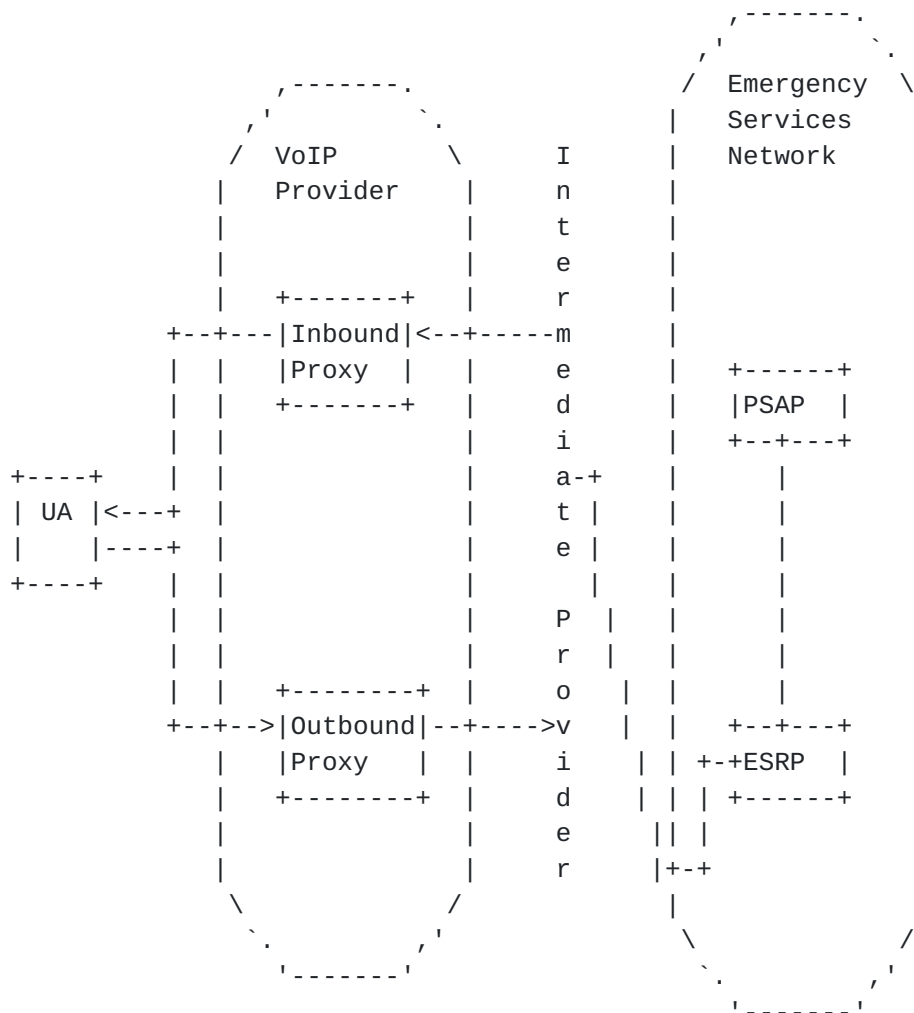


Figure 1: Example for Routing Asymmetry

3.2. Multi-Stage Routing

Consider the following 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 LoST to learn the next hop destination closer to the PSAP. This call is then sent to the user's VoIP provider. The user's VoIP provider receives the emergency call and creates state based on the destination domain, namely state.com. It then routes it to the indicated ESRP. When the ESRP receives it it needs to decide what the next hop is to get it closer to the PSAP. In our example the next hop is the PSAP with the URI psap@town.com.

When a callback is sent from psap@town.com towards the emergency caller the call will get normal treatment by the VoIP providers inbound proxy since the domain of the PSAP does not match the stored

state information.

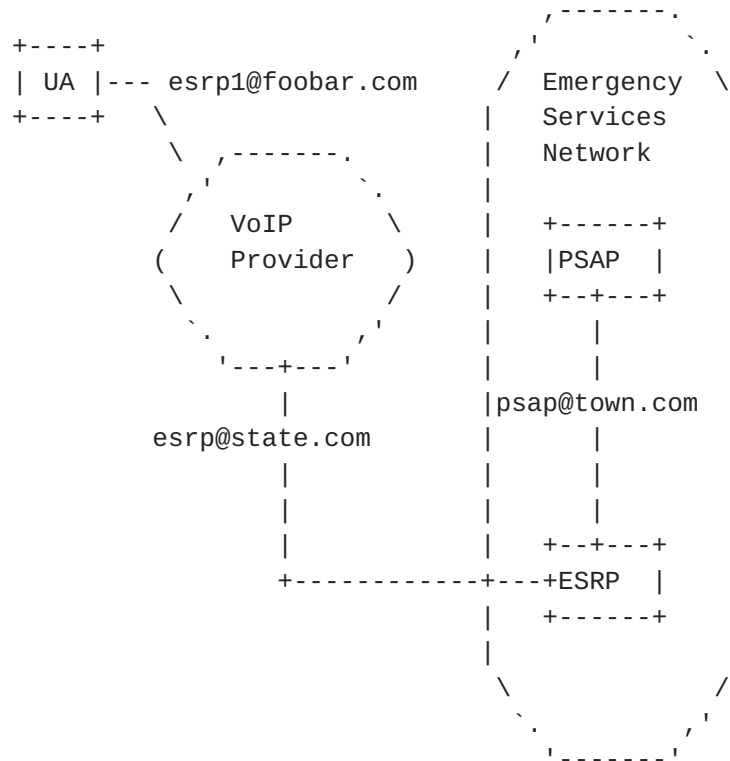


Figure 2: Example for Multi-Stage Routing

3.3. Call Forwarding

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

Similarly to the previous scenario the problem here is with the wrong state information being established during the emergency call setup procedure. A callback would originate in the `police-town.org`, `fire-town.org` or `medic-town.org` domain whereas the emergency caller's SIP UA or the VoIP outbound proxy has stored `state.org`.

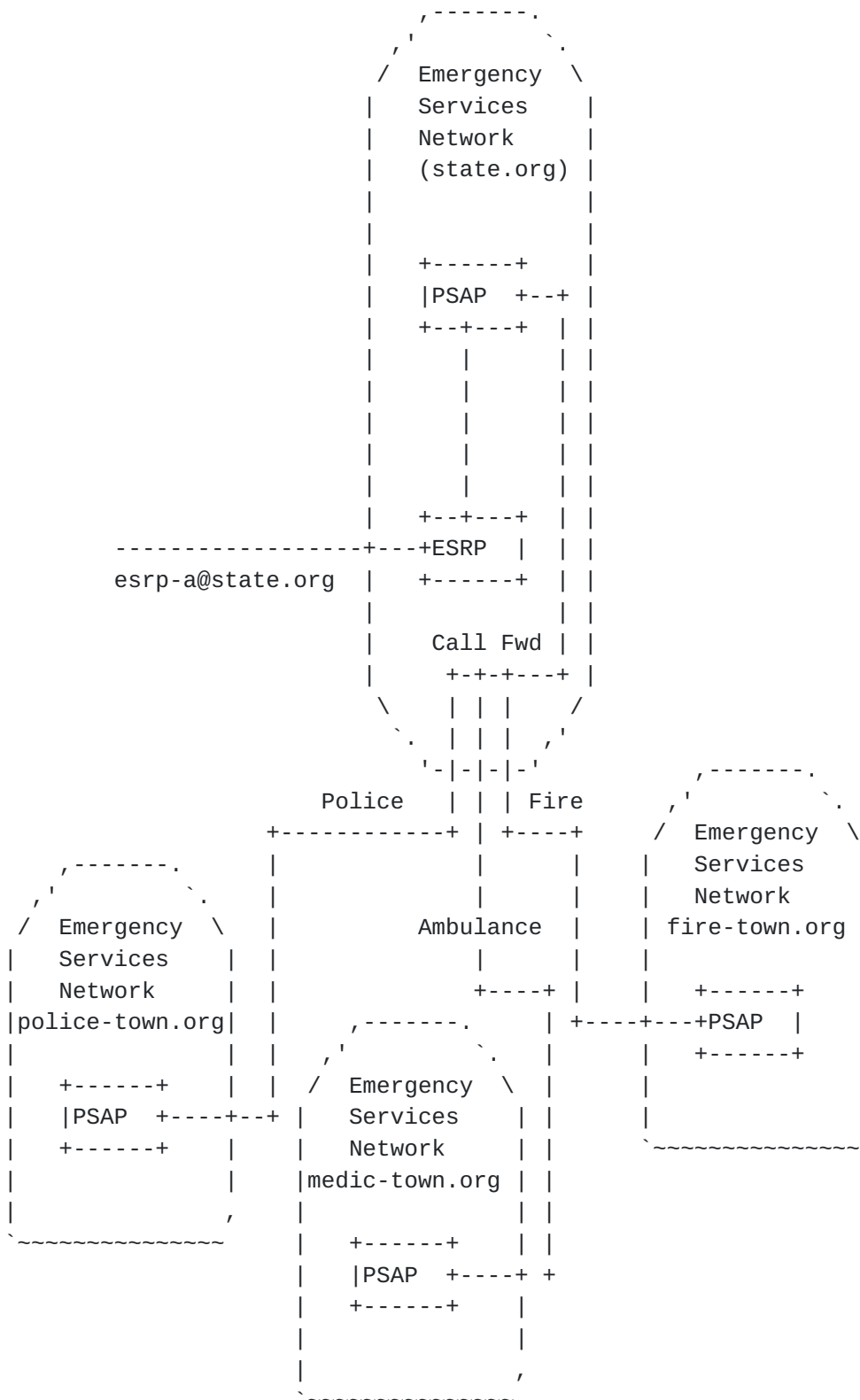


Figure 3: Example for Call Forwarding

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 PSTN, as shown in Figure 5, there is no guarantee that the callback some time later does leave the same PSTN/VoIP gateway or that the same end point identifier is used in the forward as well as in the backward direction making it difficult to reliably detect PSAP callbacks.

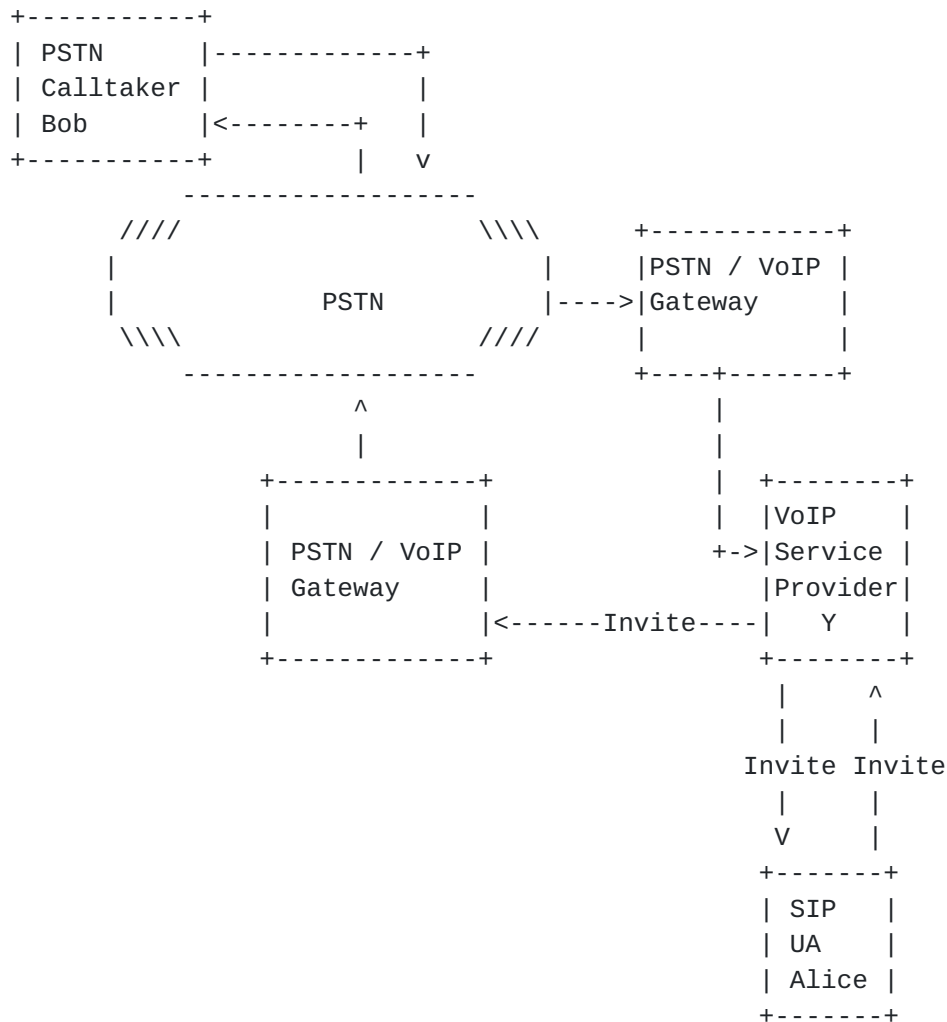


Figure 5: Example for PSTN Interworking

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 procedures taken when receiving such 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 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, ignore call forwarding procedures and similar features to contact emergency callers and to raise their attention. Regarding the latter aspect a callback, if understood by the SIP UA would allow to override user interface configurations, such as vibrate-only mode, to alert the caller of the incoming call.

5.2. Security Requirements

The requirement is to ensure that the mechanisms described in this document can not 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 call must be treated like a call that does not have any marking attached.

5.3. Security Solution

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 is compared with a whitelist of valid PSAPs available to the SIP entity. The identity assurance in SIP can come in different forms, such as SIP Identity [[RFC4474](#)] or with P-Asserted-Identity [[RFC3325](#)]. The former technique relies on a cryptographic assurance and the latter on a chain of trust. Also the usage of TLS between neighboring SIP entities may provide useful identity information.

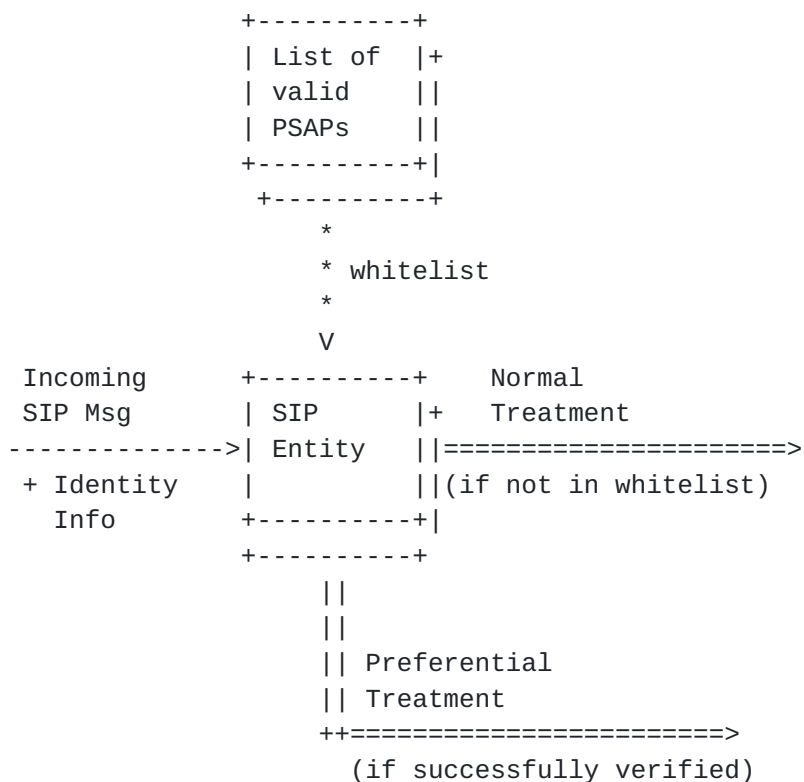


Figure 7: Identity-based Authorization

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

If there is some form of relationship between the emergency services operator and the VSP then the identification of a PSAP call back is less problematic than in the case where the two entities have not entered in some form of relationship that would allow the VSP to verify whether the marked callback message indeed came from a legitimate source.

The establishment of a whitelist with PSAP identities maybe be operationally complex. When there is a local relationship between the VSP/ASP and the PSAP then populating the whitelist is fairly simple. For SIP UAs there is no need to maintain a list of PSAPs. Instead SIP UAs are assumed to trust the correct processing of their VSP/ASP, i.e., the VSP/ASP processes the PSAP callback marking and, if it cannot be verified, the PSAP callback marking is removed. If it is left untouched then the SIP UA should assume that it has been verified successfully by the VSP/ASP and it should therefore be obeyed.

6. IANA Considerations

This document adds the "psap-callback" value to the SIP Priority header IANA registry allocated by [[I-D.ietf-sipcore-priority](#)]. The semantic of the newly defined "psap-callback" value is defined in [Section 4](#).

7. Acknowledgements

We would like to thank members from the ECRIT working group, in particular Brian Rosen, for their discussions around PSAP callbacks. The working group discussed the topic of callbacks at their virtual interim meeting in February 2010 and the following persons provided valuable input: John Elwell, Bernard Aboba, Cullen Jennings, Keith Drage, Marc Linsner, Roger Marshall, Dan Romascanu, Geoff Thompson, Janet Gunn.

At IETF#81 a small group of people got together to continue the discussions started at the working group meeting to explore a GRUU-based solution approach. Martin Thomson, Marc Linsner, Andrew Allen, Brian Rosen, Martin Dolly, and Atle Monrad participated at this side-meeting.

We would like to thank the following persons for their feedback on the solution discussion in 2012: Paul Kyzivat, Martin Thomson, Robert Sparks, Keith Drage, Brian Rosen, Roger Marshall, Martin Dolly, Bernard Aboba, Andrew Allen, John-Luc Bakker, James Polk, John Medland, Hadriel Kaplan, Kenneth Carlberg, Timothy Dwight, Janet Gunn

8. References

8.1. Normative References

- [I-D.ietf-sipcore-priority] Roach, A., "IANA Registry for the Session Initiation Protocol (SIP) "Priority" Header Field", [draft-ietf-sipcore-priority-00](#) (work in progress), December 2012.
- [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.
- [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.
- [RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", [RFC 3966](#), December 2004.
- [RFC3969] Camarillo, G., "The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)", [BCP 99](#), [RFC 3969](#), December 2004.
- [RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", [RFC 4474](#), August 2006.
- [RFC5627] Rosenberg, J., "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)", [RFC 5627](#), October 2009.

8.2. Informative References

- [I-D.ietf-ecrit-phonebcf] Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling", [draft-ietf-ecrit-phonebcf-20](#) (work in progress), September 2011.
- [RFC4484] Peterson, J., Polk, J., Sicker, D., and H. Tschofenig, "Trait-Based Authorization Requirements for the Session Initiation Protocol (SIP)", [RFC 4484](#), August 2006.
- [RFC5012] Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", [RFC 5012](#), January 2008.
- [RFC5031] Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", [RFC 5031](#), January 2008.
- [RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, [RFC 5234](#), January 2008.
- [RFC6444] Schulzrinne, H., Liess, L., Tschofenig, H., Stark, B., and A. Kuett, "Location Hiding: Problem Statement and Requirements", [RFC 6444](#), January 2012.

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
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
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
InterDigital Communications

EMail: Milan.Patel@interdigital.com

