SIPCORE
Internet-Draft
Intended status: Standards Track
Expires: September 8, 2017

H. Schulzrinne
FCC

March 7, 2017

SIP Call-Info Parameters for Labeling Calls
draft-ietf-sipcore-callinfo-spam-00

Abstract

Called parties often wish to decide whether to accept, reject or redirect calls based on the likely nature of the call. For example, they may want to reject unwanted telemarketing or fraudulent calls, but accept emergency alerts from numbers not in their address book. This document describes SIP Call-Info parameters and a feature tag that allow originating, intermediate and terminating SIP entities to label calls as to their type, spam probability and references to additional information.

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 September 8, 2017.

Table of Contents

1. Introduction

In many countries, an increasing number of calls are unwanted [RFC5039], as they might be fraudulent, telemarketing or the receiving party does not want to be disturbed by, say, surveys or solicitation by charities. Currently, called parties have to rely exclusively on the caller’s number or, if provided, caller name, but unwanted callers may not provide their true name or use a name that misleads, e.g., "Cardholder Services". On the other hand, many calls from unknown numbers may be important to the called party, whether this is an emergency alert from their emergency management office or a reminder about a doctor’s appointment. Since many subscribers now reject all calls from unknown numbers, such calls may also be inadvertently be left unanswered. Users may also install smartphone apps that can benefit from additional information in making decisions as to whether to ring, reject or redirect a call.

To allow called parties to make more informed decisions on how to handle incoming calls from unknown callers, we describe a new set of parameters for the SIP [RFC3261] Call-Info header field for labeling the nature of the call.

Providers may also find the SIP Priority header (Section 20.26) field useful in helping called parties decide how to respond to an incoming call.

2. Normative Language

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 BCP 14, RFC 2119 [RFC2119].

3. Overview of Operation

This document describes a new set of optional parameters and usage for the SIP [RFC3261] Call-Info header field, purpose "info", for labeling the nature of the call. The header field may be inserted by the call originator, an intermediate proxy or B2BUA or the terminating carrier, based on assertions by the caller, number-indexed databases, call analytics or other sources of information. The SIP provider serving the called party MUST remove any parameters enumerated in this specification that it does not trust. The Call-Info header field MAY be signed using a future "ppt" extension to [I-D.ietf-stir-rfc4474bis]. To ensure that an untrusted originating caller does not mislead the called party, a new feature tag, sip.call-info.spam, indicates whether the terminating carrier will remove untrusted information.

SIP entities MUST add a new Call-Info "info" header field instance, rather than add parameters to an existing one. Thus, there MAY be several Call-Info header fields of purpose "info" in one request.

As defined in [RFC3261], the Call-Info header field contains a URI that can provide additional information about the caller or call. For example, many call filtering services provide a web page with crowd-sourced information about the calling number. If the entity inserting the header field does not have information it wants to link to, it MUST use an empty data URL [RFC2397] as a placeholder, as in "data:". (The Call-Info header field syntax makes the URI itself mandatory.)

4. Parameters

All of the parameters listed below are optional and may appear in any combination and order. Their ABNF is defined in Section 7.

spam The spam parameter carries an estimated probability that the call will not be wanted by the called party, expressed as a whole-number percentage between 0 and 100, inclusive, with larger

numbers indicating higher probability. The computation of the estimate is beyond the scope of this specification. If not specified, the entity inserting the Call-Info information is making no claims about the likelihood of being unwanted. Note that call types other than "spam" may have a non-zero spam rating, as these calls may also be unwanted by some fraction of the recipients, even if they are not illegal in a particular jurisdiction.

type The type parameter indicates the type of the call or caller. It is drawn from an extensible set of values, with the initial set listed below. Gateways to analog phone systems MAY include the label in caller name (CNAM) information. Automated call classification systems MAY use this information as one factor in deciding how to handle the call. Calls SHOULD be labeled with types that may make it more likely that the caller will answer (e.g., for alert and health-related calls) if the entity inserting the information is confident that the calling party number is valid, e.g., because the request has been signed [I-D.ietf-stir-rfc4474bis].

reason The reason parameter provides free-text information, as a string, about the source of the type or spam parameter and is meant to be used for debugging, rather than for display to the end user. For example, it may indicate the name of an external information source, such as a list of known emergency alerters.

source The source parameter identifies the entity, by host name, domain or IP address, that inserted the parameters above. It uses the "host" ABNF syntax.

5. Call Types

The following initial set of types are defined. The call types are generally based on the caller’s telephone number or possibly an assertion by a trusted caller, as the content cannot be not known. Each call is tagged with at most one type label, i.e., the labels are meant to be mutually exclusive. The definitions are meant to be informal and reflect the common understanding of subscribers who are not lawyers. By their very nature, this classification may sometimes be erroneous, e.g., if a number has been re-assigned to another entity or if crowd-sourced information is wrong, and thus should be treated as a hint or estimate. Each entity inserting type information will need to define its own policy as to the level of certainty it requires before it inserts type information.

Other strings may be used; there does not appear to be a need for defining vendor-defined strings as the likelihood of confusion

between a service-provider-specific usage and a later extension to the list appears low. Additional labels are registered with IANA.

business Calls placed by businesses, i.e., an entity or enterprise entered into for profit. This type is used if no other, more precise, category fits.

debt-collection Calls related to collecting of debt owed or alleged to be owed by the called party.

emergency-alert Calls that provide the recipient warnings and alerts regarding a pending or on-going emergency. (This call type is unrelated to emergency calls placed by individuals using emergency numbers such as 9-1-1 or 1-1-2.)

fraud The call is considered to be fraudulent.

government A call placed by a government entity, if no more specific label such as "health" or "debt-collection" is known or applies.

health Informational calls by health plans, health care clearinghouses or health care provider, where health care means care, services, or supplies related to the health of an individual.

informational Calls intended to convey information to the called party about a transaction such as package delivery, appointment reminder, order confirmation. This call type is only used if the calling party believes to have an established business relationship with the called party.

not-for-profit A call placed by a not-for-profit organization, including for soliciting donations or providing information.

personal A non-business, person-to-person, call, e.g., from a residential line or personal mobile number.

political Calls related to elections or other political purposes.

public-service Calls that provide the recipient information regarding public services, e.g., school closings.

prison Calls from jails, prisons and other correctional facilities.

spam A call that is likely unwanted, if not otherwise classified.

spoofed The calling number for this call has been spoofed.

survey A call that solicits the opinions or data of the called party.

telemarketing Calls placed in order to induce the purchase of a product or service to the called party.

trusted The call is being placed by a trusted entity and falls outside the other categories listed. This may include call backs, e.g., from a conferencing service, or messages from telecommunication carriers and utilities.

6. Example

```
"Call-Info: <http://wwww.example.com/5974c8d942f120351143>
;source=carrier.example.com ;purpose=info ;spam=85 ;type=fraud
;reason="FTC list""
```

7. ABNF

```
label-info-params = [ci-spam] / [ci-type] / [ci-source] / [ci-re
ason]
ci-spam = "spam" EQUAL 1*3DIGIT
ci-type = "type" EQUAL ("business" / "debt-collection" / "emerge
ncy-alert" / "fraud" /
                        "government" / "health" / "informational" / "not-for
-profit" /
                        "personal" / "political" / "public-service" / "priso
n" / "spam" /
                        "spoofed" / "survey" / "telemarketing" / "trusted" /
                        iana-token)
ci-source = "source" EQUAL host
ci-reason = "reason" EQUAL quoted-string
```

8. IANA Considerations

8.1. SIP Call-Info Header Field Parameters

This document defines the 'spam', 'type', 'reason' and 'source' parameters in the Call-Info header in the "Header Field Parameters and Parameter Values" registry defined by [RFC3968].

Header Field	Parameter Name	Predefined Values	Reference
Call-Info	reason	No	[this RFC]
Call-Info	source	No	[this RFC]
Call-Info	spam	No	[this RFC]
Call-Info	type	Yes	[this RFC]

8.2. SIP Global Feature-Capability Indicator

This document defines the feature capability sip.call-info.spam in the "SIP Feature-Capability Indicator Registration Tree" registry defined in [RFC6809].

Name sip.call-info.spam

Description This feature-capability indicator when used in a REGISTER response indicates that the server will add, inspect, alter and possibly remove the Call-Info header field parameters defined in the reference.

Reference [this RFC]

8.3. SIP Call-Info Type Parameter

This specification establishes the "Call-Info Type" sub-registry under http://www.iana.org/assignments/sip-parameters. Call-Info "type" parameters are used in the "type" parameter in the SIP Call-Info header field. The initial values are listed in Section 5. Additional values are allocated by expert review [RFC5226]; only the token value, using the ABNF iana-token, and a brief description, typically no more than a few sentences, is required. The ABNF for iana-token is defined in [RFC3261]. A specification is not required.

9. Security Considerations

The security considerations in [RFC3261] (Section 20.9) apply. A user agent MUST ignore the parameters defined in this document unless the SIP REGISTER response contained the sip.call-info.spam feature capability. SIP entities MUST remove any parameters defined here that were provided by untrusted third parties.

The protection offered against rogue SIP entities by the feature capability relies on protecting the REGISTER response against man-in-the-middle attacks that maliciously add the capability indicator.

10. Acknowledgements

Jim Calme and other members of the Robocall Strikeforce helped draft the initial list of call types. Keith Drage and Paul Kyzivat provided helpful comments on the document.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2397] Masinter, L., "The "data" URL scheme", RFC 2397, DOI 10.17487/RFC2397, August 1998, <http://www.rfc-editor.org/info/rfc2397>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC3968] Camarillo, G., "The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)", BCP 98, RFC 3968, DOI 10.17487/RFC3968, December 2004, <http://www.rfc-editor.org/info/rfc3968>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC6809] Holmberg, C., Sedlacek, I., and H. Kaplan, "Mechanism to Indicate Support of Features and Capabilities in the Session Initiation Protocol (SIP)", RFC 6809, DOI 10.17487/RFC6809, November 2012, <http://www.rfc-editor.org/info/rfc6809>.

11.2. Informative References

[I-D.ietf-stir-rfc4474bis] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-stir-rfc4474bis-16 (work in progress), February 2017.

[RFC5039] Rosenberg, J. and C. Jennings, "The Session Initiation Protocol (SIP) and Spam", RFC 5039, DOI 10.17487/RFC5039, January 2008, <http://www.rfc-editor.org/info/rfc5039>.

Author's Address

Henning Schulzrinne
FCC
445 12th Street SW
Washington, DC 20554
US

Email: henning.schulzrinne@fcc.gov

SIPCORE Working Group
Internet-Draft
Updates: 5621 (if approved)
Intended status: Standards Track
Expires: December 7, 2017

C. Holmberg
I. Sedlacek
Ericsson

June 5, 2017

Content-ID header field in Session Initiation Protocol (SIP)
draft-ietf-sipcore-content-id-06

Abstract

This document specifies the Content-ID header field for usage in the Session Initiation Protocol (SIP). The document also updates RFC 5621, to enable a Content-ID URL to reference a complete message-body and metadata provided by some additional SIP header fields.

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 December 7, 2017.

Copyright Notice

Table of Contents

1. Introduction

1.1. Identifying a body part

A SIP message consists of a start-line, one or more header fields, an empty line indicating the end of the header fields, and an optional message-body, as specified in [RFC3261].

The message-body can be a non-multipart message-body or a multipart message-body as specified in [RFC3261].

[RFC5621] defines generic handling of a multipart message-body in a SIP message.

A multipart message-body contains zero, one or several body parts, encoded using [RFC2045] format.

A body part in the multipart message-body is described using header fields such as Content-Disposition, Content-Encoding, and Content-Type, which provide information on the content of the body part, as specified in [RFC5621]. A body part in the multipart message-body

can also contain a Content-ID header field with an ID value uniquely identifying the body part, as specified in [RFC2045].

1.2. Referencing a body part

A SIP header field can reference a body part using a Content-ID URL, as specified in [RFC5621].

The Content-ID URL is specified in [RFC2392]. [RFC2392] specifies how to identify the body part referenced by a Content-ID URL. The Content-ID URL value is included in the Content-ID header field of the body part.

Examples of SIP header fields referencing a body part using a Content-ID URL are:

- [RFC6442] specifies how a Geolocation header field references a body part using a Content-ID URL, for providing location.
- [RFC5368] specifies how a Refer-To header field references a body part using a Content-ID URL, to provide a list of targets.

1.3. Problem statement

It is currently not specified how to uniquely identify a complete message-body of a SIP message using a Content-ID header field, and how to reference a complete message-body using a Content-ID URL.

NOTE: In [RFC5621], the Content-ID URL references a specific body part only.

1.4. Consequences

The examples below shows the consequences of the problem described above.

1.4.1. Example 1

If a UAC sends an INVITE request conveying location as specified in [RFC6442], if the UAC decides not to include an SDP offer, and if the location is conveyed by value, then the UAC needs to include only one MIME entity in the INVITE request. This MIME entity can be e.g. of the application/pidf+xml MIME type.

However, due to [RFC6442] requiring inclusion of a Geolocation header field referencing the body part with the location information, the UAC includes a multipart message-body with single body part in the INVITE request, and includes the location information of application/

pidf+xml MIME type and an associated Content-ID header field in the body part.

1.4.2. Example 2

If a UAC sends an REFER request including a list of targets as specified in [RFC5368], then the UAC needs to include only one MIME entity in the REFER request. This MIME entity is of the application/resource-lists+xml MIME type.

However, due to [RFC5368] requiring inclusion of a Refer-To header field referencing the body part containing the list of targets, the UAC includes a multipart message-body with single body part in the REFER request, and includes the list of targets of application/resource-lists+xml MIME type and an associated Content-ID header field in the body part.

1.5. Solution

In order to solve the problems described above, this document:

- Specifies and registers the Content-ID header field as a SIP header field; and
- Specifies that, when used as a SIP header field, the Content-ID header field identifies the complete message-body, and metadata provided by some additional SIP header fields, of the SIP message; and
- Updates [RFC5621], to enable a Content-ID URL to reference a complete message-body and metadata provided by some additional SIP header fields.

2. Conventions

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].

3. Content-ID header field

3.1. Introduction

This section defines the usage of the Content-ID header field for SIP.

3.2. Syntax

The ABNF [RFC5234] for the Content-ID header field is:

```
Content-ID = "Content-ID" HCOLON msg-id

msg-id     = "<" id-left "@" id-right ">"
```

NOTE: id-left and id-right are specified in [RFC5322]. HCOLON is defined in [RFC3261].

NOTE: When used in a SIP header field, the msg-id syntax has been simplified, compared to the syntax in [RFC5322], to disallow the use of comments and to adopt to the SIP usage of leading white space.

The value of Content-Id header field value must be unique in the context of a given SIP message, including any embedded MIME Content-Id header field values. Note that the SIP Content-ID header field value is not expected to be unique among all SIP messages; it has no meaning outside of the message in which it is included.

3.3. Semantics

The Content-ID header field included in the header fields of a SIP message identifies the message-body of the SIP message, and the metadata provided by:

- a MIME-Version header field, if included in the header fields of the SIP message; and
- any 'Content-' prefixed header fields (including the Content-ID header field itself) included in the header fields of the SIP message.

The Content-ID header field can be included in any SIP message which is allowed to contain a message-body.

3.4. Procedures

3.4.1. UA procedures

A UA MAY include a Content-ID header field in any SIP message that is allowed to contain a message-body.

A UA MUST NOT include a Content-ID header field in any SIP message that is not allowed to contain a message-body.

The UA MUST set the value of the Content-ID header field to a globally unique value.

3.4.2. Proxy procedures

A proxy MUST NOT add a Content-ID header field in a SIP message.

A proxy MUST NOT modify a Content-ID header field included in a SIP message.

A proxy MUST NOT delete a Content-ID header field from a SIP message.

3.4.3. Example

The figure shows an example from [RFC5368], where the SIP Content-ID header field is used to reference the message body (non-multipart) of a SIP message.

```
REFER sip:conf-123@example.com;gruu;opaque=hha9s8d-999a  SIP/2.0
Via: SIP/2.0/TCP client.chicago.example.com
        ;branch=z9hG4bKhjhs8ass83
Max-Forwards: 70
To: "Conference 123" <sip:conf-123@example.com>
From: Carol <sip:carol@chicago.example.com>;tag=32331
Call-ID: d432fa84b4c76e66710
CSeq: 2 REFER
Contact: <sip:carol@client.chicago.example.com>
Refer-To: <cid:cn35t8jf02@example.com>
Refer-Sub: false
Require: multiple-refer, norefersub
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Allow-Events: dialog
Accept: application/sdp, message/sipfrag
Content-Type: application/resource-lists+xml
Content-Disposition: recipient-list
Content-Length: 362
Content-ID: <cn35t8jf02@example.com>

<?xml version="1.0" encoding="UTF-8"?>
<resource-lists xmlns="urn:ietf:params:xml:ns:resource-lists"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <list>
    <entry uri="sip:bill@example.com?method=BYE" />
    <entry uri="sip:joe@example.org?method=BYE" />
    <entry uri="sip:ted@example.net?method=BYE" />
  </list>
</resource-lists>
```

4. Update to RFC 5621

This section updates section 9.1 of [RFC5621], by allowing a Content-ID URL to reference a message-body and the related metadata (Section 3.3), in addition to allowing a reference to a body part.

OLD TEXT:

> Content-ID URLs allow creating references to body parts. A given Content-ID URL [RFC2392], which can appear in a header field or within a body part (e.g., in an SDP attribute), points to a particular body part.

NEW TEXT:

> Content-ID URLs allow creating references to body parts or message-bodies (and the header fields describing the message-bodies). A given Content-ID URL [RFC2392], which can appear in a header field or within a body part (e.g., in an SDP attribute), points to a particular body part or the message-body (and the header fields describing the message-body).

5. Security considerations

The Content-ID header field value MUST NOT reveal sensitive user information.

If the message-body associated with the Content-ID header field is an encrypted body, it MUST NOT be possible to derive a key that can be used to decrypt the body from the Content-ID header field value.

6. IANA considerations

This specification registers a new SIP header field according to the procedures in [RFC3261].

6.1. Header field

The header field described in Section 3 has been registered in the "Header Fields" sub-registry of the "Session Initiation Protocol (SIP) Parameters" registry by adding a row with these values:

[RFC EDITOR NOTE: Please replace XXXX with the RFC number of this document when publishing]

Header Name: Content-ID

compact:

Reference: RFCXXXX

7. Change log

[RFC EDITOR NOTE: Please remove this section when publishing]

Changes from draft-ietf-sipcore-content-id-05

- Changes based on AD comments from Ben Campell:
- - Clarifying that Content-ID header field value is unique within the scope of a SIP message.

Changes from draft-ietf-sipcore-content-id-04

- Minor editorial fix.

Changes from draft-ietf-sipcore-content-id-03

- Changes based on doc shepard review:
- - Reference to RFC 5234 added.
- - SIP message example added.
- - Editorial changes.

Changes from draft-ietf-sipcore-content-id-02

- Editorial changes based on comments from Paul Kyzivat.

Changes from draft-ietf-sipcore-content-id-01

- Update to RFC 5621 added.
- Editorial changes.

8. Normative references

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <http://www.rfc-editor.org/info/rfc2045>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2392] Levinson, E., "Content-ID and Message-ID Uniform Resource Locators", RFC 2392, DOI 10.17487/RFC2392, August 1998, <http://www.rfc-editor.org/info/rfc2392>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <http://www.rfc-editor.org/info/rfc5234>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <http://www.rfc-editor.org/info/rfc5322>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC5368] Camarillo, G., Niemi, A., Isomaki, M., Garcia-Martin, M., and H. Khartabil, "Referring to Multiple Resources in the Session Initiation Protocol (SIP)", RFC 5368, DOI 10.17487/RFC5368, October 2008, <http://www.rfc-editor.org/info/rfc5368>.

[RFC5621] Camarillo, G., "Message Body Handling in the Session Initiation Protocol (SIP)", RFC 5621, DOI 10.17487/RFC5621, September 2009, <http://www.rfc-editor.org/info/rfc5621>.

[RFC6442] Polk, J., Rosen, B., and J. Peterson, "Location Conveyance for the Session Initiation Protocol", RFC 6442, DOI 10.17487/RFC6442, December 2011, <http://www.rfc-editor.org/info/rfc6442>.

Authors' Addresses

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: christer.holmberg@ericsson.com

Ivo Sedlacek
Ericsson
Sokolovska 79
Praha 18600
Czech Republic

Email: ivo.sedlacek@ericsson.com

Network Working Group
Internet-Draft
Updates: 3261, 3325, 3515, 3892, 4508, 5002, 5318, 5360, 5502 (if approved)
Intended status: Standards Track
Expires: December 3, 2017

R. Sparks
Oracle

June 01, 2017

Clarifications for when to use the name-addr production in SIP messages
draft-ietf-sipcore-name-addr-guidance-02

Abstract

RFC3261 constrained several SIP header fields whose grammar contains the "name-addr / addr-spec" alternative to use name-addr when certain characters appear. Unfortunately it expressed the constraints with prose copied into each header field definition, and at least one header field was missed. Further, the constraint has not been copied into documents defining extension headers whose grammar contains the alternative.

This document updates RFC3261 to state the constraint generically, and clarifies that the constraint applies to all SIP header fields where there is a choice between using name-addr or addr-spec. It also updates the RFCs that define extension SIP header fields using the alternative to clarify that the constraint applies (RFCs 3325, 3515, 3892, 4508, 5002, 5318, 5360, and 5502).

Table of Contents

1. Introduction

[RFC3261] defines several header fields that contain URIs to allow both a form that contains the bare URI (addr-spec) and one that provides a name and the URI (name-addr). This subset, taken from the ABNF [RFC5234] specified in [RFC3261] shows the relevant part of the definition of the syntax of the "From" header field:

```
From        =  ( "From" / "f" ) HCOLON from-spec
from-spec   =  ( name-addr / addr-spec )
               *( SEMI from-param )
name-addr       =  [ display-name ] LAQUOT addr-spec RAQUOT
addr-spec       =  SIP-URI / SIPS-URI / absoluteURI
```

The prose in section 20.20 of [RFC3261], which discusses the "From" header field, constrains how the production may be used by saying:

> Even if the "display-name" is empty, the "name-addr" form MUST be used if the "addr-spec" contains a comma, question mark, or semicolon.

Section 20.39, which discusses the "To" header field contains no such constraining text.

This constraint is specified slightly differently, but with the same intent, in the introduction to section 20:

> The Contact, From, and To header fields contain a URI. If the URI contains a comma, question mark or semicolon, the URI MUST be enclosed in angle brackets (< and >).

Unfortunately, this can be read to only apply to the Contact, From, and To header fields, making it necessary to provide the constraint explicitly in the prose discussing any other header field using the name-addr or addr-spec alternative.

As extension header fields were standardized, the specifications sometimes failed to include the constraint. Many errata have been entered to correct this omission. When the constraint was called out, the form has not been consistent.

This memo updates the specifications of SIP and its extensions to clarify that the constraint to use the name-addr form applies anywhere there is a choice between the name-addr and addr-spec production rules in the grammar for SIP header fields.

It is important to note that a message formed without honoring the constraint will still be syntactically valid, but would very likely be interpreted differently. The characters after the comma, question mark, or semicolon will, in most cases, be interpreted as header field parameters or additional header field values as discussed in section 7.3.1 of [RFC3261]. (An exception is the degenerate case of a URL like sip:10.0.0.1,@10.0.0.0 where it is possible to parse the comma via the ’user’ production).

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Updates to RFC3261

This text from the introduction to section 20 of [RFC3261]:

> The Contact, From, and To header fields contain a URI. If the URI contains a comma, question mark or semicolon, the URI MUST be enclosed in angle brackets (< and >). Any URI parameters are contained within these brackets. If the URI is not enclosed in angle brackets, any semicolon-delimited parameters are header-parameters, not URI parameters.

is replaced with:

> When constructing the value of any SIP header field whose grammar allows choosing between name-addr and addr-spec, such as those that use the form '(name-addr / addr-spec)', the "addr-spec" form MUST NOT be used if its value would contain a comma, semicolon, or question mark.
>
> When a URI appears in such a header field, any URI parameters MUST be contained within angle brackets (< and >). If the URI is not enclosed in angle brackets, any semicolon-delimited parameters are header-parameters, not URI parameters.
>
> The header fields defined in this specification that allow this choice are "To", "From", "Contact", and "Reply-To".

4. Updates to RFCs defining SIP Extension header fields

The following standards track RFCs: [RFC3515], [RFC3892], [RFC4508], and [RFC5360]

and the following informational RFCS: [RFC3325], [RFC5002], [RFC5318], and [RFC5502]

are updated to include:

> This RFC contains the definition of one or more SIP header fields that allow choosing between addr-spec and name-addr when constructing header field values. As specified in RFCxxxx, the "addr-spec" form MUST NOT be used if its value would contain a comma, semicolon, or question mark.

The status of the Informational RFCs remains Informational.

5. IANA Considerations

This memo has no considerations for IANA.

6. Security Considerations

The updates specified in this memo clarify a constraint on the grammar for producing SIP messages. It introduces no new security considerations. One pre-existing consideration is worth reiterating: messages produced without honoring the constraint will very likely be mis-interpreted by the receiving element.

7. Acknowledgments

Brett Tate identified this issue in several extension documents, submitted several corresponding errata, and drove the discussion that led to this memo. Substantive comments leading to this text were provided by Paul Kyzivat, Gonzalo Camarillo, Dale Worley, and Yehoshua Gev.

8. Instructions to the RFC Editor

Please remove this section in its entirety before publication as an RFC.

Please replace any instances of RFCxxxx with the RFC number assigned to this memo.

This memo, if it is approved, obviates Errata 3744, 3894, and 4648-4652 inclusive.

9. Normative References

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <http://www.rfc-editor.org/info/rfc5234>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <http://www.rfc-editor.org/info/rfc8174>.

[RFC3515] Sparks, R., "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, DOI 10.17487/RFC3515, April 2003, <http://www.rfc-editor.org/info/rfc3515>.

[RFC3892] Sparks, R., "The Session Initiation Protocol (SIP) Referred-By Mechanism", RFC 3892, DOI 10.17487/RFC3892, September 2004, <http://www.rfc-editor.org/info/rfc3892>.

[RFC4508] Levin, O. and A. Johnston, "Conveying Feature Tags with the Session Initiation Protocol (SIP) REFER Method", RFC 4508, DOI 10.17487/RFC4508, May 2006, <http://www.rfc-editor.org/info/rfc4508>.

[RFC5360] Rosenberg, J., Camarillo, G., Ed., and D. Willis, "A Framework for Consent-Based Communications in the Session Initiation Protocol (SIP)", RFC 5360, DOI 10.17487/RFC5360, October 2008, <http://www.rfc-editor.org/info/rfc5360>.

[RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, DOI 10.17487/RFC3325, November 2002, <http://www.rfc-editor.org/info/rfc3325>.

[RFC5002] Camarillo, G. and G. Blanco, "The Session Initiation Protocol (SIP) P-Profile-Key Private Header (P-Header)", RFC 5002, DOI 10.17487/RFC5002, August 2007, <http://www.rfc-editor.org/info/rfc5002>.

[RFC5318] Hautakorpi, J. and G. Camarillo, "The Session Initiation Protocol (SIP) P-Refused-URI-List Private-Header (P-Header)", RFC 5318, DOI 10.17487/RFC5318, December 2008, <http://www.rfc-editor.org/info/rfc5318>.

[RFC5502] van Elburg, J., "The SIP P-Served-User Private-Header (P-Header) for the 3GPP IP Multimedia (IM) Core Network (CN) Subsystem", RFC 5502, DOI 10.17487/RFC5502, April 2009, <http://www.rfc-editor.org/info/rfc5502>.

Author’s Address

Robert Sparks
Oracle

Email: rjsparks@nostrum.com

SIPCORE
Internet-Draft
Intended status: Standards Track
Expires: November 9, 2017

H. Schulzrinne
FCC

May 8, 2017

A SIP Response Code for Unwanted Calls
draft-ietf-sipcore-status-unwanted-06

Abstract

This document defines the 607 (Unwanted) SIP response code, allowing called parties to indicate that the call or message was unwanted. SIP entities may use this information to adjust how future calls from this calling party are handled for the called party or more broadly.

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 November 9, 2017.

Table of Contents

1. Introduction

In many countries, an increasing number of calls are unwanted [RFC5039]: they might be fraudulent, illegal telemarketing or the receiving party does not want to be disturbed by, say, surveys or solicitation by charities. Carriers and other service providers may want to help their subscribers avoid receiving such calls, using a variety of global or user-specific filtering algorithms. One input into such algorithms is user feedback. User feedback may be offered through smartphone apps, APIs or within the context of a SIP-initiated call. This document addresses feedback within the SIP call. Here, the called party either rejects the SIP [RFC3261] request as unwanted or terminates the session with a BYE request after answering the call. INVITE and MESSAGE requests are most likely to trigger such a response.

To allow the called party to express that the call was unwanted, this document defines the 607 (Unwanted) response code. The user agent of the called party, based on input from the called party or some UA-internal logic, uses this to indicate that this call is unwanted and that future attempts are likely to be similarly rejected. While factors such as identity spoofing and call forwarding may make authoritative identification of the calling party difficult or impossible, the network can use such a rejection -- possibly combined with a pattern of rejections by other callees and/or other information -- as input to a heuristic algorithm for determining future call treatment. The heuristic processing and possible treatment of persistently unwanted calls are outside the scope of this document.

As in [I-D.ietf-stir-rfc4474bis], we use the term "caller identity" or "calling party identity" in this document to mean either a

canonical address-of-record (AoR) SIP URI employed to reach a user (such as 'sip:alice@atlanta.example.com'), or a telephone number, which commonly appears in either a tel URI [RFC3966] or as the user portion of a SIP URI.

2. Normative Language

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 BCP 14, RFC 2119 [RFC2119].

3. Motivation

None of the existing 4xx, 5xx or 6xx response codes signify that this SIP request is unwanted by the called party. For example, 603 (Decline) might be used if the called party is currently at dinner or in a meeting, but does not want to indicate any specific reason. As described in Section 21.6.2 [RFC3261], a 603 response may include a Retry-After header field to indicate a better time to attempt the call. Thus, the call is rejected due to the called party's (temporary) status. As described in Section 4, the called party invokes the "unwanted call" user interface and 607 (Unwanted) response indicating that it is instead the caller's identity that is causing the call to be rejected.

4. Behavior of SIP Entities

The response code 607 MAY be used in a failure response for an INVITE, MESSAGE, SUBSCRIBE or other out-of-dialog SIP request to indicate that the offered communication is unwanted. The response code MAY also be used as the value of the "cause" parameter of a SIP reason-value in a Reason header field [RFC3326], typically when the called party user agent issues a BYE request terminating an incoming call or a forking proxy issues a CANCEL request after receiving a 607 response from one of the branches. (Including a Reason header field with the 607 status code allows the called party user agent that receives a CANCEL request to make an informed choice whether and how to include such calls in their missed-call list or whether to show an appropriate indication to the user.)

The SIP entities receiving this response code are not obligated to take any particular action beyond those appropriate for 6xx responses. Following the default handling for 6xx responses in [RFC5057], the 607 response destroys the transaction. The service provider delivering calls or messages to the user issuing the response MAY take a range of actions, for example, add the calling party to a personal blacklist specific to the called party, use the

information as input when computing the likelihood that the calling party is placing unwanted calls ("crowd sourcing"), initiate a traceback request, or report the calling party identity to consumer complaint databases. As discussed in Section Section 6, reversing the 'unwanted' labeling is beyond the scope of this mechanism, as it will likely require a mechanism other than call signaling.

The user experience is envisioned to be somewhat similar to email spam buttons where the detailed actions of the email provider remain opaque to the user.

The mechanism described here is only one of many inputs likely to be used by call filtering algorithms operated by service providers, using data on calls from a particular identifier such as a telephone number to establish handling for future calls from the same identifier. Call handling for unwanted calls is likely to involve a combination of heuristics, analytics, and machine learning. These may use call characteristics such as call duration and call volumes for a particular caller, including changes in those metrics over time, as well as user feedback via non-SIP approaches and the mechanism described here. Implementations will have to make appropriate trade-offs between falsely labeling a caller as unwanted and delivering unwanted calls.

Systems receiving 607 responses could decide to treat pre-call and mid-call responses differently, given that the called party has had access to call content for mid-call rejections.

Depending on the implementation, the response code does not necessarily automatically block all calls from that caller identity. The same user interface action might also trigger addition of the caller identity to a local, on-device blacklist or graylist, e.g., causing such calls to be flagged or alerted with a different ring tone.

The actions described here do not depend on the nature of the SIP URI, e.g., whether it describes a telephone number or not; however, the same anonymous SIP URI [RFC3323] may be used by multiple callers and thus such URIs are unlikely to be appropriate for URI-specific call treatment. SIP entities tallying responses for particular callers may need to consider canonicalzing SIP URIs, including telephone numbers, as described in [I-D.ietf-stir-rfc4474bis]. The calling party may be identified in different locations in the SIP header, e.g., the From header field, P-Asserted-Identity or History-Info, and may also be affected by diverting services.

This document defines a SIP feature-capability [RFC6809], sip.607, that allows the registrar to indicate that the corresponding proxy

supports this particular response code. This allows the UA, for example, to provide a suitable user interface element, such as a "spam" button, only if its service provider actually supports the feature. The presence of the feature capability does not imply that the provider will take any particular action, such as blocking future calls. A UA may still decide to render a "spam" button even without such a capability if, for example, it maintains a device-local blacklist or reports unwanted calls to a third party.

5. IANA Considerations

5.1. SIP Response Code

This document registers a new SIP response code. This response code is defined by the following information, which is to be added to the "Response Codes" sub-registry under http://www.iana.org/assignments/sip-parameters.

Response Code Number 607

Default Reason Phrase Unwanted

Reference [this RFC]

5.2. SIP Global Feature-Capability Indicator

This document defines the feature capability sip.607 in the "SIP Feature-Capability Indicator Registration Tree" registry defined in [RFC6809].

Name sip.607

Description This feature-capability indicator, when included in a Feature-Caps header field of a REGISTER response, indicates that the server supports, and will process, the 607 (Unwanted) response code.

Reference [this RFC]

6. Security Considerations

If the calling party address is spoofed, users may report the caller identity as placing unwanted calls, possibly leading to the blocking of calls from the legitimate user of the caller identity in addition to the unwanted caller, i.e., creating a form of denial-of-service attack. Thus, the response code SHOULD NOT be used for creating global call filters unless the calling party identity has been authenticated using [I-D.ietf-stir-rfc4474bis] as being assigned to

the caller placing the unwanted call. (The creation of call filters local to a user agent is beyond the scope of this document.)

Even if the identity is not spoofed, a call or message recipient might flag legitimate caller identities, e.g., to exact vengeance on a person or business, or simply by mistake. To correct errors, any additions to a personal list of blocked caller identities should be observable and reversible by the party being protected by the blacklist. For example, the list may be shown on a web page or the subscriber may be notified by periodic email reminders. Any additions to a global or carrier-wide list of unwanted callers needs to consider that any user-initiated mechanism will suffer from an unavoidable rate of false positives and tailor their algorithms accordingly, e.g., by comparing the fraction of delivered calls for a particular caller that are flagged as unwanted rather than just the absolute number, and considering time-weighted filters that give more credence to recent feedback.

If an attacker on an unsecured network can spoof SIP responses for a significant number of call recipients, it may be able to convince the call filtering algorithm to block legitimate calls. Use of TLS to protect signaling mitigates against this risk.

Since caller identities are routinely re-assigned to new subscribers, algorithms are advised to consider whether the caller identity has been re-assigned to a new subscriber and possibly reset any related rating. (In some countries, there are services that track which telephone numbers have been disconnected before they are re-assigned to a new subscriber.)

Some call services such as 3PCC [RFC3725] and call transfer [RFC5359] increase the complexity of identifying who (if anyone) should be impacted by the receipt of 607 within BYE. Such services might cause the wrong party to be flagged or prevent flagging the desired party.

For both individually-authenticated and unauthenticated calls, recipients of response code 607 may want to distinguish responses sent before and after the call has been answered, ascertaining whether either response timing suffers from a lower false-positive rate.

7. Acknowledgements

Tolga Asveren, Ben Campbell, Peter Dawes, Spencer Dawkins, Martin Dolly, Keith Drage, Vijay Gurbani, Christer Holmberg, Olle Johansson, Paul Kyzivat, Jean Mahoney, Marianne Mohali, Adam Montville, Al Morton, Denis Ovsienko, Brian Rosen, Brett Tate, Chris Wendt, Dale Worley and Peter Yee (Gen-ART reviewer) provided helpful comments.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC3326] Schulzrinne, H., Oran, D., and G. Camarillo, "The Reason Header Field for the Session Initiation Protocol (SIP)", RFC 3326, DOI 10.17487/RFC3326, December 2002, <http://www.rfc-editor.org/info/rfc3326>.

[RFC6809] Holmberg, C., Sedlacek, I., and H. Kaplan, "Mechanism to Indicate Support of Features and Capabilities in the Session Initiation Protocol (SIP)", RFC 6809, DOI 10.17487/RFC6809, November 2012, <http://www.rfc-editor.org/info/rfc6809>.

8.2. Informative References

[I-D.ietf-stir-rfc4474bis] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-stir-rfc4474bis-16 (work in progress), February 2017.

[RFC3323] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, DOI 10.17487/RFC3323, November 2002, <http://www.rfc-editor.org/info/rfc3323>.

[RFC3725] Rosenberg, J., Peterson, J., Schulzrinne, H., and G. Camarillo, "Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)", BCP 85, RFC 3725, DOI 10.17487/RFC3725, April 2004, <http://www.rfc-editor.org/info/rfc3725>.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, DOI 10.17487/RFC3966, December 2004, <http://www.rfc-editor.org/info/rfc3966>.

[RFC5039] Rosenberg, J. and C. Jennings, "The Session Initiation Protocol (SIP) and Spam", RFC 5039, DOI 10.17487/RFC5039, January 2008, <http://www.rfc-editor.org/info/rfc5039>.

[RFC5057] Sparks, R., "Multiple Dialog Usages in the Session Initiation Protocol", RFC 5057, DOI 10.17487/RFC5057, November 2007, <http://www.rfc-editor.org/info/rfc5057>.

[RFC5359] Johnston, A., Ed., Sparks, R., Cunningham, C., Donovan, S., and K. Summers, "Session Initiation Protocol Service Examples", BCP 144, RFC 5359, DOI 10.17487/RFC5359, October 2008, <http://www.rfc-editor.org/info/rfc5359>.

Author’s Address

Henning Schulzrinne
FCC
445 12th Street SW
Washington, DC 20554
US

Email: henning.schulzrinne@fcc.gov

SIPCORE
Internet-Draft
Updates: RFC6442 (if approved)
Intended status: Standards Track
Expires: August 19, 2017

J. Winterbottom
Winterb Consulting Services
R. Jesske
Deutsche Telekom
B. Chatras
Orange Labs
A. Hutton
Unify

February 15, 2017

Location Source Parameter for the SIP Geolocation Header Field
draft-winterbottom-sipcore-locparam-00.txt

Abstract

There are some circumstances where a geolocation header field may contain more than one location value. Knowing the identity of the node adding the location value allows the recipient more freedom in selecting the value to look at first rather than relying solely on the order of the location values.

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 August 19, 2017.

Copyright Notice

Table of Contents

1. Introduction

The SIP geolocation specification [RFC6442] describes a SIP header field that is used to indicate that the SIP message is conveying location information. The specification suggests that only one location value should be conveyed. However, some communications architectures, such as 3GPP [TS23-167] and ETSI [M493], prefer to use information provided by edge-proxies or acquired through the use of core-network nodes, before using information provided solely by user equipment (UE). These solutions don't preclude the use of UE provided location but require a means of being able to distinguish the identity of the node adding the location value to the SIP message from that provided by the UE. [RFC6442] stipulates that the order of location values in the geolocation header field aligns with the order in which they were added to the header field. Whilst this order provides guidance to the recipient as to which values were added to the message earlier in the communication chain, it does not provide any indication of which node actually added the location value. Knowing the identity of the entity that added the location to the message allows the recipient to choose which location to consider first rather than relying solely on the order of the location values in the geolocation header field.

This document adds a location-source (loc-src) parameter to the location values in [RFC6442] so that the entity adding the location value to geolocation header field can identify itself using its hostname. How the entity adding the location value to the header field obtains the location information is out of scope of this document.

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].

3. Rationale

The primary intent of the parameter defined in this specific is for use in emergency calling. There are various architectures defined for providing emergency calling using SIP-based messaging. Each has it own characteristics with corresponding pros and cons. All of them allow the UE to provide location information, however, many also attach other sources of location information to support veracity checks, provide backup information, or to be used as the primary location. This document makes no attempt to comment on these various architectures or the rationale for them wishing to include multiple location values. It does recognize that these architectures exist

and that there is a need to identify the entity adding the location information.

The parameter defined in this specification adds the location source generating the location value to increase the trustworthiness of the location information. Thus it is intended to use this parameter in trust domains where Spec(T) as described in [RFC3325] exists only. The functional architecture described within ETSI [M493] is an example of architecture where this parameter makes sense to be used.

4. Mechanism

The mechanism employed adds a parameter to the location value defined in [RFC6442] that identifies the hostname of the entity adding the location value to the geolocation header field. The Augmented BNF (ABNF) [RFC5234] for this parameter is shown in Figure 1.

```
location-source = "loc-src=" (host / other-loc-src)
other-loc-src = token
```

Figure 1: Location Source

Only a fully qualified host name is valid, an IP address MUST NOT be added by an entity conforming with this specification. If a node conforming to this specification receives a geolocation header field with a loc-src parameter containing an IP address then the parameter MUST be removed.

Any proxy adding a location value to a geolocation header field SHOULD also add its host name using the loc-src parameter so that it is clearly identified as the node adding the location. A UE MUST NOT provide a loc-src parameter value. If a proxy receives a message from an untrusted source with the loc-src parameter set then it MUST remove the loc-src parameter before passing the message into a trusted network.

5. Example

The following example shows a SIP INVITE message containing a geolocation header field with two location values. The first location value points to a PIDF-LO in the SIP body using a content-indirection (cid:) URI per [RFC4483] and this is provided by the UE. The second location value is an https URI the provided by a proxy which identifies itself using the loc-src parameter.

```
INVITE sips:bob@biloxi.example.com SIP/2.0
Via: SIPS/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bK74bf9
Max-Forwards: 70
To: Bob <sips:bob@biloxi.example.com>
From: Alice <sips:alice@atlanta.example.com>;tag=9fxced76sl
Call-ID: 3848276298220188511@atlanta.example.com
Geolocation: <cid:target123@atlanta.example.com>,
     <https://lis.example.com:8222/y77syc7cuecbh>;
               loc-src=edgeproxy.example.com
Geolocation-Routing: yes
Accept: application/sdp, application/pidf+xml
CSeq: 31862 INVITE
Contact: <sips:alice@atlanta.example.com>
Content-Type: multipart/mixed; boundary=boundary1
Content-Length: ...
```

Figure 2: Example Location Request.

6. Privacy Considerations

This document doesn’t change any of the privacy considerations described in [RFC6442]. While the addition of the loc-src parameter does provide an indicator of the entity that added the location in the signaling path this provides little more exposure than a proxy identity being added to the record-route header field.

7. Security Considerations

This document introduces the ability of a proxy or middle box to insert a host name indicating the that they added the specific location value to the geolocation header field. The intent is for this field to be used by the location recipient in the event that the SIP message contains multiple location values. As a consequence this parameter should only be used by the location recipient in a trusted network.

The use of this parameter is not restricted to a specific architecture but using multiples locations and loc-src may end in compatibility issues. [RFC6442] already addresses the issue of multiples locations. To avoid problems of wrong interpretation of loc-src the value may be discarded when passed to an other domain.

8. IANA Considerations

8.1. Registration of loc-src Parameter for geolocation header field

This document calls for IANA to register a new SIP header parameter as per the guidelines in [RFC3261], which will be added to header sub-registry under http://www.iana.org/assignments/sip-parameters.

Header Field: geolocation

Parameter Name: loc-src

9. Acknowledgements

NONE

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, DOI 10.17487/RFC3325, November 2002, <http://www.rfc-editor.org/info/rfc3325>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <http://www.rfc-editor.org/info/rfc5234>.

[RFC6442] Polk, J., Rosen, B., and J. Peterson, "Location Conveyance for the Session Initiation Protocol", RFC 6442, DOI 10.17487/RFC6442, December 2011, <http://www.rfc-editor.org/info/rfc6442>.

10.2. Informative References

[M493] European Telecommunications Standards Institute, "Functional architecture to support European requirements on emergency caller location determination and transport", ES 203 178, V 1.1.1, Februar 2015.

[RFC4483] Burger, E., Ed., "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages", RFC 4483, DOI 10.17487/RFC4483, May 2006, <http://www.rfc-editor.org/info/rfc4483>.

[TS23-167] 3rd Generation Partnership Project, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions", TS 23.167, V 12.1.0, March 2015.

Authors' Addresses

James Winterbottom
Winterb Consulting Services
Gwynneville, NSW 2500
AU

Phone: +61 448 266004
Email: a.james.winterbottom@gmail.com

Roland Jesske
Deutsche Telekom
Heinrich-Hertz Str, 3-7
Darmstadt 64295
Germany

Email: r.jesske@telekom.de
URI: www.telekom.de

Bruno Chatras
Orange Labs
38-40 rue du General Leclerc
Issy Moulineaux Cedex 9 F-92794
France

Email: bruno.chatras@orange.com

Andrew Hutton
Unify
Technology Drive
Nottingham NG9 1LA
UK

Email: andrew.hutton@unify.com

SIP Core
Internet-Draft
Updates: 3261 (if approved)
Intended status: Standards Track
Expires: September 10, 2017

R. Shekh-Yusef, Ed.
Avaya
C. Holmberg
Ericsson
V. Pascual
Oracle

March 9, 2017

Third-Party Authentication for Session Initiation Protocol (SIP) draft-yusef-sipcore-sip-authn-01

Abstract

This document defines an authentication mechanism for SIP, that is based on the OAuth 2.0 and OpenID Connect Core 1.0 specifications, to enable the delegation of the user authentication to a dedicated third-party IdP entity that is separate from the SIP network elements that provide the SIP service.

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 September 10, 2017.

Table of Contents

1. Introduction

The SIP protocol [RFC3261] uses the framework used by the HTTP protocol for authenticating users, which is a simple challenge-response authentication mechanism that allows a server to challenge a client request and allows a client to provide authentication information in response to that challenge.

OAuth 2.0 [RFC6749] defines a token based authorization framework to allow clients to access resources on behalf of their user.

The OpenID Connect 1.0 [OPENID] specifications defines a simple identity layer on top of the OAuth 2.0 protocol, which enables clients to verify the identity of the user based on the authentication performed by a dedicated IdP entity, as well as to obtain basic profile information about the user.

This document defines an authentication mechanism for SIP, that is based on the OAuth 2.0 and OpenID Connect Core 1.0 specifications, to enable the delegation of the user authentication to a dedicated third-party IdP entity that is separate from the SIP network elements that provide the SIP service.

1.1. 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].

1.2. Roles

resource owner

An entity capable of granting access to a protected resource. When the resource owner is a person, it is referred to as an end-user.

In a typical SIP network, it is the management element in the system that acts as a resource owner.

resource server

The server hosting the protected resources or services, capable of accepting and responding to protected resource and services requests using access tokens.

OAuth 2.0 client

An application making protected resource requests on behalf of the resource owner and with its authorization. The term "client" does not imply any particular implementation characteristics (e.g., whether the application executes on a server, a desktop, or other devices).

SIP client

An application making requests to access SIP services on behalf of the end-user.

authorization server

The server issuing tokens to the OAuth 2.0 client or SIP Client after successfully authenticating the resource owner and obtaining authorization.

Identity Provider (IdP)

This definition is borrowed from [MITKB]

"IdP (Identity Provider), is a system that creates, maintains, and manages identity information for principals (users, services, or systems) and provides principal authentication to other service providers (applications) within a federation or distributed network. It is a trusted third party that can be relied upon by users and servers when users and servers are establishing a dialog that must be authenticated. The IdP sends an attribute assertion containing trusted information about the user to the SP".

1.3. ID Token

ID token, as defined in the OpenID document, is a security token that contains claims about the authentication of an end-user by an authorization server.

1.4. SIP User Agent Types

[RFC6749] defines two types of clients, confidential and public, that apply to the SIP User Agents.

- Confidential User Agent: is a SIP UA that is capable of maintaining the confidentiality of the user credentials and any tokens obtained using these user credentials.

- Public User Agent: is a SIP UA that is incapable of maintainings the confidentiality of the user credentials and any obtained tokens.

1.5. Authentication Types

There are two types of user authentications in SIP:

- Proxy-to-User: which allows a server that is providing a service to authenticate the identity of a user before providing the service.

- User-to-User: which allows a user receiving a request to authenticate the identity of the remote user before processing the request.

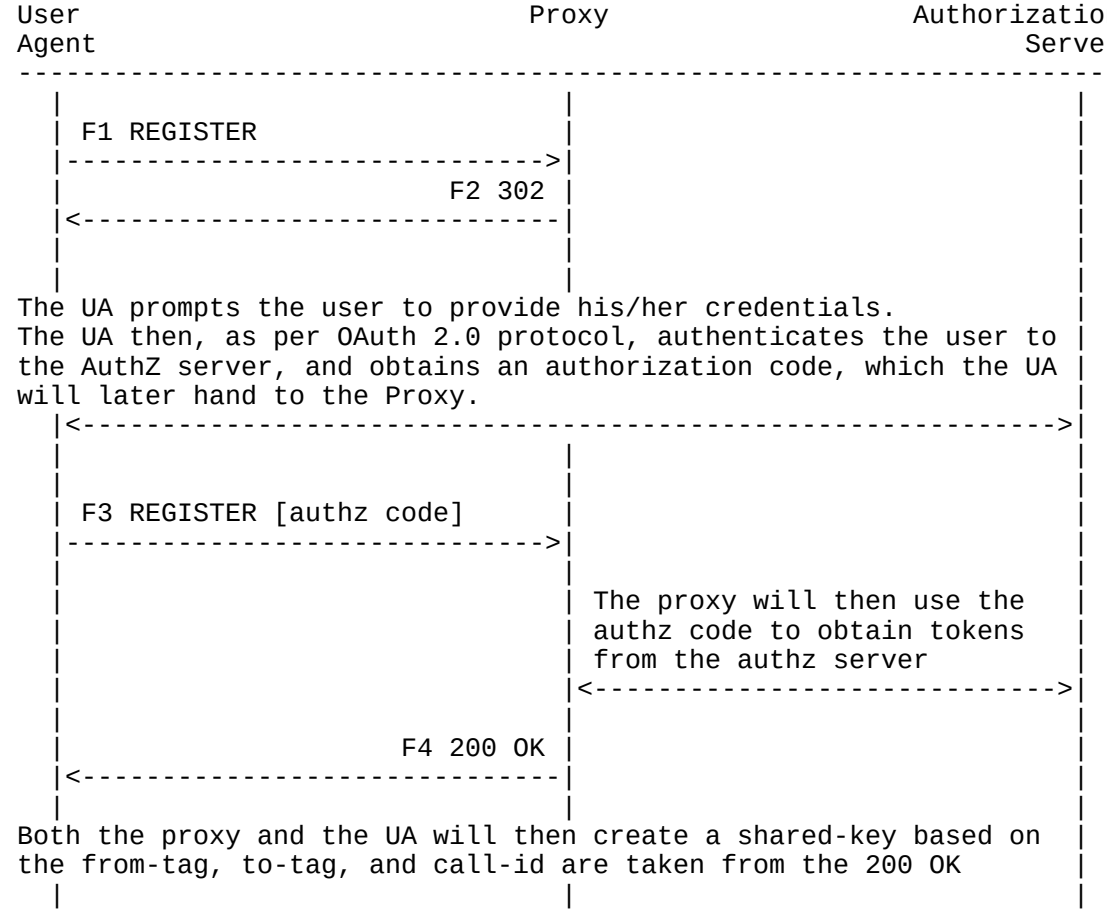
The mechanism defined in this document addresses the proxy-to-user authentication only. For user-to-user authentication refer to the mechanism defined in [STIR].

2. Authentication using the Authorization Code Flow

Authorization Code Flow is used by the SIP UA to authenticate to a third-party IdP entity to obtain an authorization code that would be later used by the SIP Proxy to obtain tokens to allow the SIP UA to register and get service from the SIP network.

2.1. Public UA with Rich UI

The following figure provides a high level view of flow of messages for the user authentication using a Public UA that has a rich UI that would prompt the user for his credentials:



The UA initially sends a REGISTER request (F1) without providing any credentials. The proxy redirects the UA by responding with 302 (F2).

The UA will then contact the Authorization Server and obtain an authorization code to be used with the SIP proxy.

The UA then retries the request (F3) and includes the authorization code in the body of the request.

The proxy then contacts the Authorization Server and exchanges the authorization code for tokens. If the proxy is successful in exchanging the authorization code with the tokens, the proxy then replies with 200 OK to completed the registration process, and locally generates the shared-key with the UA for this user.

When the UA receives the 200 OK, it will follow the same procedure used by the proxy and calculate its shared-key locally.

2.1.1. Registration

The UA initiates the process by sending a REGISTER request (F1) to the proxy. The proxy will redirect the UA to the Authorization Server by responding with 302 (F2) that includes the address of the Authorization Server in the form of an HTTP URI.

The UA will then contact the Authorization Server and obtain an authorization code to be used with the SIP proxy. The method used by the UA to obtain the code is out of scope for this document.

Then, the UA will send a new REGISTER request (F3) and include the authorization code in the body of the request with the following parameters:

grant_type (REQUIRED)

Value MUST be set to "authorization_code".

code (REQUIRED)

The authorization code received from the authorization server.

The proxy then contacts the Authorization Server and exchanges the authorization code for ID token, access token, and refresh token. The method used by the UA to obtain the tokens is out of scope for this document.

If the proxy is successful in exchanging the authorization code with the tokens, the proxy then responds with 200 OK (F4) to the UA to complete the registration process.

2.1.2. Shared-Key

After sending the 200 OK to the UA to complete the registration process, the proxy and the UA use the HMAC-SHA256(key, message) to calculates the shared-key associated with this user as follows:

key

The authorization code obtained from the Authorization Server.

message

The concatenation of the ’from-tag’, ’to-tag’, and ’call-id’ of the 200 OK that completes the registration process.

This shared-key will be used to allow the UA to re-register to the proxy, in case of a connection lost to the proxy, without the need to obtain a new code or prompt the user for his credentials.

2.1.3. Re-Registration Requests

When the UA loses its connection to the proxy and it wants to send a new registration request to the proxy, the UA will send a new REGISTER request and include the proof-of-possession (pop) of the shared-key in the body of the request:

grant_type (REQUIRED)

Value MUST be set to "proof_of_possession".

pop (REQUIRED)

The pop calculated the first time the UA registered with the proxy.

The pop is calculated using the shared-key as follows:

```
pop = HMAC-SHA256(shared-key, digest-string)
```

See rfc4474, section 9, for the SIP headers to hash to create digest-string.

[[OPEN ISSUE]] Should this be not limited to re-registration, and instead be used with all subsequent requests?

2.1.4. Token Refresh

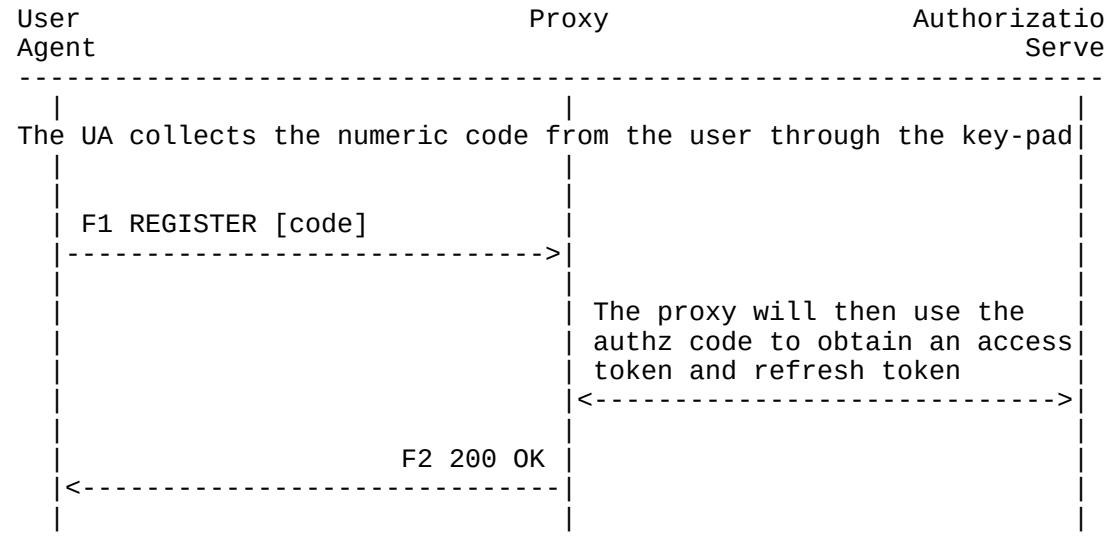
Before the tokens expire, the proxy makes a refresh request to the Authorization Server to try to obtain new tokens. The method used by the UA to refresh the tokens is out of scope for this document.

If the proxy fails to refresh the tokens, then it MUST challenge the next request from the UA, and as a result the UA MUST go through the authorization process again.

2.2. Public UA with Limited UI

The following figure provides a high level view of flow of messages for the user authentication using a Public UA that has a limited UI that cannot prompt the user for his credentials.

This use case requires the user to use his browser to authenticate to the Authorization Server and obtain a short lived numeric authorization code that would be used by the phone to register with the SIP proxy.



2.2.1. Registration

The UA will send a REGISTER request (F1) and include the code in the body of the request with the following parameters:

grant_type (REQUIRED)

Value MUST be set to "authorization_code".

code (REQUIRED)

The code received from the authorization server through the browser.

The proxy then contacts the Authorization Server and exchanges the authorization code for ID token, access token, and refresh token. The method used by the UA to obtain the tokens is out of scope for this document.

If the proxy is successful in exchanging the authorization code with the tokens, the proxy then responds with 200 OK (F2) to the UA to complete the registration process.

2.2.2. Shared-Key

After sending the 200 OK to the UA to complete the registration process, the proxy and the UA use the HMAC-SHA256(key, message) to calculates the shared-key associated with this user as follows:

key

The authorization code obtained from the Authorization Server.

message

The concatenation of the ’from-tag’, ’to-tag’, and ’call-id’ of the 200 OK that completes the registration process.

This shared-key will be used to allow the UA to re-register to the proxy, in case of a connection lost to the proxy, without the need to obtain a new authorization code.

2.2.3. Token Refresh

Before the tokens expire, the proxy makes a refresh request to the Authorization Server to try to obtain new tokens. The method used by the UA to refresh the tokens is out of scope for this document.

If the proxy fails to refresh the tokens, then it MUST challenge the next request from the UA, and as a result the UA MUST go through the authorization process again.

2.2.4. Re-Registration Requests

When the UA loses its connection to the proxy and it wants to send a new registration request to the proxy, the UA will send a new REGISTER request and include the proof-of-possession (pop) of the shared-key in the body of the request:

grant_type (REQUIRED)

Value MUST be set to "proof_of_possession".

pop (REQUIRED)

The pop calculated the first time the UA registered with the proxy.

The pop is calculated using the shared-key as follows:

pop = HMAC-SHA256(shared-key, digest-string)

See rfc4474, section 9, for the SIP headers to hash to create digest-string.

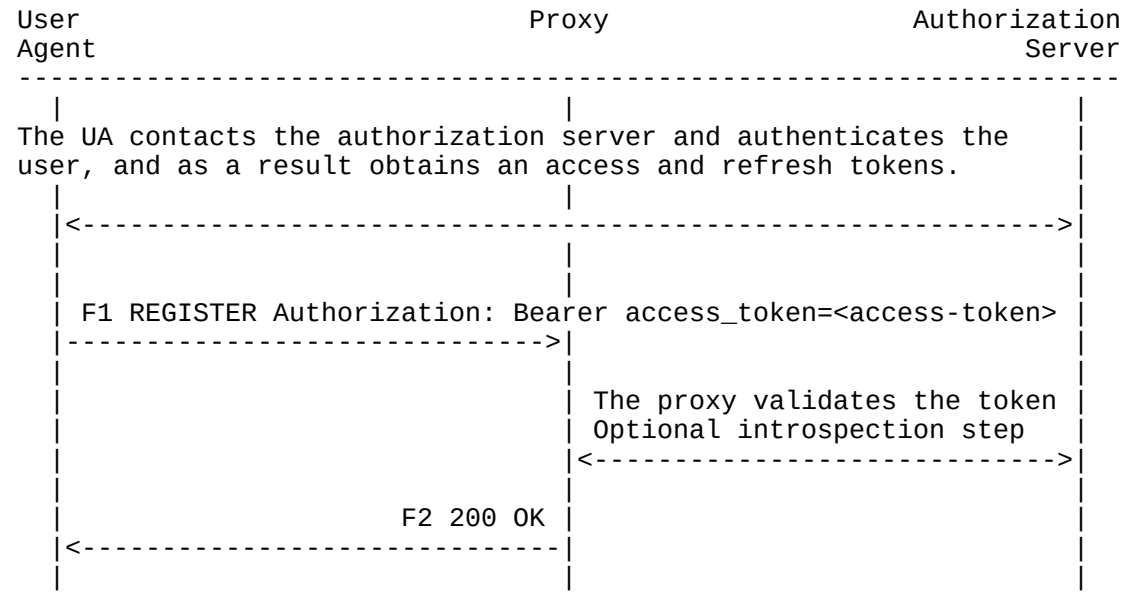
[[OPEN ISSUE]] Should this be not limited to re-registration, and instead be used with all subsequent requests?

3. Authentication using the Resource Owner Password Credentials flow

The resource owner password credentials flow is used by a Confidential UA with rich UI to authenticate to a third-party IdP entity and to directly obtain tokens to be able to register and get service from the SIP network.

3.1. Overview

The following figure provides a high level view of flow of messages for the OAuth Resource Owner Password Credentials flow:



3.2. Registration

The UA first contacts the Authorization Server to authenticate the user and obtain tokens to be used to get access to the SIP network. The method used by the UA to obtain the tokens is out of scope for this document.

The UA starts the registration process with the SIP proxy by sending a REGISTER request (F1) with the access token it obtained previously.

The UA includes an Authorization header field with the Bearer scheme in the request to carry the access token obtained previously.

The proxy then validates the token, and MAY perform an introspection step to get more information about the token and its scope. The introspection step is out of scope for this document.

When the proxy is satisfied with the token, it then replies with the 200 OK to complete the registration process.

3.3. Subsequent Requests

All subsequent requests from the UA MUST include a valid access token. The UA MUST obtain a new access token before the access token expiry period to continue to get service from the system.

4. Authorization Header Syntax

This section describes the syntax of the authorization header with the Bearer scheme.

```
Authorization = "Authorization" HCOLON "Bearer" LWS
                "access_token" EQUAL access_token
access-token = quoted-string
```

5. Security Considerations

<Security considerations text>

6. IANA Considerations

<IANA considerations text>

7. Acknowledgments

<Acknowledgments text>

8. Normative References

[MITKB] "IdP (Identity Provider)", MIT Knowledge Base, http://kb.mit.edu/confluence/x/XoK2, March 2011.

[OPENID] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, "OpenID Connect Core 1.0", February 2014.

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

[RFC6749] Hardt, D., "The OAuth 2.0 Authorization Framework", RFC 6749, October 2012.

[RFC7662] Richer, J., "OAuth 2.0 Token Introspection", RFC 7662, October 2015.

Authors' Addresses

Rifaat Shekh-Yusef (editor)
Avaya
250 Sidney Street
Belleville, Ontario
Canada

Phone: +1-613-967-5267
EMail: rifaat.ietf@gmail.com

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

EMail: christer.holmberg@ericsson.com

Victor Pascual
Oracle
Spain

EMail: victor.pascual.avila@oracle.com