

DISPATCH
Internet-Draft
Intended status: Standards Track
Expires: April 3, 2017

H. Schulzrinne
FCC
September 30, 2016

SIP Call-Info Parameters for Labeling Calls
draft-schulzrinne-dispatch-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 April 3, 2017.

Copyright Notice

Copyright (c) 2016 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

Internet-Draft

Call-Info Spam

September 2016

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	2
2.	Normative Language	3
3.	Parameters	3
4.	Example	5
5.	IANA Considerations	5
5.1.	SIP Call-Info Header Field Parameters	5
5.2.	SIP Global Feature-Capability Indicator	6
6.	Security Considerations	6
7.	Acknowledgements	6
8.	References	6
8.1.	Normative References	6
8.2.	Informative References	7
	Author's Address	7

[1.](#) Introduction

In many countries, an increasing number of calls are unwanted [[RFC5039](#)], as they might be fraudulent, illegal 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.

This document describes a new set of optional parameters and usage for the SIP [[RFC3261](#)] Call-Info header field, purpose "info" [TBD: re-use or define new purpose?], 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 header field, rather than add parameters to an existing one. There MAY be several Call-Info header fields 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.)

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.](#) Parameters

All of the parameters listed below are optional and may appear in any combination and order.

spam The spam parameter indicates the estimated probability that the call is unwanted by the called party, expressed as a whole-number percentage between 0 and 100, inclusive, with larger numbers indicating a 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.

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 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.

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. The definitions are meant to be informal and reflect the common understanding of subscribers who are not lawyers. 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 information regarding an emergency.

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.

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.

4. Example

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

5. IANA Considerations

5.1. 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]

5.2. SIP Global Feature-Capability Indicator

This document defines the feature capability sip.call-info.spam in the "Global 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]

6. 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.

7. Acknowledgements

Jim Calme and other members of the Robocall Strikeforce 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>>.

[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>>.

[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-13](#) (work in progress), September 2016.
- [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
450 12th Street SW
Washington, DC 20554
US

Email: henning.schulzrinne@fcc.gov