SIPCORE	E. Burger
Internet-Draft	Georgetown University
Intended status: Standards Track	July 10, 2018
Expires: January 11, 2019	

A Session Initiation Protocol (SIP) Response Code for Rejected Calls

draft-burger-sipcore-rejected-00

Abstract

This document defines the 608 (Rejected) SIP response code. This response code enables calling parties to learn their call was rejected by an intermediary and will not be answered. As a 6xx code, the caller will be aware that future attempts to contact the same UAS will be likely to fail. The present use case driving the need for the 608 response code is when the intermediary is an analytics engine. In other words, the rejection is by a machine or other process, as opposed to a human at the target UAS indicating the call was not wanted. This document also defines the use of the Call-Info header in 608 responses to enable rejected callers to contact entities that blocked their calls in error.

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 https://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 January 11, 2019.

Copyright Notice

Copyright (c) 2018 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 (https://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.

1. Introduction

The IETF has been addressing numerous issues surrounding how to handle unwanted and, depending on the jurisdiction, illegal calls [RFC5039]. Technologies such as STIR and SHAKEN address cryptographic signing and attestation, respectively, of signaling to ensure the integrity and authenticity of the asserted identity.

This document describes a new SIP response code, 608, which allows calling parties to learn their call was rejected by an intermediary. As will be described below, we need a distinct indicator to differentiate between

a user rejection and an intermediary's rejection of a call. In many jurisdictions, some calls, even if unwanted by the user, may not be blocked unless there is an explicit user request. Moreover, users may misidentify the nature of a caller. For example, a legitimate caller may call a user who finds the call to be unwanted. However, instead of marking the call as unwanted, the user may mark the call as illegal. With that information, an analytics engine may determine that all calls from that source should be blocked. However, in many jurisdictions blocking calls from that source from other users may not be legal. Likewise, one can envision jurisdictions that allow an operator to block such calls, but only if there is a remediation mechanism in place to address false positives.

Today, some call blocking services may return responses such as 604 (Does Not Exist Anywhere). This might be a strategy to attempt to get a destination's address removed from a calling database. However, other network elements might interpret this to mean the user truly does not exist and result in the user not being able to receive calls. As well, in many jurisdictions, providing false signaling is illegal.

The 608 response code addresses this need of addressing falsely blocked calls. Specifically, this code informs the UAC the call was blocked, the call was blocked by an intermediary, and, to satisfy some jurisdiction's requirements for providing a redress mechanism, how to contact the operator of the intermediary.

In the call handling ecosystem, users can explicitly reject a call or later mark a call is being unwanted by issuing a 607 SIP response code (Unwanted). Figure 1 shows the operation of the 607 SIP response code. The UAS indicates the call was unwanted. As RFC8197 explains, not only does the called party desire to reject that call, they wish to let their proxy know they do not ever want to get calls from that source. The proxy may send call information to a call analytics engine. For various reasons described in RFC8197, if a network operator receives multiple reports of unwanted calls, that may indicate the entity placing the calls is likely to be a source of unwanted calls for many people. As such, other users of the service provider's service may wish the service provider to automatically reject calls on their behalf based on that and other analytics.

Another value of the 607 rejection is presuming the proxy forwards the response code to the UAC, the calling UAC or intervening proxies know the user is not interested in receiving calls from that sender.

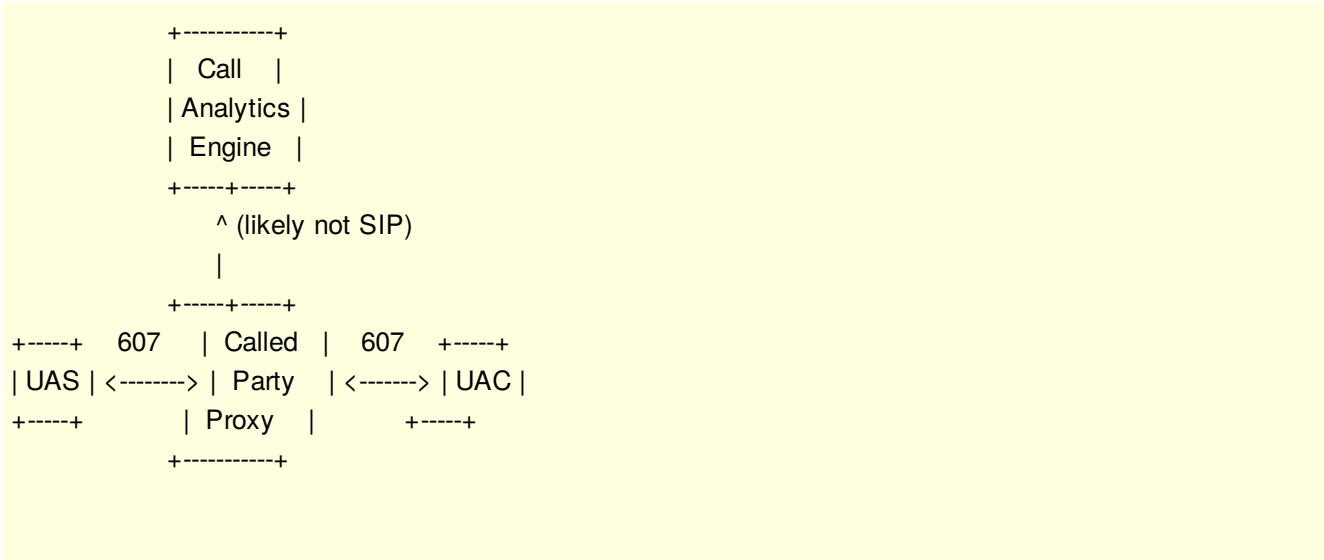

Figure 1: Unwanted (607) Call Flow

For calls rejected with a 607 from a legitimate caller, receiving a 607 response code can inform the caller to stop attempting to call the user. Moreover, if the legitimate caller believes the user is rejecting their calls in error, they can use other channels to contact the user. For example, if a pharmacy calls a user to let them know their prescription is available for pickup and the user mistakenly thinks the call is unwanted and issues a 607 response code, the pharmacy, having an existing relationship with the customer, can send the user an email, also noting they might consider not rejecting their calls in the future.

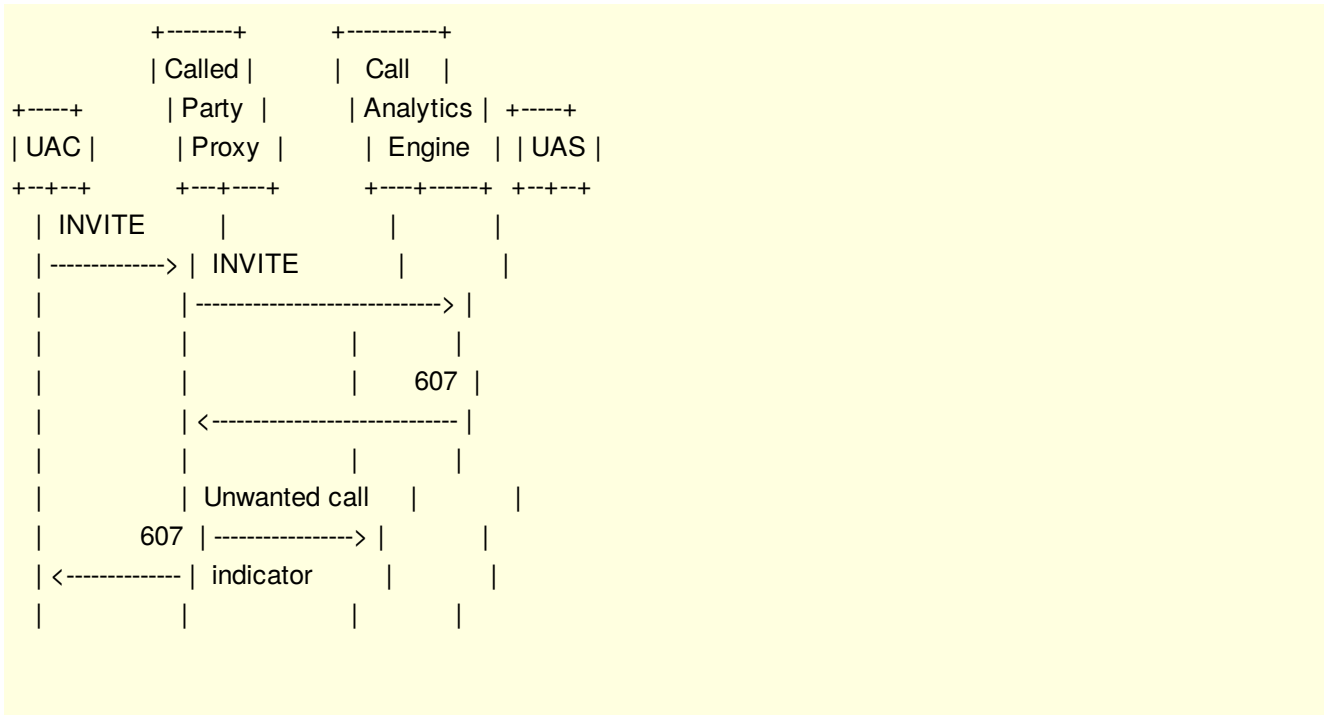

Figure 2: Unwanted (607) Ladder Diagram

However, things get more complicated if an intermediary, such as a third-party provider of call management services that classify calls based on the relative likelihood the call is unwanted, misidentifies the call as unwanted. Figure 3 shows this case. In this situation, it would be beneficial for the caller to be able to learn who rejected the call, so they might be able to correct the misidentification.

In this situation, one might be tempted to have the intermediary use the 607 response code. 607 indicates to the caller the subscriber did not get the call and they do not want the call. However, RFC8197 specifies that one of the uses of 607 is to inform analytics engines that a user (human) has rejected a call. The problem here is network elements downstream from the intermediary might interpret the 607 as a user (human) marking the call as unwanted, as opposed to a statistical, machine learning, vulnerable to the base rate fallacy algorithm rejecting the call. In other words, those downstream entities should not be relying on another entity 'deciding' the call is unwanted. By distinguishing between a (human) user rejection and an intermediary's statistical rejection, a downstream network element that sees a 607 result code can weight it as a human rejection in its call analytics.

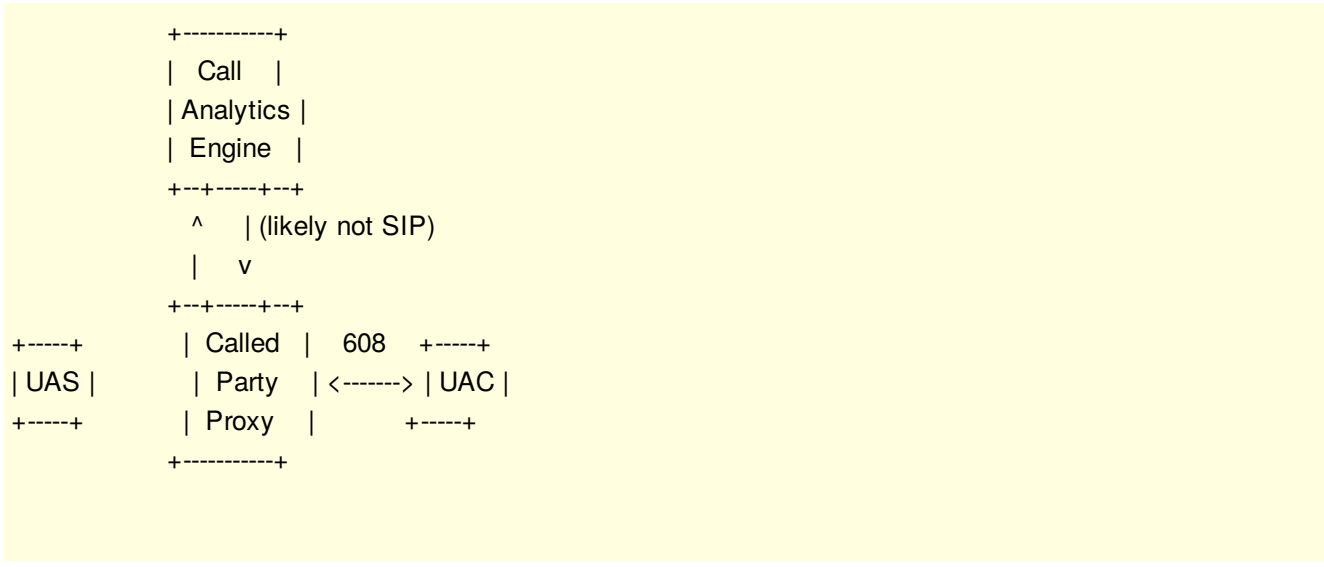

Figure 3: Rejected (608) Call Flow

It is useful for blocked callers to have a redress mechanism. One can imagine that some jurisdictions will require it. However, we must be mindful that most of the calls that will be blocked will, in fact, be illegal and

eligible for blocking. Thus, providing alternate contact information for a user would be counterproductive to protecting that user from illegal communications. This is another reason we do not propose to simply allow alternate contact information in a 607 response message.

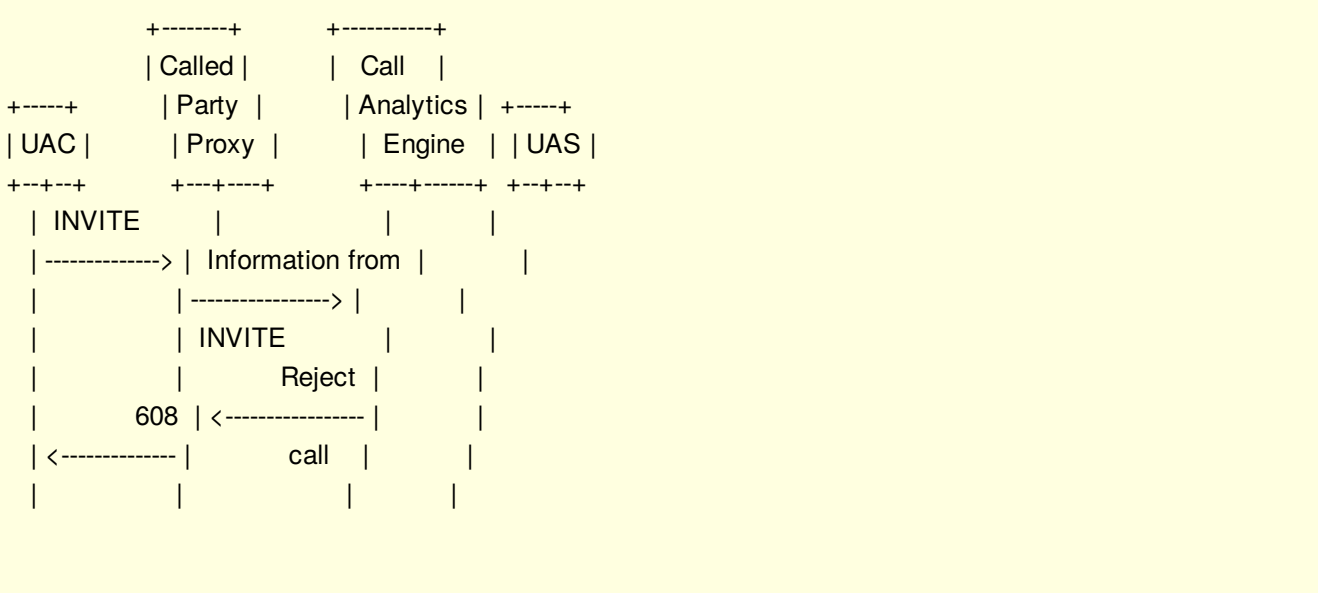

Figure 4: Rejected (608) Ladder Diagram

As such, we need a mechanism for indicating an intermediary rejected a call while providing contact information for the operator of the intermediary that provides call rejection services to the called party, without exposing the target user's contact information.

2. Terminology

This document uses the terms "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" as described in BCP14 [RFC2119][RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Protocol Operation

For clarity, this section uses the term 'intermediary' as the entity that acts as a SIP User Agent Server (UAS) on behalf of the user in the network, as opposed to the user's UAS (colloquially, but not necessarily, their phone). The intermediary could be a back-to-back user agent (B2BUA) or a SIP Proxy.

An intermediary MAY issue the 608 code in a failure response for an INVITE, MESSAGE, SUBSCRIBE, or other out-of-dialog SIP request to indicate that an intermediary rejected the offered communication as unwanted by the user. An intermediary MAY issue the 608 as the value of the "cause" parameter of a SIP reason-value in a Reason header field [RFC3326].

Unless there are indicators the calling party will use the contents of the Call-Info header for malicious purposes (see Section 6), if an intermediary issues a 608 code, the intermediary MUST include a Call-Info header in the response.

Proxies need to be mindful that a downstream intermediary may reject the attempt with a 608 while other paths may still be in progress. In this situation, the requirements stated in Section 16.7 of RFC3261 apply. Specifically, the proxy should cancel pending transactions and must not create any new branches. Note this is not a new requirement but simply pointing out the existing 6xx protocol mechanism.

If there is a Call-Info header, it MUST have the 'purpose' parameter of 'card'. The value of the Call-Info header MUST refer to a valid vCard object.

The vCard referenced in the Call-Info header MUST include at least one of the URL, EMAIL, TEL, or ADR

properties. UACs supporting this specification MUST be prepared to receive a full vCard. Call originators (at the UAC) can use the information returned by the vCard to contact the intermediary that rejected the call to appeal the intermediary's future blocking of the call attempt. What the intermediary does if the blocked caller contacts the intermediary is outside the scope of this document.

Upon receiving a 608 response, UACs perform normal SIP processing for 6xx responses.

4. Example

Given an INVITE (shamelessly taken from [SHAKEN]:

```
INVITE sip:+12155551213@tel.example1.net SIP/2.0
Max-Forwards: 69
Contact: <sip:+12155551212@69.241.19.12:50207;rinstance=9da3088f36cc>
To: <sip:+12155551213@tel.example1.net>
From: "Alice" <sip:+12155551212@tel.example2.net>;tag=614bdb40
Call-ID: 79048YzkxNDA5NTI1MzA0OWFjOTFkMmFlODhiNTI2OWQ1ZTI
P-Asserted-Identity: "Alice"<sip:+12155551212@tel.example2.net>,
   <tel:+12155551212>
CSeq: 2 INVITE
Allow: SUBSCRIBE, NOTIFY, INVITE, ACK, CANCEL, BYE, REFER, INFO,
   MESSAGE, OPTIONS
Content-Type: application/sdp
Date: Tue, 16 Aug 2016 19:23:38 GMT
Identity:
eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwicHB0Ijoic2hha2VuIiwieDV1I
joiaHR0cDovL2NlcnQtYXV0aC5wb2Muc3lzLmNvbWNhc3QubmV0L2V4YW1wbGUuY2VydC
J9eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6IisxMjE1NTU1MTIxMyJ9LCJpYXQiOiI
xNDcxMzc1NDE4Iiwib3JpZyI6eyJ0biI64oCdKzEyMTU1NTUxMjEyIn0sIm9yaWdpZCI6
IjEyM2U0NTY3LWU4OWItMTJkMy1hNDU2LTQyNjY1NTQ0MDAwMCJ9._28kAwRWnheXyA6n
Y4MvmK5JKHZH9hSYkWI4g75mnq9Tj2lW4WPm0PlvudoGaj7wM5XujZUTb_3MA4modoDtC
A;info=<http://cert.example2.net/example.cert>;alg=ES256
Content-Length: 153

v=0
o=- 13103070023943130 1 IN IP4 192.0.2.177
c=IN IP4 192.0.2.177
t=0 0
m=audio 54242 RTP/AVP 0
a=sendrecv
```

An intermediary could reply:

```
SIP/2.0 608 Rejected
Via: SIP/2.0/UDP 192.0.2.177:60012;branch=z9hG4bK-524287-1
From: "Alice" <sip:+12155551212@tel.example2.net>;tag=614bdb40
To: <sip:+12155551213@tel.example1.net>
Call-ID: 79048YzkxNDA5NTI1MzA0OWFjOTFkMmFlODhiNTI2OWQ1ZTI
CSeq: 2 INVITE
Call-Info: <https://blocker.example.net/complaints.vcf>;purpose=card
```

A minimal vCard, in this example at https://blocker.example.net/complaints.vcf, could contain:

```
BEGIN:VCARD
VERSION:4.0
FN:Robocall Adjudication
EMAIL;TYPE=work:bitbucket@blocker.example.net
END:VCARD
```

For an intermediary that provides a Web site for adjudication, the vCard could contain:

```
BEGIN:VCARD
VERSION:4.0
FN:Robocall Adjudication
URL;TYPE=work:https://blocker.example.net/adjudication-form
END:VCARD
```

For an intermediary that provides a telephone number and a postal address, the vCard could contain:

```
BEGIN:VCARD
VERSION:4.0
FN:Robocall Adjudication
ADR;TYPE=work;Argument Clinic;12 Main St;Anytown;AP;000000;Somewhere
TEL;VALUE=uri;TYPE=work:tel:+1-555-555-1212
END:VCARD
```

Note that it is up to the receiver to decide which modality, if any, it will use.

5. IANA Considerations

5.1. SIP Response Code

This document registers a new SIP response code, 608. Please register the response code in the "Response Codes" subregistry of the "Session Initiation Protocol (SIP) Parameters" registry at <http://www.iana.org/assignments/sip-parameters>.

Response code: 608

Description: Rejected

Reference: [RFCXXXX]

6. Security Considerations

Intermediary operators need to be mindful of whom they are sending the 608 response to. There is a risk that a truly malicious caller is being rejected. This raises two issues. The first is the caller, being alerted their call is being automatically rejected, may change their call behavior to defeat call blocking systems. The second, and more significant risk, is that by providing a contact modality in the Call-Info field, the intermediary may be giving the malicious caller a vector for attack. In other words, the intermediary will be publishing an address that a malicious actor may use to launch an attack on the intermediary. Because of this, intermediary operators may wish to configure their response to only include a Call-Info field for INVITE or other initiating methods that are signed by STIR.

7. Acknowledgements

This document liberally lifts from [RFC8197] in its text and structure. However, the mechanism and purpose is quite different. Any errors are the current editor's and not the editor of RFC8197. Thanks also go to Ken Carlberg of the FCC, Russ Housley, Paul Kyzivat, and Tolga Asveren for their suggestions on improving the draft.

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.

[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.

[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.

[RFC6350] Perreault, S., "vCard Format Specification", RFC 6350, DOI 10.17487/RFC6350, August 2011.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017.

8.2. Informative References

[BaseRate] Bar-Hillel, M., "The Base-Rate Fallacy in Probability Judgements", April 1977.

[RFC5039] Rosenberg, J. and C. Jennings, "The Session Initiation Protocol (SIP) and Spam", RFC 5039, DOI 10.17487/RFC5039, January 2008.

[RFC7340] Peterson, J., Schulzrinne, H. and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", RFC 7340, DOI 10.17487/RFC7340, September 2014.

[RFC8197] Schulzrinne, H., "A SIP Response Code for Unwanted Calls", RFC 8197, DOI 10.17487/RFC8197, July 2017.

[RFC8224] Peterson, J., Jennings, C., Rescorla, E. and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 8224, DOI 10.17487/RFC8224, February 2018.

[SHAKEN] Alliance for Telecommunications Industry Solutions (ATIS) and the SIP Forum, "Signature-based Handling of Asserted information using toKENs (SHAKEN)", ATIS 1000074, January 2017.

Author's Address

Eric W. Burger
Georgetown University
37th & O St, NW
Washington, DC 20057
USA
EMail: eburger@standardstrack.com

Table of Contents