A Session Identifier for the Session Initiation Protocol (SIP)
draft-kaplan-sip-session-id-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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".

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on May 18, 2009.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

There are several reasons for having a globally unique session identifier for the same SIP session, which can be maintained across B2BUA’s and other SIP middle-boxes. This draft proposes a new SIP header to carry such a value: Session-ID.
1. Introduction

The SIP [RFC3261] Call-ID header value is a globally unique identifier, mandatory in all requests/responses, which identifies SIP messages belonging to the same dialog or registration. It provides a portion of the SIP message dialog-matching criteria, and is used in [Replaces] headers and [dialog-events] package for matching to such, and in [SIP-Identity] and [Connected-identity] as one of the inputs for signing.

Unfortunately, the Call-ID is often changed by B2BUA’s and other such middle-boxes in the end-to-end message path. A B2BUA logically represents a UAS and UAC, and as such may use a new Call-ID value for the dialog it creates on its UAC half; but there are several use-cases for having a common, consistent end-to-end identifier, as described later in this draft.

There are several reasons the Call-ID value is changed by B2BUA’s. There are security and privacy reasons, since Call-ID values
typically contain UA IP Addresses; some B2BUA’s need to change them to keep track of spiraling dialogs; and some need to change them to keep track of separate forks. In fact, some have argued a B2BUA has no choice but to create a new one, in order to strictly comply with RFC 3261 as a UAC. In general, B2BUA’s modify the Call-ID value in both directions, "fixing" it to be what each side of the B2BUA would expect. This works fine if the B2BUA is in the message path, and knows all SIP message or body contents which use or reference the value. However for subsequent out-of-dialog requests, or new SIP uses, a B2BUA often does not or cannot "fix" the value correctly.

Therefore, in order to provide an identifier which will not be modified/replaced by B2BUA’s, this draft proposes a new SIP Header "Session-ID", and mandatory rules for the value of such a header. The rules are designed to be such that the value in the Session-ID header is not considered unsafe, private, or have any property which would cause B2BUA’s to change it. The goal of this draft is to enable use-cases which need a unique identifier for a given session which can successfully cross B2BUA’s.

1.1. Example use-cases for Session-ID

The need for a unique identifier is driven by the following use-cases:

1. Certain SIP applications need to reference dialogs in out-of-dialog requests at a layer above the SIP message dialog matching rules, and wish it to work across B2BUA domains. For example, the SIP Media Control Channel Framework [media-ctrl] needs to reference a dialog identifier used between a UAC and UAS by a third party. The mechanism originally used the Call-ID and remote/local-tags for such matching, but changed due to concerns over B2BUA’s changing them, and now uses a new cfw-id SDP attribute.

2. Multiple RFC 3265 Event packages use the Call-ID value in their package bodies to reference established sessions, even though they don’t actually need to match a Call-ID per se - and should work across B2BUA domains. These packages could be updated to include a Session-ID XML attribute as an alternative, optional matching criteria.

3. Several proposed and documented identity verification mechanisms need a hard-to-guess dialog identifier for verification. For example, RFC 4474 uses the Call-ID header value in its signature to prevent replay/copy-paste attacks, even though it does not need a Call-ID value per se; it just needs a unique dialog identifier. Likewise, [draft-derive] wishes to perform a reverse dialog-verification to verify a caller identity based on some
unique identifier for the dialog; [draft-pass] creates a header-parameter to perform something similar.

4. Some SIP service providers implement call admission control (CAC) for bandwidth, and only allow SIP INVITE requests if the network has sufficient bandwidth for the given SDP. If a call request is forked by B2BUA’s, or crosses them, however, the CAC model treats each fork as a separate call because there is no identifier to tie them together. This leads to rejected forks due to CAC, when they should have been allowed to proceed. A common identifier would provide the information to correlate the requests. Currently proprietary SIP headers are used for this purpose.

5. Troubleshooting SIP sessions is more complicated if multiple legs of the session are on different sides of B2BUA’s, due to the lack of a common identifier to tie the legs together. Currently proprietary mechanisms are used to achieve this.

6. When SIP requests cross B2BUA’s, the only form of loop detection that will stop a loop is the Max-Forwards hop-count limit being reached (value reaching zero). Via header values are removed by B2BUA’s, so both spirals and simple loops cannot be detected by Via branch-parameter matching. A Session-ID value could be used to detect loops by imposing a limit on the number of times the same Session-ID can cross the same B2BUA. This would be a local decision, and an optimization, but it would be useful.

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 RFC 2119. The terminology in this document conforms to RFC 2828, "Internet Security Glossary".

3. Applicability

This draft proposes a new SIP header for all requests and responses.

4. Overview of Operation

The general concept is that the UAC generating an out-of-dialog request generates a new, pseudo-random, unique value which remains constant for the duration of the transaction, any dialog created from the request, or a registration. The value is based on the rules for creating a pseudo-random value (a UUID?), and is inserted in a new Session-ID header defined in this draft.

This Session-ID is not used for message dialog-matching rules in RFC 3261, nor does it change the Call-ID usage, nor does it replace the
5. Session-ID Behavior

5.1. Generating a Session-ID value

This draft proposes the Session-ID header value be generated based on a defined mechanism for creating a 128-bit pseudo-random value, and encode it as its lower-case hex representation. The reason for specifying the mechanism, and its length, is to make it impossible to determine the manufacturer of the device which generated it by looking at its format or value. For example, the theoretically random "session id" value in SDP origin line has been found to be fairly vendor-specific in nature, and one can narrow the vendor that generated the SDP simply by the origin session id value. (In fact, this drove some SBC’s to modify that SDP field for "anonymization" purposes).

One proposal is to generate it based on the rules for a UUID as defined in RFC 4122. [NOTE: the actual mechanism to use is TBD]

5.2. UAC Behavior

The rules for when a UAC generates a new Session-ID value are similar as those for Call-ID value: a UAC supporting this draft MUST generate a *new* unique Session-ID value whenever it generates an out-of-dialog request, or for a new Registration. The UAC MUST re-use the same Session-ID for any out-of-dialog request it retransmits or re-generates in response to a 3xx, or it re-formulates due to failure responses.

Session-ID values in Registration refreshes - REGISTER requests which are used to update the expiry time but not to register a new contact - MUST use the same Session-ID value as previous REGISTER requests.

The UAC MUST include the Session-ID header and value in any out-of-dialog request, including Registration refreshes, and any retransmitted or regenerate out-of-dialog request. It MAY include them in in-dialog requests or responses, but since they are not used for dialog-matching rules this is not mandatory, and MUST NOT cause dialog or transaction failure if they do not match previous ones.

5.3. Proxy Behavior

A Proxy MUST NOT remove or modify the Session-ID header values it receives. If the Proxy forks a request, it MUST copy the same Session-ID value into all the forked request copies. If the Proxy
recurses requests due to 3xx redirection, or regenerates requests due to failures, it MUST use the same Session-ID value, just as the UAC does.

5.4. B2BUA Behavior

A B2BUA MUST copy the Session-ID it receives in requests as a UAS, into the related requests it generates as a UAC; and any Session-ID value it receives in responses as a UAC into the correlated responses it generates as a UAS. If the B2BUA forks or creates multiple requests as a UAC, from a request it received as a UAS, the B2BUA MUST copy the same Session-ID header value it received into all the forks/requests. If the B2BUA recurses requests due to 3xx redirection, or regenerates requests due to failures, it MUST use the same Session-ID value, just as the UAC does.

5.5. UAS Behavior

A UAS MAY copy the received Session-ID value into responses and subsequent upstream requests within the dialog.

6. New Header

<table>
<thead>
<tr>
<th>Hdr-field when ACK BYE CAN INV OPT REG PRA INF REF UPD SUB NOT MSG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session-ID r o o o o o o o o o o o o o o o o o o o o o o o o o</td>
</tr>
<tr>
<td>Session-ID R o o o o m m m m o o m m m m m m m m m m m m m m m</td>
</tr>
</tbody>
</table>

The header is only mandatory for out-of-dialog requests; for others it is optional. [Open Issue: should this be mandatory for all?]

6.1. "Session-ID" header

This draft proposes Session-ID to be added to the definition of the element "message-header" in the SIP message grammar.

The Session-ID header is a single-instance header.

6.2. Augmented BNF Definitions

```plaintext
Session-ID       =  "Session-ID" HCOLON sess-id
                 *( SEMI generic-param )
sess-id         =  32(DIGIT / %x61-7A)  ; 32 chars of [0-9a-z]
```

NOTE: The sess-id value is case-SENSITIVE, just as Call-ID is, however only lower-case characters are defined and allowed.
7. Example Exchange

In the following example, Alice initiates a call to Bob. Alice generates a Session-ID header in the out-of-dialog INVITE.

Alice generates the following: (note: much has been left out for simplicity)

```
INVITE sip:bob@example.com SIP/2.0
Via: SIP/2.0/UDP 192.0.2.1:5060;branch=z9hG4bKnashds10
From: Alice <sip:alice@example.net>;tag=1234567
To: Bob <sip:bob@example.com>
Call-Id: 123456mcmxcix@1.2.3.4
Session-ID: f81d4fae7dec11d0a76500a0c91e6bf6
CSeq: 1 INVITE
Contact: <sip:alice@192.168.1.1>
```

8. Security Considerations

There are no specific security issues for this mechanism, beyond those already applicable to SIP-based session signaling. [TBD]

9. IANA Considerations

This document makes no request of IANA.

10. Acknowledgments

Thanks to Raphael Coeffic and Bob Penfield for their input.

11. References

11.1. Normative References


11.2. Informative References


SIP Session Identifier

November 2008

"RFC 4916, June 2007.

[Replaces] Elwell, J., "The Session Initiation Protocol (SIP)

[dialog-events] Elwell, J., "The Session Initiation Protocol (SIP)

[RFc4122] Leach, P., Mealling, M., Salz, R., "A Universally Unique
Identifier (UUID) URN Namespace", RFC 4122, July 2005.

[media-ctrl] Boulton, C., Melanchuk, T., McGlashan, S., "Media
Control Channel Framework", draft-ietf-mediactrl-sip-control-
framework-06, October 2008.

[draft-derive] Kuthan, J., Sisalem, D., Coeffic, R., Pascual V.,
"Dialog Event foR Identity VErification", draft-kuthan-sip-
derive-00, October 2008.

[draft-pass] Kaplan, H., "Private Extensions to the Session
Initiation Protocol (SIP) for Asserter Identification within
Trusted Networks", draft-kaplan-sip-asserter-identity-00, July
2008.

Author’s Address

Hadriel Kaplan
Acme Packet
71 Third Ave.
Burlington, MA 01803, USA

Email: hkaplan@acmepacket.com
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).