Network Working Group	A. Johnston
Internet-Draft	Avaya
Intended status: Standards Track	J. McMillen
Expires: June 17, 2011	Unaffiliated
	J. Rafferty
	Dialogic
	December 14, 2010

TOC

A Mechanism for Transporting User to User Call Control Information in SIP
draft-johnston-cuss-sip-uui-01

Abstract

There is a need for applications using SIP to exchange User to User Information (UUI) data during session establishment. This information, known as call control UUI, is a small piece of data inserted by an application initiating the session, and utilized by an application accepting the session. This data is opaque to SIP and its function is unrelated to any basic SIP function. Several approaches to transporting call control UUI in SIP have been proposed. As networks move to SIP it is important that applications requiring this data can continue to function in SIP networks as well as the ability to interwork with this ISDN service for end-to-end transparency. This document discusses three mechanisms to meet the requirements defined in the Requirements for SIP Call Control UUI document. A new SIP header field which bests meets these requirements is proposed.

Status of this Memo

Copyright Notice

Table of Contents

---

1. Overview

TOC

This document describes the transport of User to User Information (UUI) using SIP [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, “SIP: Session Initiation Protocol,” June 2002.). Specifically, we discuss a mechanism for the transport of general application UUI and also for the transport of call control related ITU-T Q.931 User to User Information Element (UU IE) [Q931] (, “ITU-T Q.931 User to User Information Element (UU IE),” .) and ITU-T Q.763 User to User Information Parameter [Q763] (, “ITU-T Q.763 Signaling System No. 7 - ISDN user part formats and codes,” .) data in SIP. UUI is widely used in the PSTN today in contact centers and call centers which are transitioning away from ISDN to SIP. This extension will also be used for native SIP endpoints implementing similar services and interworking with ISDN services.

This mechanism was designed to meet the use cases, requirements, and call flows for SIP call control UUI detailed in [I-D.ietf-cuss-sip-uui-reqs] (Johnston, A., McMillen, J., and L. Liess, “Problem Statement and Requirements for Transporting User to User Call Control Information in SIP,” November 2010.). All references to requirement numbers (REQ-N) and figure numbers refer to this document.

2. Terminology

TOC

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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

3. Possible Mechanisms

TOC

Three possible mechanisms for transporting UUI will be described: MIME body, URI parameter, and header field transport.

3.1. Why INFO is Not Used

TOC

Since the INFO method [RFC2976] (Donovan, S., “The SIP INFO Method,” October 2000.), was developed for ISUP interworking of user-to-user information, it might seem to be the logical choice here. For non-call control user-to-user information, INFO can be utilized for end to end transport. However, for transport of call control user-to-user information, INFO can not be used. As the call flows in [I-D.ietf-cuss-sip-uui-reqs] (Johnston, A., McMillen, J., and L. Liess, “Problem Statement and Requirements for Transporting User to User Call Control Information in SIP,” November 2010.) show, the information is related to an attempt to establish a session and must be passed with the session setup request (INVITE), responses to that INVITE, or session termination requests. As a result, it is not possible to use INFO in these cases.

3.2. Why Other Protocol Encapsulation UUI Mechanisms are Not Used

TOC

Other protocols have the ability to transport UUI information. For example, consider the ITU-T Q.931 User to User Information Element (UU IE) [Q931] (, “ITU-T Q.931 User to User Information Element (UU IE),” .) and the ITU-T Q.763 User to User Information Parameter [Q763] (, “ITU-T Q.763 Signaling System No. 7 - ISDN user part formats and codes,” .). In addition, NSS (Narrowband Signaling System) [Q1980] (, “ITU-T Q.1980.1 The Narrowband Signalling Syntax (NSS) - Syntax Definition,” .) is also able to transport UUI information. Should one of these protocols be in use, and present in both User Agents, then utilizing these other protocols to transport UUI might be a logical solution. Essentially, this is just adding an additional layer in the protocol stack. In these cases, SIP is not transporting the UUI; it is encapsulating another protocol, and that protocol is transporting the UUI. Once a mechanism to transport that other protocol using SIP exists, the UUI transport function is essentially obtained without any additional effort or work.

However, the authors believe that SIP needs to have its own native UUI transport mechanism. It is not reasonable for a SIP UA to have to implement another entire protocol (either ISDN or NSS, for example) just to get the very simple UUI transport service. Of course, this work does not preclude anyone from using other protocols with SIP to transport UUI information.

3.3. Discovery Mechanism

TOC

Two requirements, REQ-8 and REQ-10 relate to discovery of the mechanism and supported applications. As such, these requirements are independent of the actual transport mechanism. Mechanisms to support these requirements are now discussed.

REQ-8 could be met by defining a new SIP option tag 'uui'. The use of a 'Require: uui' in a request, or 'Supported: uui' in an OPTIONS response could be used to require or discover support of the mechanism. REQ-10 could be met by creating a new class of SIP feature tags. For example, the feature tag 'sip.uui.isdn' could be used to indicate support of the ISDN UUI service, or 'sip.uui.app1' could be used to indicate support for a particular application.

3.4. MIME body Approach

TOC

One method of transport is to use a MIME body. This is in keeping with the SIP-T architecture [RFC3372] (Vemuri, A. and J. Peterson, “Session Initiation Protocol for Telephones (SIP-T): Context and Architectures,” September 2002.) in which MIME bodies are used to transport ISUP information. Since the INVITE will normally have an SDP message body, the resulting INVITE with SDP and UUI will be multipart MIME. This is not ideal as many SIP UAs do not support multipart MIME INVITEs.

A bigger problem is the insertion of a UUI message body by a redirect server or in a REFER. The body would need to be encoded in the Contact URI of the 3xx response or the Refer-To URI of a REFER. Currently, the authors are not aware of any UAs that support this capability today for any body type. As such, the complete set of semantics for this operation would need to be determined and defined. Some issues will need to be resolved, such as, do all the Content-* header fields have to be escaped as well? And, what if the escaped Content-Length does not agree with the escaped body?

Since proxies cannot remove a body from a request or response, it is not at all clear how this mechanism could meet REQ-9.

The requirement for integrity protection could be met by the use of an S/MIME signature over the body, as defined in Section 23.3 of RFC 3261 "Securing MIME bodies". Alternatively, this could be achieved using RFC 4474 (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.) [RFC4474]. The requirement for end-to-end privacy could be met using S/MIME encryption or using encryption at the application layer. However, note that neither S/MIME or RFC 4474 enjoys deployment in SIP today.

An example:

```
<allOneLine>
Contact: <sip:+12125551212@gateway.example.com?Content-Type=
application/uui&body=ZeGl9i2icVqaNVailT6F5iJ90m6mvuTS4OK05M0vDk0Q4Xs>
</allOneLine>
```

Note that the <allOneLine> tag convention from SIP Torture Test Messages (Sparks, R., Hawrylyshen, A., Johnston, A., Rosenberg, J., and H. Schulzrinne, “Session Initiation Protocol (SIP) Torture Test Messages,” May 2006.) [RFC4475] is used to show that there are no line breaks in the actual message syntax.

As such, the MIME body approach meets REQ-1, REQ-2, REQ-4, REQ-5, REQ-7, REQ-11, REQ-13, and REQ-14. Meeting REQ-12 seems possible, although the authors do not have a specific mechanism to propose.

Meeting REQ-3 is problematic, but not impossible for this mechanism. However, this mechanism does not seem to be able to meet REQ-9.

3.5. URI Parameter

TOC

Another proposed approach is to encode the UUI as a URI parameter. This UUI parameter could be included in a Request-URI or in the Contact URI or Refer-To URI. It is not clear how it could be transported in a responses which does not have a Request-URI, or in BYE requests or responses.

```
<allOneLine>
Contact: <sip:+12125551212@gateway.example.com;uui=ZeGl9i2icVqaNVailT6
F5iJ90m6mvuTS4OK05M0vDk0Q4Xs>
</allOneLine>
```

An INVITE sent to this Contact URI would contain UUI in the Request-URI of the INVITE. The URI parameter has a drawback in that a URI parameter carried in a Request-URI will not survive retargeting by a proxy as shown in Figure 2 of [I-D.ietf-cuss-sip-uui-reqs] (Johnston, A., McMillen, J., and L. Liess, “Problem Statement and Requirements for Transporting User to User Call Control Information in SIP,” November 2010.). That is, if the URI is included with an Address of Record instead of a Contact URI, the URI parameter in the Reqeuest-URI will not be copied over to the Contact URI, resulting in the loss of the information. Note that if this same URI was present in a Refer-To header field, the same loss of information would occur.
The URI parameter approach would meet REQ-3, REQ-5, REQ-7, REQ-9, and REQ-11. It is possible the approach could meet REQ-12 and REQ-13. The mechanism does not appear to meet REQ-1, REQ-2, REQ-4, and REQ-14.

3.6. Header Field Approach

TOC

Another approach that has been proposed is to use a header field to transport the UUI information. The header field would be included in INVITE requests and responses and BYE requests and responses, and would pass transparently through proxies.
For redirection and referral use cases and REQ-3, the header field would be escaped into the Contact or Refer-To URI. Currently, UAs that support attended transfer support the ability to escape a Replaces header field into a Refer-To URI, and when acting upon this URI add the Replaces header field to the triggered INVITE. This logic and behavior is identical for the proposed UUI header field. As such, the existing running code for this behavior could be easily extended to allow this

to happen for the UUI header field. Note that this does require code changes in UAs.

To meet REQ-12 in redirection and referral use cases, a History-Info [I-D.ietf-sipcore-rfc4244bis] (Barnes, M., Audet, F., Schubert, S., Netherlands, T., and C. Holmberg, “An Extension to the Session Initiation Protocol (SIP) for Request History Information,” October 2010.) extension could be used. During redirection or retargeting, History-Info captures the history and the identity of the entity performing the redirection or referral. It seems likely that a new History-Info parameter could be defined to indicate that the UUI was inserted during this operation. The source of UUI inserted during redirection or referral could then be determined by examination of the History-Info header field.

The requirement for integrity protection in REQ-13 could be met by the use of an S/MIME signature over a subset of header fields, as defined in Section 23.4 of RFC 3261 "SIP Header Privacy and Integrity using S/MIME: Tunneling SIP". It could not be achieved using RFC 4474 without some sort of extension. The requirement for end-to-end privacy could be met using S/MIME or using encryption at the application layer. Note that the use of S/MIME to secure the UUI will result in an additional body being added to the request. However, note that neither S/MIME or RFC 4474 enjoys deployment in SIP today.

For example, here is an example User-to-User header field from message F1 in Figure 1 of [I-D.ietf-cuss-sip-uui-reqs] (Johnston, A., McMillen, J., and L. Liess, “Problem Statement and Requirements for Transporting User to User Call Control Information in SIP,” November 2010.):

```
User-to-User: 56a390f3d2b7310023a;encoding=hex;purpose=isdn-interwork
 ;content=isdn-uui
```

As another example, here is an escaped User-to-User header field from the redirection response F2 of Figure 3:

```
<allOneLine>
Contact: <sip:+12125551212@gateway.example.com?User-to-User=
56a390f3d2b7310023a%3Bencoding%3Dhex%3Bpurpose%3Disdn-interwork%3B
content%3Disdn-uui>
</allOneLine>
```

The resulting INVITE F5 would contain:

```
User-to-User: 56a390f3d2b7310023a;encoding=hex;purpose=isdn-interwork
 ;content=isdn-uui
```

An escaped User-to-User header field from the REFER message response F1 of Figure 4:

```
<allOneLine>
Refer-To: <sip:+12125551212@gateway.example.com?User-to-User=
56a390f3d2b7310023a%3Bencoding%3Dhex%3Bpurpose%3Disdn-interwork%3B
content%3Disdn-uui>
</allOneLine>
```

This would result in the INVITE F4 containing:

```
User-to-User: 56a390f3d2b7310023a;encoding=hex;purpose=isdn-interwork
 ;content=isdn-uui
```

The header field approach meets REQ-1, REQ-2, REQ-3, REQ-4, REQ-5, REQ-7, REQ-9, REQ-11, REQ-13, and REQ-14. The mechanism can likely meet REQ-12 with a History-Info extension.

---

4. Recommendation

TOC

The recommendation of this document is to define a new SIP header field "User-to-User" to transport call control UUI since this mechanism best supports the requirements in [I-D.ietf-cuss-sip-uui-reqs] (Johnston, A., McMillen, J., and L. Liess, “Problem Statement and Requirements for Transporting User to User Call Control Information in SIP,” November 2010.). There are also existing implementations and running code for this header field approach. The remainder of this document is a start at defining the details of the mechanism. Further work is needed.
To help tag and identify the UUI used with this header field, "purpose", "content", and "encoding" parameters are defined. This specification only defines "encoding=hex". Other specifications can define other purposes and contents for this header field per the requirements of this document.

---

5. Syntax for UUI Header Field

TOC

The User-to-User header field can be present in INVITE requests and responses only and in BYE requests and responses.
The following syntax specification uses the augmented Backus-Naur Form (BNF) as described in RFC 2234 and extends RFC 3261.

```
UUI          = "User-to-User" HCOLON uui-data *(SEMI uui-param)
uui-data     = token
uui-param    = enc-param | cont-param | purp-param | generic-param
enc-param    = "encoding="("hex" | token)
cont-param   = "content=" token
purp-param   = "purpose=" token
```

If the encoding parameter is not present, the default value of "hex" MUST be assumed. Other encoding methods of encoding MAY also be standardized.

User-to-User header fields with different purpose parameters may be present in a request or response. The number of User-to-User header fields which may be present in a request or response is defined for a particular purpose (application). Any size limitations on the UUI for a particular purpose must be defined by that purpose.

5.1. Definition of New Parameter Values

TOC

This specification defines only the values of "hex" for the "encoding" parameter. New values can be defined and added to the IANA registry with a standards track RFC, which needs to discuss the issues in this section.

New "encoding" values must reference a common encoding scheme or define the exact new encoding scheme.

New "content" values must describe the content of the UUI and give some example use cases. The default "encoding" and other allowed encoding methods must be defined for this new content.

New "purpose" values must describe the new purpose and give some example use cases. The default "content" value and other allowed contents must be defined for this new purpose. Any restrictions on the size of the UUI data must be described for the new purpose.

---

6. IANA Considerations

TOC

6.1. Registration of Header Field

TOC

This document defines a new SIP header field named "User-to-User".

The following row shall be added to the "Header Fields" section of the SIP parameter registry:

Header Name	Compact Form	Reference
User-to-User		[RFCXXXX]

Editor's Note: [RFCXXXX] should be replaced with the designation of this document.

6.2. Registration of Header Field Parameters

TOC

This document defines the parameters for the header field defined in the preceding section. The header field "User-to-User" can contain the parameters "encoding", "content", and "purpose".
The following rows shall be added to the "Header Field Parameters and Parameter Values" section of the SIP parameter registry:

Header Field	Parameter Name	Predefined Values	Reference
User-to-User	encoding	hex	[RFCXXXX]

Editor's Note: [RFCXXXX] should be replaced with the designation of this document.

6.3. Registration of SIP Option Tag

TOC

This specification registers a new SIP option tag, as per the guidelines in Section 27.1 of [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, “SIP: Session Initiation Protocol,” June 2002.).
This document defines the SIP option tag "uui".
The following row has been added to the "Option Tags" section of the SIP Parameter Registry:

```
+------------+----------------------------------------+-----------+
| Name       | Description                            | Reference |
+------------+----------------------------------------+-----------+
| uui        | This option tag is used to indicate that | [RFCXXXX] |
|            | a UA supports and understands the      |           |
|            | User-to-User header field.             |           |
+------------+----------------------------------------+-----------+
```

Editor's Note: [RFCXXXX] should be replaced with the designation of this document.

7. Security Considerations

TOC

User to user information can potentially carry sensitive information that might require privacy or integrity protection. Standard deployed SIP security mechanisms such as TLS transport, offer these properties on a hop-by-hop basis. To preserve multi-hop or end-to-end confidentiality and integrity of UUI, approaches using S/MIME or RFC 4474 can be used, as discussed in the draft. However, the lack of deployment of these mechanisms means that applications can not in general rely on them. As such, applications are encouraged to utilize their own security mechanisms.

8. Acknowledgements

TOC

Thanks to Spencer Dawkins, Keith Drage, Vijay Gurbani, and Laura Liess for their review of the document. The authors wish to thank Francois Audet, Denis Alexeitsev, Paul Kyzivat, Cullen Jennings, and Mahalingam Mani for their comments.

9. References

TOC

9.1. Informative References

TOC

[Q763]	"ITU-T Q.763 Signaling System No. 7 - ISDN user part formats and codes," http://www.itu.int/rec/T-REC-Q.931-199805-I/en .
[Q931]	

	"ITU-T Q.931 User to User Information Element (UU IE)," http://www.itu.int/rec/T-REC-Q.931-199805-I/en .
[ETSI]	"ETSI ETS 300 207-1 Ed.1 (1994), Integrated Services Digital Network (ISDN); Diversion supplementary services."
[RFC3372]	Vemuri, A. and J. Peterson, "Session Initiation Protocol for Telephones (SIP-T): Context and Architectures," BCP 63, RFC 3372, September 2002 (TXT).
[RFC2976]	Donovan, S., "The SIP INFO Method," RFC 2976, October 2000 (TXT).
[RFC4475]	Sparks, R., Hawrylyshen, A., Johnston, A., Rosenberg, J., and H. Schulzrinne, "Session Initiation Protocol (SIP) Torture Test Messages," RFC 4475, May 2006 (TXT).
[Q1980]	"ITU-T Q.1980.1 The Narrowband Signalling Syntax (NSS) - Syntax Definition," http://www.itu.int/itudoc/itu-t/aap/sg11aap/history/q1980.1/q1980.1.html .

9.2. Normative References

TOC

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3261]	Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261, June 2002 (TXT).
[RFC3324]	Watson, M., "Short Term Requirements for Network Asserted Identity," RFC 3324, November 2002 (TXT).
[I-D.ietf-cuss-sip-uui-reqs]	Johnston, A., McMillen, J., and L. Liess, "Problem Statement and Requirements for Transporting User to User Call Control Information in SIP," draft-ietf-cuss-sip-uui-reqs-00 (work in progress), November 2010 (TXT).
[RFC4474]	Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," RFC 4474, August 2006 (TXT).
[I-D.ietf-sipcore-rfc4244bis]	Barnes, M., Audet, F., Schubert, S., Netherlands, T., and C. Holmberg, "An Extension to the Session Initiation Protocol (SIP) for Request History Information," draft-ietf-sipcore-rfc4244bis-02 (work in progress), October 2010 (TXT).

Authors' Addresses

TOC

	Alan Johnston
	Avaya
	St. Louis, MO 63124
Email:	alan.b.johnston@gmail.com
	Joanne McMillen
	Unaffiliated
Email:	c.joanne.mcmillen@gmail.com
	James Rafferty
	Dialogic
Email:	james.rafferty@dialogic.com