Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 12, 2012

A. Johnston
Avaya
J. Rafferty
Dialogic

July 11, 2011

A Mechanism for Transporting User to User Call Control Information in SIP

draft-ietf-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. This document defines a new SIP header field, User-to-User, to transport UUI, along with an extension mechanism.

Status of this Memo

Copyright Notice

Table of Contents

1. Overview

This document describes the transport of User to User Information (UUI) using SIP [RFC3261]. 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] and ITU-T Q.763 User to User Information Parameter [Q763] 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]. All references to requirement numbers (REQ-N) and figure numbers refer to this document.

The mechanism chosen is a new SIP header field, along with a new SIP option tag and media feature tag. The header field carries the UUI information, along with parameters indicating the encoding of the UUI, the application user of the UUI, and optionally the content of the UUI. The header field can be escaped into URIs supporting referral and redirection scenarios. In these scenarios, History-Info is used to indicate the inserter of the UUI. The SIP option tag is used to indicate support for the header field. Support for the header field indicates that a UA is able to extract the information in the UUI and pass it up the protocol stack. The media feature tag is used to indicate that a UA supports a particular application user of UUI.

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 BCP 14, RFC 2119 [RFC2119].

3. Requirements Discussion

This section describes how the User-to-User header field meets the requirements in [I-D.ietf-cuss-sip-uui-reqs]. The header field can be included in INVITE requests and responses and BYE requests and responses, meeting REQ-1 and REQ-2.

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 UUI header field. The UA processing the REFER or the 3xx to the INVITE will need to support the UUI mechanism, as UAs in general do not process unknown escaped header fields.

Since SIP proxy forwarding and retargeting does not affect header fields, the header field meets REQ-4.

The UUI header field will carry the UUI data and not a pointer to the data, so REQ-5 is met.

Since the basic design of the UUI header field is similar to the ISDN UUI service, interworking with PSTN protocols will be straightforward and will be documented in a separate specification, meeting REQ-6

Requirements REQ-7, REQ-8, and REQ-10 relate to discovery of the mechanism and supported applications. REQ-7 relates to support of the UUI header field, while REQ-8 relates to routing based on support of the UUI header field. REQ-7 is 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. The presence of a Supported:uui or Require:uui header field can be used by proxies to route to an appropriate UA, meeting REQ-8. REQ-10 is 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, app1.

Proxies commonly apply policy to the presence of certain SIP header fields in requests by either passing them or removing them from requests. REQ-9 is met by allowing proxies and other intermediaries to remove UUI header fields in a request or response based on policy.

Carrying UUI data elements of at least 129 octets is trivial in the UUI header field, meeting REQ-11. Note that very large UUI elements should be avoided, as SIP header fields have traditionally not been large.

To meet REQ-12 in redirection and referral use cases, History-Info [I-D.ietf-sipcore-rfc4244bis] can be used. In these retargeting cases, the changed Request-URI will be recorded in the History-Info header field along with the identity of the element that performed the retargeting.

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". The requirement of REQ-14 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. Hopwise TLS allows the header field to meet REQ-15 for hop-by-hop security.

4. Normative Definition

This document defines a new SIP header field "User-to-User" to transport call control UUI to meet the requirements in [I-D.ietf-cuss-sip-uui-reqs].

To help tag and identify the UUI used with this header field, "app", "content", and "encoding" parameters are defined. The "app" parameter identifies the application which generates and consumes the UUI information. For the case of interworking with the ISDN UUI Service, the application is unknown, so a value to indicate ISDN UUI Service interworking will be defined. If the "app" parameter is not present, interworking with the ISDN UUI Service MUST be assumed. The "content" parameter identifies the actual content of the UUI data. If not present, the content MUST be assumed to be unknown as it is in the ISDN UUI Service. For newly defined applications using the SIP UUI service, a "content" value MUST be defined and SHOULD be used. The "encoding" parameter indicates the method of encoding the information in the UUI. This specification only defines "encoding=hex". If the "encoding" parameter is not present, "hex" MUST be assumed.

4.1. Syntax for UUI Header Field

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 | app-param | generic-param
enc-param   = "encoding="("hex" | token)
cont-param  = "content=" token
app-param   = "app=" token
```

User-to-User header fields with different "app" 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 application. Any size limitations on the UUI for a particular purpose must be defined by that application.

4.2. Definition of New Parameter Values

This specification defines only the value 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 "app" values must describe the new application which is utilizing the UUI data 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 application.

5. IANA Considerations

5.1. Registration of Header Field

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.

5.2. Registration of Header Field Parameters

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.

5.3. Registration of SIP Option Tag

This specification registers a new SIP option tag, as per the guidelines in Section 27.1 of [RFC3261].

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 a UA supports and understands the User-to-User header field.	[RFCXXXX]

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

Registration of SIP media feature tag is TBD.

6. Security Considerations

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 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.

7. Appendix - Other Possible Mechanisms

Two other possible mechanisms for transporting UUI will be described: MIME body and URI parameter transport.

7.1. Why INFO is Not Used

Since the INFO method [RFC2976], 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] 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.

7.2. Why Other Protocol Encapsulation UUI Mechanisms are Not Used

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] and the ITU-T Q.763 User to User Information Parameter [Q763]. In addition, NSS (Narrowband Signaling System) [Q1980] 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.

7.3. MIME body Approach

One method of transport is to use a MIME body. This is in keeping with the SIP-T architecture [RFC3372] 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 [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 [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.

7.4. URI Parameter

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]. 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.

8. Acknowledgements

Joanne McMillen was a major contributor and co-author of earlier versions of this document. 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

9.1. Informative References

[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.

[RFC2976] Donovan, S., "The SIP INFO Method", RFC 2976, October 2000.

[RFC4475] Sparks, R., Hawrylyshen, A., Johnston, A., Rosenberg, J., and H. Schulzrinne, "Session Initiation Protocol (SIP) Torture Test Messages", RFC 4475, May 2006.

[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

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

[RFC3324] Watson, M., "Short Term Requirements for Network Asserted Identity", RFC 3324, November 2002.

[I-D.ietf-cuss-sip-uui-reqs] Johnston, A. and L. Liess, "Problem Statement and Requirements for Transporting User to User Call Control Information in SIP", draft-ietf-cuss-sip-uui-reqs-02 (work in progress), May 2011.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

[I-D.ietf-sipcore-rfc4244bis] Barnes, M., Audet, F., Schubert, S., Gmbh, D., and C. Holmberg, "An Extension to the Session Initiation Protocol (SIP) for Request History Information", draft-ietf-sipcore-rfc4244bis-05 (work in progress), April 2011.

Authors' Addresses

Alan Johnston
Avaya
St. Louis, MO 63124

Email: alan.b.johnston@gmail.com

James Rafferty
Dialogic

Email: james.rafferty@dialogic.com