

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

This Internet-Draft is submitted to IETF 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 January 12, 2012.

Copyright Notice

Copyright (c) 2011 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 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. Overview	3
2. Terminology	3
3. Requirements Discussion	3
4. Normative Definition	5
4.1. Syntax for UUI Header Field	5
4.2. Definition of New Parameter Values	6
5. IANA Considerations	6
5.1. Registration of Header Field	6
5.2. Registration of Header Field Parameters	7
5.3. Registration of SIP Option Tag	7
6. Security Considerations	7
7. Appendix - Other Possible Mechanisms	8
7.1. Why INFO is Not Used	8
7.2. Why Other Protocol Encapsulation UUI Mechanisms are Not Used	8
7.3. MIME body Approach	9
7.4. URI Parameter	10
8. Acknowledgements	10
9. References	10
9.1. Informative References	10
9.2. Normative References	11
Authors' Addresses	12

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.appl' could be used to indicate support for a particular application, appl.

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 Request-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/ql980.1/ql980.1.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

CUSS WG
Internet-Draft
Intended status: Informational
Expires: January 12, 2012

A. Johnston
Avaya
L. Liess
Deutsche Telekom AG
July 11, 2011

Problem Statement and Requirements for Transporting User to User Call
Control Information in SIP
draft-ietf-cuss-sip-uui-reqs-03

Abstract

This document introduces the transport of call control related User to User Information (UUI) using the Session Initiation Protocol (SIP), and develops several requirements for a new SIP mechanism. Some SIP sessions are established by or related to a non-SIP application. This application may have information that needs to be transported between the SIP User Agents during session establishment. In addition to interworking with the ISDN UUI Service, this extension will also be used for native SIP endpoints requiring application UUI.

Status of this Memo

This Internet-Draft is submitted to IETF 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 January 12, 2012.

Copyright Notice

Copyright (c) 2011 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 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. Overview	3
2. Use Cases	4
2.1. User Agent to User Agent	4
2.2. Proxy Retargeting	4
2.3. Redirection	5
2.4. Referral	6
3. Requirements	7
4. Security Considerations	8
5. Acknowledgements	10
6. Informative References	10
Authors' Addresses	11

1. Overview

This document describes the transport of User to User Information (UUI) during SIP session setup. This section introduces UUI and explains how it relates to SIP.

We define SIP UUI information as application-specific information that is related to a session being established using SIP. It is assumed that the application is running in both endpoints in a two party session. That is, the application interacts with both the User Agents in a SIP session. In order to function properly, the application needs a small piece of information, the UUI, to be transported at the time of session establishment. This information is essentially opaque data to SIP - it is unrelated to SIP routing, authentication, or any other SIP function. This application can be considered to be operating at a higher layer on the protocol stack. As a result, SIP should not interpret, understand, or perform any operations on the UUI. Should this not be the case, then the information being transported is not considered UUI, and another SIP-specific mechanism will be needed to transport the information (such as a new header field).

UUI is defined this way for two reasons. Firstly, this supports a strict layering of protocols and data. Providing information and understanding of the UUI to the transport layer (SIP in this case) would not provide any benefits and instead could create cross layer coupling. Secondly, it is neither feasible nor desirable for a SIP User Agent (UA) to understand the information; instead the goal is for the UA to simply pass the information as efficiently as possible to the application which does understand the information.

An important application is the interworking with User to User Information (UUI) in ISDN, specifically, the transport of the 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. ISDN UUI is widely used in the PSTN today in contact centers and call centers. These applications are currently transitioning away from using ISDN for session establishment to using SIP. Native SIP endpoints will need to implement a similar service and be able to interwork with this ISDN service.

Note that the distinction between call control UUI and non-call control UUI is very important. SIP already has a mechanism for sending arbitrary UUI information between UAs during a session or dialog - the SIP INFO [RFC2976] method. Call control UUI, in contrast, must be exchanged at the time of setup and needs to be carried in the INVITE and a few other methods and responses. Applications that exchange UUI but do not have a requirement that it

be transported and processed during call setup can simply use SIP INFO and do not need a new SIP extension.

In this document, four different use case call flows are discussed. Next, the requirements for call control UUI transport are discussed.

2. Use Cases

This section discusses four use cases for the transport of call control related user to user information. What is not discussed here is the transport of non-call control UUI which can be done using the SIP INFO method. These use cases will help motivate the requirements for SIP call control UUI.

2.1. User Agent to User Agent

In this scenario, the originator UA includes UUI in the INVITE sent through a proxy to the terminating UA. The terminator can use the UUI in any way. If it is an ISDN gateway, it could map the UUI into the appropriate DSS1 information element or QSIG information element or ISUP parameter. Alternatively, the using application might render the information to the user, or use it during alerting or as a lookup for a screen pop. In this case, the proxy does not need to understand the UUI mechanism, but normal proxy rules should result in the UUI being forwarded without modification. This call flow is shown in Figure 1.

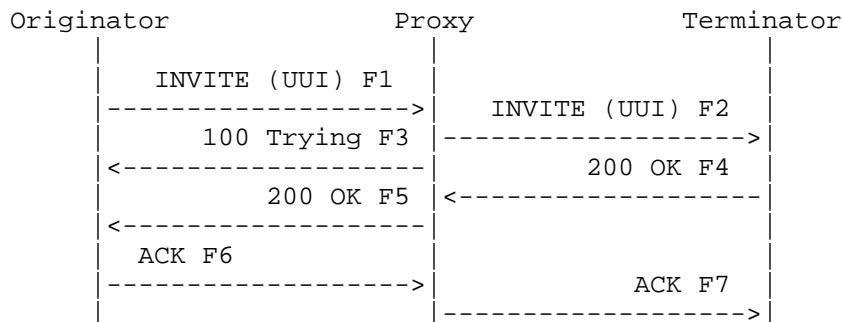


Figure 1. Call flow with UUI exchanged between Originator and Terminator.

2.2. Proxy Retargeting

In this scenario, the originator UA includes UUI in the INVITE sent through a proxy to the terminating UA. The proxy retargets the INVITE, sending it to a different termination UA. The UUI

information is then received and processed by the terminating UA. This call flow is identical to Figure 1 but with a different destination for the INVITE. The UUI in the INVITE needs to be passed unchanged through this proxy retargeting operation.

2.3. Redirection

In this scenario, UUI is inserted by an application which utilizes a SIP redirect server. The UUI is then included in the INVITE sent by the Originator to the Terminator. In this case, the Originator does not necessarily need to support the UUI mechanism but does need to support the SIP redirection mechanism used to include the UUI information. Two examples of UUI with redirection (transfer and diversion) are defined in [ANSII] and [ETSI].

Note that this case may not precisely map to an equivalent ISDN service use case. This is because there is no one-to-one mapping between elements in a SIP network and elements in an ISDN network. Also, there is not an exact one-to-one mapping between SIP call control and ISDN call control. However, this should not prevent the usage of SIP call control UUI in these cases. Instead, these slight differences between the SIP UUI service and the ISDN service need to be carefully noted and discussed in an interworking specification.

Figure 2 shows this scenario, with the Redirect inserting UUI which is then included in the INVITE F4 send to the Terminator.

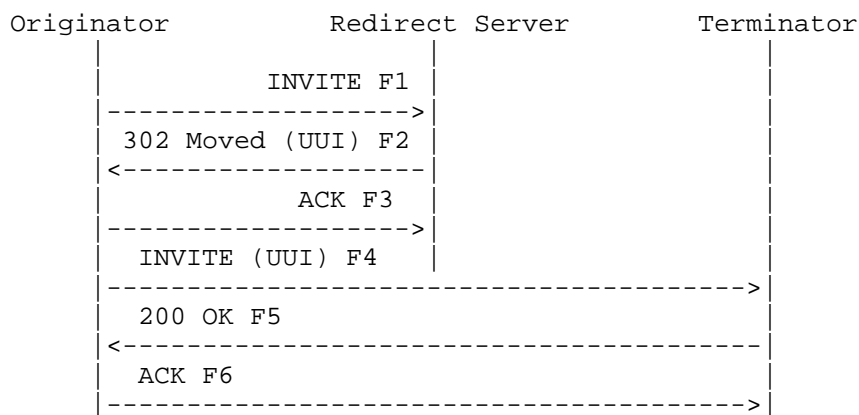


Figure 2. Call flow with UUI exchanged between Redirect Server and Terminator.

A common example application of this call flow is an Automatic Call Distributer (ACD) in a PSTN contact center. The originator would be a PSTN gateway. The ACD would act as a Redirect Server, inserting

UUI based on called number, calling number, time of day, and other information. The resulting UUI would be passed to the agent's handset which acts as the Terminator. The UUI could be used to lookup information for rendering to the agent at the time of call answering.

This redirection scenario, and the referral scenario in the next section, are the most important scenarios for contact center applications. Incoming calls to a contact center almost always are redirected or referred to a final destination, sometimes multiple times, based on collected information and business logic. The ability to pass along UUI in these call redirection scenarios is critical.

2.4. Referral

In this scenario, the application uses a UA to initiate a referral, which causes an INVITE to be generated between the Originator and Terminator with UUI information inserted by the Referrer UA. Note that this REFER [RFC3515] could be part of a transfer operation or it might be unrelated to an existing call, such as out-of-dialog REFER. In some cases, this call flow is used in place of the redirection call flow where immediately upon answer, the REFER is sent. This scenario is shown in Figure 3.

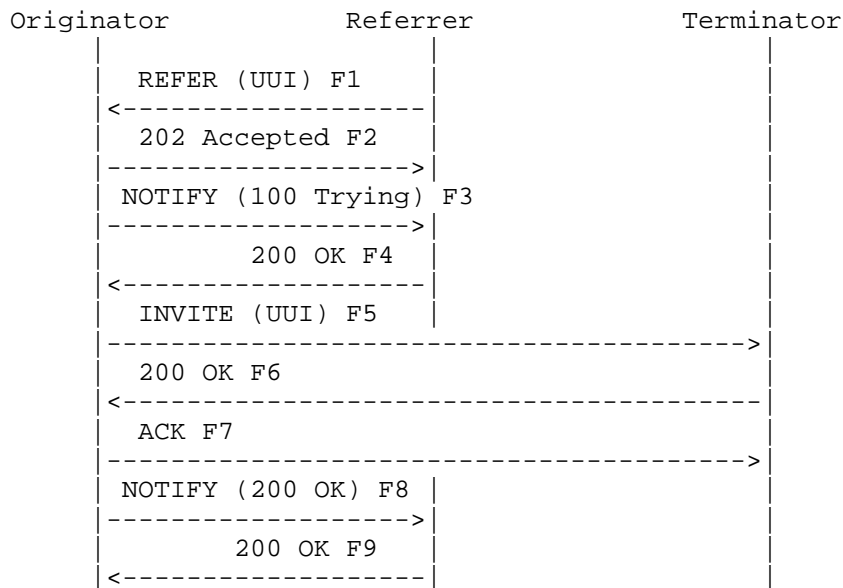


Figure 3. Call flow with Referral and UUI.

3. Requirements

This section states the requirements for the transport of call control related user to user information (UUI).

REQ-1: The mechanism will allow UAs to insert and receive UUI data in SIP call setup requests and responses.

SIP messages covered by this include INVITE requests and end-to-end responses to the INVITE, which includes 18x, 200, and 3xx responses.

REQ-2: The mechanism will allow UAs to insert and receive UUI data in SIP dialog terminating requests and responses.

Q.931 UUI supports inclusion in release and release completion messages. SIP messages covered by this include BYE and 200 OK responses to a BYE.

REQ-3: The mechanism will allow UUI to be inserted and retrieved in SIP redirects and referrals.

SIP messages covered by this include REFER requests and 3xx responses to INVITE requests.

REQ-4: The mechanism will allow UUI to be able to survive proxy retargeting or any other form of redirection of the request.

Retargeting is a common method of call routing in SIP, and must not result in the loss of user to user information.

REQ-5: The mechanism should not require processing entities to dereference a URL in order to retrieve the UUI information.

Passing a pointer or link to the UUI information will not meet the real-time processing considerations and would complicate interworking with the PSTN.

REQ-6: The mechanism will support interworking with call control related DSS1 information elements or QSIG information elements or ISUP parameters.

REQ-7: The mechanism will allow a UAC to learn that a UAS understands the UUI mechanism.

REQ-8: The mechanism will allow a UAC to require that a UAS understands the call control UUI mechanism have a request routed based on this information.

This could be useful in ensuring that a request destined for the PSTN is routed to a gateway that supports the UUI mechanism rather than an otherwise equivalent PSTN gateway that does not support the ISDN mechanism. Note that support of the UUI mechanism does not, by itself, imply that a particular application is supported - see REQ-10.

REQ-9: The mechanism will allow proxies to remove a particular application usage of UUI information from a request or response.

This is a common security function provided by border elements to header fields such as Alert-Info or Call-Info URIs.

REQ-10: The mechanism will provide the ability for a UA to discover which application usages of UUI another UA understands or supports.

The creation of a registry of application usages for the SIP UUI mechanism is implied by this requirement. The ISDN Service utilizes a field known as the protocol discriminator, which is the first octet of the ISDN UUI information, for this purpose.

REQ-11: The solution will provide a mechanism of transporting at least 128 octets of user data and a one octet protocol discriminator, i.e. 129 octets in total.

There is the potential for non-ISDN services to allow UUI to be larger than 128 octets. However, users of the mechanism will need be cognizant of the size of SIP messages and the ability of parsers to handle extremely large values.

REQ-12: The recipient of UUI will be able to determine the entity that inserted the UUI. It is acceptable that this is performed implicitly where it is known that there is only one other end UA involved in the dialog. Where that does not exist, some other mechanism will need to be provided.

This requirement comes into play during redirection, retargeting, and referral scenarios.

4. Security Considerations

The security requirements for the SIP UUI mechanism are described in this section. It is important to note that UUI security is jointly provided at the application layer and at the SIP layer. As such, is important for application users of SIP UUI to know the realistic level of security used and deployed in SIP, and not assume that some rarely deployed SIP level security mechanism is in place.

There are two main security models that need to be addressed by the SIP UUI mechanism. One model treats the SIP layer as untrusted and requires end-to-end integrity protection and/or encryption. This model can be achieved by providing these security services at a layer above SIP. In this case, the application integrity protects and/or encrypts the UUI information before passing it to the SIP layer. This method has two advantages: it does not assume or rely on end-to-end security mechanisms in SIP which have virtually no deployment, and allows the application which understands the contents of the UUI to apply a proper level of security. The other approach is for the application to pass the UUI without any protection to the SIP layer and require the SIP layer to provide this security. This approach is possible in theory, although its practical use would be extremely limited. The SIP UUI mechanism should support both of these approaches.

The other model utilizes a trust domain and relies on perimeter security at the SIP layer. This is the security model of the PSTN and ISDN where UUI is commonly used today. This approach uses hop-by-hop security mechanisms and relies on border elements for filtering and application of policy. This approach is used today in SIP UUI deployments. However, there is no requirement that an intermediary element be able to read or interpret the UUI, as UUI only has end-to-end significance. An intermediary element may remove a UUI element based on policy, however. This SIP UUI mechanism needs to support this model.

The next three requirements capture the SIP UUI security requirements.

REQ-13: The mechanism will allow integrity protection of the UUI.

This allows the UAS to be able to know that the UUI has not been modified or tampered with by intermediaries. This property is not guaranteed by the protocol in the ISDN application.

REQ-14: The mechanism will allow end-to-end privacy of the UUI.

Some UUI may contain private or sensitive information and may require different security handling from the rest of the SIP message. Note that this property is not available in the ISDN application.

REQ-15: The mechanism will allow both end-to-end and hop-by-hop security models.

The hop-by-hop model is required by the ISDN UUI service.

5. Acknowledgements

Thanks to Joanne McMillen who was a co-author of earlier versions of this specification. Thanks to Spencer Dawkins, Keith Drage, and Vijay Gurbani for their review of earlier versions of this document. The authors wish to thank Christer Holmberg, Frederique Forestie, Francois Audet, Denis Alexeitsev, Paul Kyzivat, Cullen Jennings, and Mahalingam Mani for their comments on this topic.

6. Informative References

- [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.
- [Q931] "ITU-T Q.931 User to User Information Element (UU IE)", <http://www.itu.int/rec/T-REC-Q.931-199805-I/en> .
- [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> .
- [ANSII] "ANSI T1.643-1995, Telecommunications-Integrated Services Digital Network (ISDN)-Explicit Call Transfer Supplementary Service".
- [ETSI] "ETSI ETS 300 207-1 Ed.1 (1994), Integrated Services Digital Network (ISDN); Diversion supplementary services".
- [QSIG] "ECMA-143 "Private Integrated Services Network (PISN) - Circuit Mode Bearer Services - Inter-Exchange Signalling Procedures and Protocol" December 2001".
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2976] Donovan, S., "The SIP INFO Method", RFC 2976, October 2000.
- [RFC3372] Vemuri, A. and J. Peterson, "Session Initiation Protocol for Telephones (SIP-T): Context and Architectures", BCP 63, RFC 3372, September 2002.

[RFC3515] Sparks, R., "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, April 2003.

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

Authors' Addresses

Alan Johnston
Avaya
St. Louis, MO 63124

Email: alan.b.johnston@gmail.com

Laura Liess
Deutsche Telekom AG

Email: laura.liess.dt@gmail.com

