

This Internet-Draft, draft-drage-cuss-sip-uu-isdn-00.txt, has expired, and has been deleted from the Internet-Drafts directory. An Internet-Draft expires 185 days from the date that it is posted unless it is replaced by an updated version, or the Secretariat has been notified that the document is under official review by the IESG or has been passed to the RFC Editor for review and/or publication as an RFC. This Internet-Draft was not published as an RFC.

Internet-Drafts are not archival documents, and copies of Internet-Drafts that have been deleted from the directory are not available. The Secretariat does not have any information regarding the future plans of the authors or working group, if applicable, with respect to this deleted Internet-Draft. For more information, or to request a copy of the document, please contact the authors directly.

Draft Authors:

Keith Drage<keith.drage@alcatel-lucent.com>

Alan Johnston<alan.b.johnston@gmail.com>

Joanne McMillen<c.joanne.mcmillen@gmail.com>

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: June 17, 2011

A. Johnston  
Avaya  
J. McMillen  
Unaffiliated  
J. Rafferty  
Dialogic  
December 14, 2010

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

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 June 17, 2011.

Copyright Notice

Copyright (c) 2010 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. Possible Mechanisms . . . . .	3
3.1. Why INFO is Not Used . . . . .	3
3.2. Why Other Protocol Encapsulation UII Mechanisms are Not Used . . . . .	3
3.3. Discovery Mechanism . . . . .	4
3.4. MIME body Approach . . . . .	4
3.5. URI Parameter . . . . .	5
3.6. Header Field Approach . . . . .	6
4. Recommendation . . . . .	7
5. Syntax for UII Header Field . . . . .	8
5.1. Definition of New Parameter Values . . . . .	8
6. IANA Considerations . . . . .	9
6.1. Registration of Header Field . . . . .	9
6.2. Registration of Header Field Parameters . . . . .	9
6.3. Registration of SIP Option Tag . . . . .	9
7. Security Considerations . . . . .	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.

## 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. Possible Mechanisms

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

### 3.1. 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.

### 3.2. 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.

### 3.3. Discovery Mechanism

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

### 3.4. 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.

### 3.5. 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.

### 3.6. Header Field Approach

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] 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]:

```
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

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]. 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

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

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

### 6.1. 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.

### 6.2. 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.

### 6.3. 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.

## 7. 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 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

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., 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.
- [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., 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.

Authors' Addresses

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



CUSS WG  
Internet-Draft  
Intended status: Informational  
Expires: March 19, 2011

A. Johnston, Ed.  
Avaya  
J. McMillen  
Unaffiliated  
L. Liess  
Deutsche Telekom AG  
September 15, 2010

Problem Statement and Requirements for Transporting User to User Call  
Control Information in SIP  
draft-johnston-cuss-sip-uui-reqs-00

Abstract

This document introduces the transport of call control related User to User Information (UUI) in 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. A common example in another protocol is the ITU-T Q.931 User to User Information Service. 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 requirements and approaches. This extension will also be used for native SIP endpoints implementing similar services and interworking with ISDN services. Example use cases include an exchange between two user agents, retargeting by a proxy, and redirection. An example application is an Automatic Call Distributor (ACD) in a contact center.

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 March 19, 2011.

Copyright Notice

Copyright (c) 2010 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 . . . . .	4
2. Terminology . . . . .	4
3. Use Cases . . . . .	5
3.1. User Agent to User Agent . . . . .	5
3.2. Proxy Retargeting . . . . .	5
3.3. Redirection . . . . .	6
3.4. Referral . . . . .	7
4. Requirements . . . . .	9
5. Security Considerations . . . . .	11
6. Acknowledgements . . . . .	11
7. Informative References . . . . .	11
Authors' Addresses . . . . .	12

## 1. Overview

This document describes the transport of User to User Information (UUI) during session setup. This section will introduce UUI and explain 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 the originator of the session and the terminator of the session. That is, the application interacts with the User Agent Client (UAC) and User Agent Server (UAS). In order to function, the application needs 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 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 would not provide any benefits and instead could create cross layer coupling. Secondly, it is neither feasible nor desirable for a SIP User Agent to understand the information but instead the goal is for the User Agent to pass the information as efficiently as possible to an application which does understand the information.

An important application is the interworking with User to User Information (UUI) in ISDN, specifically, 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. 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.

In the rest of this document, the requirements are discussed with use cases. Five different use case call flows are then discussed.

## 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. 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.

#### 3.1. 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 Q.931 or Q.763 element. 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.

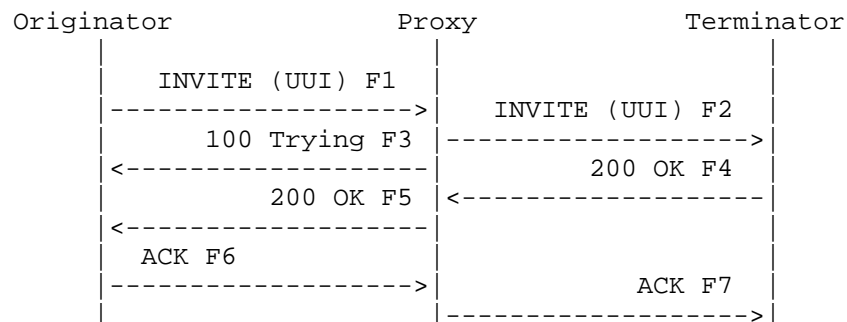


Figure 1. Call flow with UUI exchanged between Originator and Terminator.

#### 3.2. 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 shown in Figure 2.

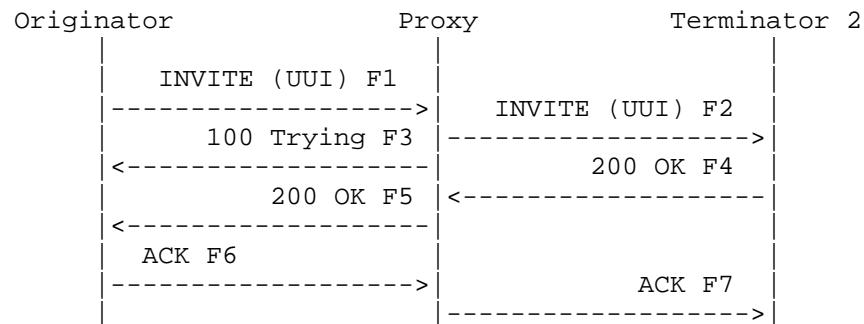


Figure 2. Call flow with Proxy Retargeting.

The UUI in the INVITE needs to be passed unchanged through this proxy retargeting operation.

### 3.3. 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 [ANSI] 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.

In redirection scenarios, if the Redirect Server is not in the same administrative domain as the Terminator, the Redirect Server must not remove or replace any UUI in the initial INVITE. In Figure 3, this means that if F1 included UUI, the Redirect Server could not modify or replace the UUI in F2. However, if the Redirect Server and the Terminator are part of the same administrative domain, they may have a policy allowing the Redirect Server to modify or rewrite UUI information. In fact, many UUI uses within an Enterprise rely on this feature to work today in ISDN.

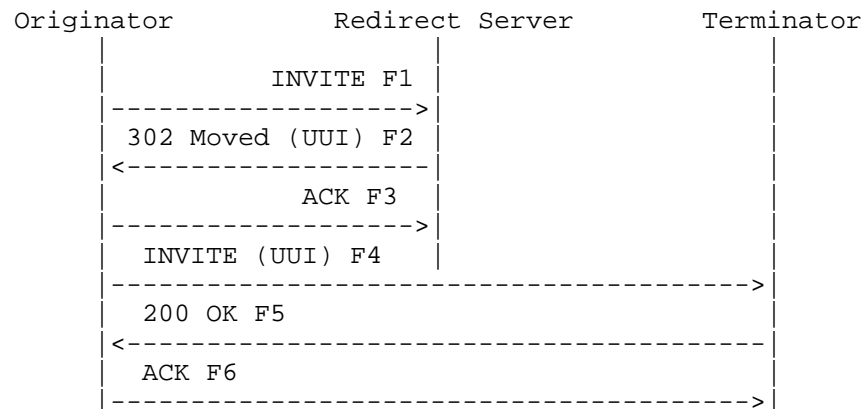


Figure 3. Call flow with UUI exchanged between Redirect Server and Terminator

A common 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 rendered 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 maintain UUI in these scenarios is critical.

### 3.4. Referral

In this scenario, application uses a UA 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 call control. In some cases, this call flow is used in place of the redirection call flow, but where immediately upon answer, the REFER is sent. This scenario is shown in Figure 4.

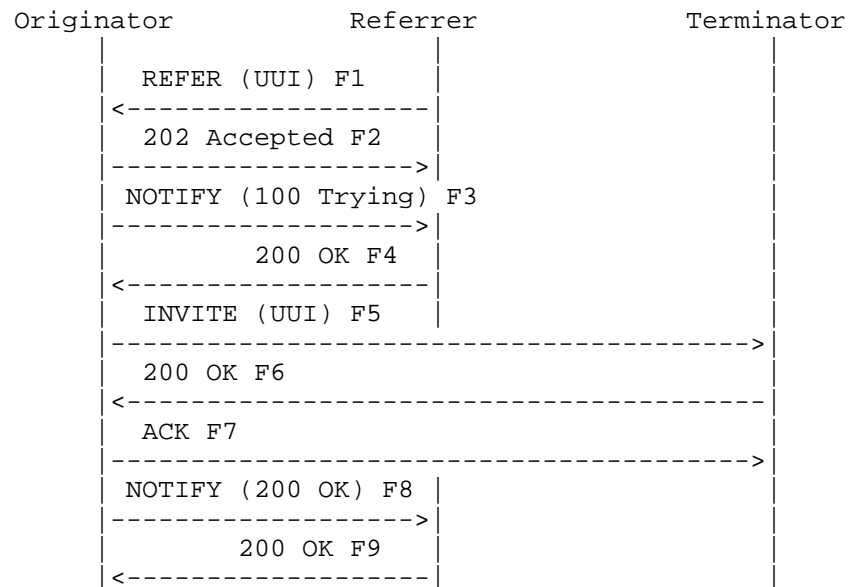


Figure 4. Call flow with transfer after answer.

Some scenarios involving referral have been proposed to use a REFER sent during an early dialog. This NOT RECOMMENDED call flow is shown in Figure 5. This flow is not recommended due to the number of messages exchanged (due to the REFER, CANCEL, and 487 responses) and the sending of the REFER in the early dialog. Also, there are race conditions that can occur if a 200 OK to the INVITE is received by the Originator while the REFER is in progress.

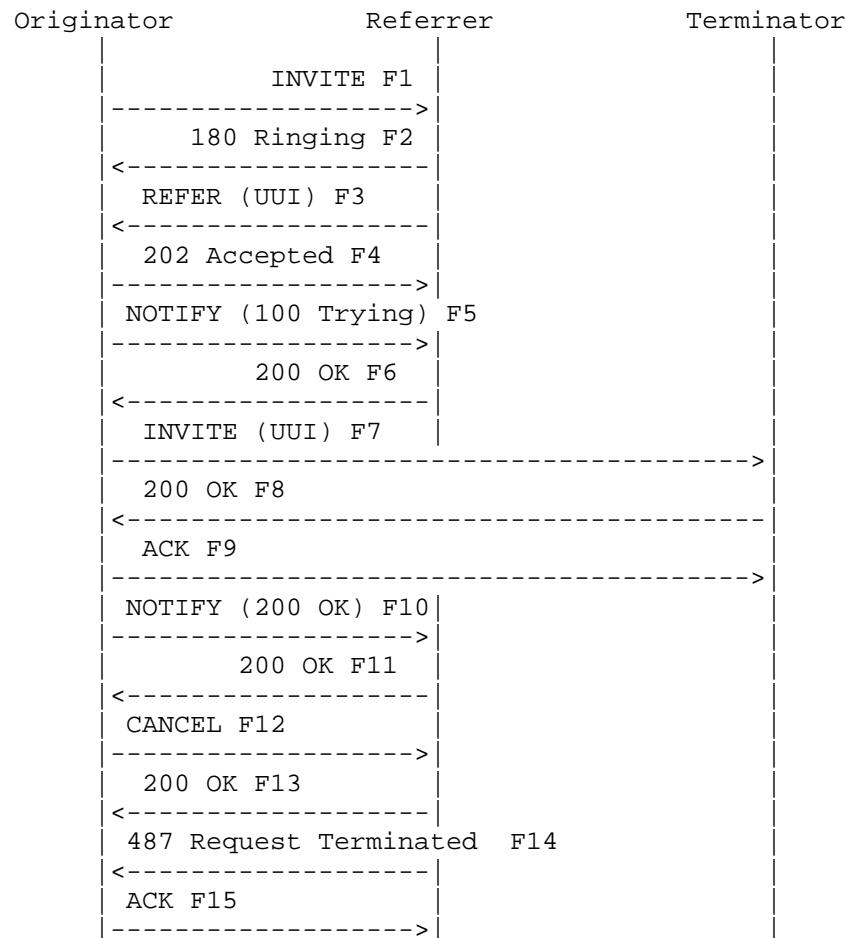


Figure 5. NOT RECOMMENDED call flow showing REFER prior to answer.

#### 4. Requirements

This section discusses the requirements for the transport of call control related user to user information (UUI). We define call control UUI as information that is generated, transported, and consumed at the time of call setup (i.e. during a pending INVITE transaction). The information can be used for call routing, alerting, call distribution, or simply rendering. The exact usage and semantics of call control UUI is out of scope - SIP is simply providing the transport function for this, in the same manner as the ISDN service provides in the PSTN. Non-call control UUI can be sent using the INFO method, and is outside the scope of this work.

REQ-1: The mechanism will allow user agents (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 and 200 responses.

REQ-2: The mechanism will allow UAs to insert and receive UUI data in SIP call teardown 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 to INVITES.

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

REQ-4: The mechanism will allow UUI to be able to survive proxy retargeting.

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 to retrieve the UUI information.

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

REQ-6: The mechanism will minimize reliance on SIP extensions or uncommon SIP behavior.

REQ-7: The mechanism will support interworking with 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].

REQ-8: The mechanism will allow the inserter of UUI to be sure that the recipient understands the call control UUI mechanism.

Understanding the mechanism means that the UAS will extract and utilize the UUI information transported. Understanding the protocol, format, and nature of the actual UUI data is not covered by this requirement. Note that this requirement is not strictly needed to implement the UUS 1 implicit service, but maps more accurately to the UUS 1 explicit service. However, having an



option tag is good design for high reliability systems, and the dynamic and heterogeneous nature of SIP interconnection (as opposed to the PSTN's static trunking) makes this option tag much more important and hence relevant to even the UUS 1 implicit service.

REQ-9: The mechanism will allow proxies to remove a particular type of UUI information from a request or response, or to block requests based on the presence of a particular type of UUI.

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

## 5. Security Considerations

User to user information can be exchanged over SIP on a hop-by-hop or end-to-end basis. In some cases, UUI may carry privacy information that would require confidentiality and message integrity. Standard SIP security mechanisms, viz., based on TLS, offer these properties per-hop. To preserve multi-hop or end-end confidentiality and integrity, an S/MIME profile MUST be utilized. Since the security requirements and key management of the UUI information are likely to be quite different from the SIP signaling transport, another approach would be for the UUI information to be encrypted before being passed to SIP for transport.

Received User-to-User information should only be trusted if it is authenticated or if it is received within a trust domain. For example, Spec-T, defined in [RFC3324] could be used to define a trust domain. When utilized by a gateway to map information to or from ISDN Q.931 and ISUP Q.763, appropriate policy should be applied based on the PSTN trust domain.

## 6. Acknowledgements

Thanks to Spencer Dawkins, Keith Drage, and Vijay Gurbani for their review of earlier versions of this document. The authors wish to thank Francois Audet, Denis Alexeitsev, Paul Kyzivat, Cullen Jennings, and Mahalingam Mani for their comments on this topic.

## 7. 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".
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate  
Requirement Levels", BCP 14, RFC 2119, March 1997.
- [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.
- [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 (editor)  
Avaya  
St. Louis, MO 63124

Email: [alan.b.johnston@gmail.com](mailto:alan.b.johnston@gmail.com)

Joanne McMillen  
Unaffiliated

Email: [c.joanne.mcmillen@gmail.com](mailto:c.joanne.mcmillen@gmail.com)

Laura Liess  
Deutsche Telekom AG

Email: [laura.liess.dt@gmail.com](mailto:laura.liess.dt@gmail.com)

