Internet Engineering Task Force (IETF)
Request for Comments: 7433
Category: Standards Track
ISSN: 2070-1721

A. Johnston
Avaya
J. Rafferty
Human Communications

January 2015

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

Abstract

There is a class of applications that benefit from using SIP to exchange User-to-User Information (UUI) data during session establishment. This information, known as call control UUI data, is a small piece of data inserted by an application initiating the session and utilized by an application accepting the session. The syntax and semantics for the UUI data used by a specific application are defined by a UUI package. This UUI 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 data, along with an extension mechanism.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7433.

Table of Contents

1. Overview

This document describes the transport of UUI data using SIP [RFC3261]. It defines a mechanism for the transport of general application UUI data and for the transport of the call control related ITU-T Recommendation Q.931 User-user information element [Q931] and ITU-T Recommendation Q.763 User-to-User information parameter [Q763] data in SIP. UUI data is widely used in the Public Switched Telephone Network (PSTN) today for contact centers and call centers. There is also a trend for the related applications to transition from ISDN to SIP. The UUI extension for SIP may also be used for native SIP User Agents (UAs) implementing similar services and to interwork with ISDN services. Note that in most cases, there is an a priori understanding between the UAs in regard to what to do with received UUI data. This document enables the definition of packages and related attributes that can make such understandings more explicit.

The UUI mechanism is designed to meet the use cases, requirements, and call flows for SIP call control UUI detailed in [RFC6567]. All references to requirement numbers (REQ-N) and figure numbers refer to [RFC6567].

The mechanism is a new SIP header field, along with a new SIP option tag. The header field carries the UUI data, along with parameters indicating the encoding of the UUI data, the UUI package, and optionally the content of the UUI data. The package definition contains details about how a particular application can utilize the UUI mechanism. The header field can be included (sometimes called "escaped") into URIs supporting referral and redirection scenarios. In these scenarios, the History-Info header field is used to indicate the inserter of the UUI data. The SIP option tag can be used to indicate support for the header field. Support for the UUI header field indicates that a UA is able to extract the information in the UUI data and pass it up the protocol stack. Individual packages using the UUI mechanism can utilize SIP media feature tags to indicate that a UA supports a particular UUI package. Guidelines for defining UUI packages are provided.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

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.

3. Requirements Discussion

This section describes how the User-to-User header field meets the requirements in [RFC6567]. 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 is included (escaped) within the Contact or Refer-To URI. The details of this mechanism as it applies for redirection and referral use cases are covered in Section 4.1.

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 is straightforward and is documented in a separate specification [RFC7434], meeting REQ-6.

Requirements REQ-7, REQ-8, and REQ-10 relate to discovery of the mechanism and supported packages, and hence 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. However, note that only UAs are expected to understand the UUI data -- proxies and other intermediaries do not. REQ-10 is met by utilizing SIP feature tags [RFC3840]. For example, the feature tag "sip.uui-isdn" could be used to indicate support of the ISDN UUI package, or "sip.uui-pk1" could be used to indicate support for a particular package, pk1.

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 avoiding having very large UUI data elements is a good idea, as SIP header fields have traditionally not been large.

To meet REQ-12 for the redirection and referral use cases, the History-Info header field [RFC7044] 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 "SIP Header Privacy and Integrity using S/MIME: Tunneling SIP", Section 23.4 of RFC 3261. Note that the lack of deployment of S/MIME with SIP means that, in general, REQ-13 is not met. 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 data will result in an additional body being added to the request. Hop-wise Transport Layer Security (TLS) [RFC5246] 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 data to meet the requirements in [RFC6567].

To help tag and identify the UUI data used with this header field, "purpose", "content", and "encoding" header field parameters are defined. The "purpose" header field parameter identifies the package that defines the generation and usage of the UUI data for a particular application. The value of the "purpose" parameter is the package name, as registered in the "UUI Packages" subregistry defined in Section 6.3. For the case of interworking with the ISDN UUI service, the ISDN UUI service interworking package is used. The default value for the "purpose" header field is "isdn-uui" as defined in [RFC7434]. If the "purpose" header field parameter is not present, the ISDN UUI MUST be used. The "content" header field parameter identifies the actual content of the UUI data. If not present, the default content defined for the package MUST be used. Newly defined UUI packages MUST define or reference at least a default "content" value. The "encoding" header field parameter indicates the method of encoding the information in the UUI data associated with a particular "content" value. This specification

only defines "encoding=hex". If the "encoding" header field parameter is not present, the default encoding defined for the package MUST be used.

UUI data is considered an opaque series of octets. This mechanism MUST NOT be used to convey a URL or URI, since the Call-Info header field in [RFC3261] already supports this use case.

4.1. Syntax for UUI Header Field

The UUI header field can be present in INVITE requests and responses and in BYE requests and responses. Note that when the UUI header is used in responses, it can only be utilized in end-to-end responses, e.g., 1xx (excluding 100), 2xx, and 3xx responses.

The following syntax specification uses the Augmented Backus-Naur Form (ABNF) as described in RFC 5234 and extends RFC 3261 (where token, quoted-string, and generic-param are defined).

```
UUI         = "User-to-User" HCOLON uui-value *(COMMA uui-value)
uui-value   = uui-data *(SEMI uui-param)
uui-data    = token / quoted-string
uui-param   = pkg-param / cont-param / enc-param / generic-param
pkg-param   = "purpose" EQUAL pkg-param-value
pkg-param-value = token
cont-param   = "content" EQUAL cont-param-value
cont-param-value = token
enc-param   = "encoding" EQUAL enc-param-value
enc-param-value = token / "hex"
```

Each package defines how many User-to-User header fields of each package may be present in a request or a response. A sender MAY include multiple User-to-User header fields, and a receiver MUST be prepared to receive multiple User-to-User header fields. Consistent with the rules of SIP syntax, the syntax defined in this document allows any combination of individual User-to-User header fields or User-to-User header fields with multiple comma separated UUI data elements. Any size limitations on the UUI data for a particular purpose are to be defined by the related UUI package.

UAs SHALL ignore UUI data from packages or encoding that they do not understand.

For redirection use cases, the header field is included (escaped) within the Contact URI. For referral use cases, the header field is included (escaped) within the Refer-To URI. For example, if a UA supports this specification, it SHOULD include any UUI data included in a redirection URI (if the UUI data and encoding is understood).

Note that redirection can occur multiple times to a request. Currently, UAs that support attended transfer support the ability to include a Replaces header field [RFC3891] into a Refer-To URI, and when acting upon this URI, UAs add the Replaces header field to the triggered INVITE. This sort of logic and behavior is utilized for the UUI header field (that is, the UUI header field is included in the triggered INVITE). The UA processing the REFER [RFC3515] or the 3xx response to the INVITE SHOULD support the UUI mechanism. If the REFER or redirect target does not support UUI, the UUI header will be discarded as per [RFC3261]. However, this may limit the utility of use cases that depend upon the UUI being supported by all elements.

Here is an example of an included User-to-User header field from the redirection response F2 of Figure 2 in [RFC6567]:

```
<allOneLine>
Contact: <sip:+12125551212@gateway.example.com?User-to-User=
56a390f3d2b7310023a2%3Bencoding%3Dhex%3Bpurpose%3Dfoo%3B
content%3Dbar>
</allOneLine>
```

The resulting INVITE F4 would contain:

```
User-to-User: 56a390f3d2b7310023a2;encoding=hex;purpose=foo;content=bar
```

4.2. Hex Encoding Definition

This specification defines hex encoding of UUI data. When the value of "hex" is used in the "encoding" parameter of a header field, the data is encoded using base16 encoding according to Section 8 of [RFC4648]. The hex-encoded value is normally represented using the "token" construction from RFC 3261, although the "quoted-string" construction is permitted, in which case the quotes MUST be ignored.

If a canonicalized version of a normally case-insensitive hex encoded UUI data object is needed for a digital signature or integrity checking, then the base16 encoding with all upper case MUST be used.

4.3. Source Identity of UUI Data

It is important for the recipient of UUI data to know the identity of the UA that inserted the UUI data. In a request without a History-Info header field, the identity of the entity that inserted the UUI data will be assumed to be the source of the SIP message. For a SIP request, typically this is the UA identified by the URI in the From header field or a P-Asserted-Identity [RFC3325] header field. In a request with a History-Info header field, the recipient needs to parse the Targeted-to-URIs present (hi-targeted-to-uri defined in

[RFC7044]) to see if any included User-to-User header fields are present. If an included User-to-User header field is present and matches the UUI data in the request, this indicates that redirection has taken place, resulting in the inclusion of UUI data in the request. The inserter of the UUI data will be the UA identified by the Targeted-to-URI of the History-Info element prior to the element with the included UUI data. In a response, the inserter of the UUI data will be the identity of the UA that generated the response. Typically, this is the UA identified in the To header field of the response. Note that any updates to this identity by use of the SIP connected identity extension [RFC4916] or other identity modifiers will update this information.

For an example of History-Info and redirection, consider Figure 2 from [RFC6567] where the Originating UA is Carol, the Redirector Bob, and the Terminating UA Alice. The INVITE F4 containing UUI data could be:

```
INVITE sips:alice@example.com SIP/2.0
Via: SIP/2.0/TLS lab.example.com:5061
 ;branch=z9hG4bKnashds9
To: Bob <sips:bob@example.com>
From: Carol <sips:carol@example.com>;tag=323sf33k2
Call-ID: dfaosidfoiwe83ifkdf
Max-Forwards: 70
Contact: <sips:carol@lab.example.com>
Supported: histinfo
User-to-User: 342342ef34;encoding=hex
History-Info: <sips:bob@example.com>;index=1
<allOneLine>
History-Info: <sips:alice@example.com?Reason=SIP%3Bcause%3D302
   &User-to-User=342342ef34%3Bencoding%3Dhex>;index=1.1;rc=1
</allOneLine>
```

Without the redirection captured in the History-Info header field, Alice would conclude that the UUI data was inserted by Carol. However, the History-Info containing UUI data (index=1.1) indicates that the inserter was Bob (index=1).

To enable maintaining a record of the inserter identity of UUI data, UAs supporting this mechanism SHOULD support History-Info [RFC7044] and include Supported: histinfo in all requests and responses.

If a border element such as a proxy or a Back-to-Back User Agent (B2BUA) removes a History-Info header field containing a User-to-User parameter, the UA consuming the UUI data may not be able at the SIP level to identify the source of the UUI data.

5. Guidelines for UUI Packages

UUI packages defined using this SIP UUI mechanism MUST follow the "Standards Action" guideline as defined in [RFC5226] and publish a Standards Track RFC that describes the usage. The CUSS WG chose to adopt this conservative policy while it considers other potential registration policies. Note that this mechanism is not suitable for the transport of arbitrary data between UAs. The following guidelines are provided to help determine if this mechanism is appropriate or not. The SIP UUI mechanism is applicable when all of the following conditions are met:

1. The information is generated and consumed by an application during session setup using SIP, but the application is not necessarily SIP aware.

2. The behavior of SIP entities that support it is not significantly changed (as discussed in Section 4 of [RFC5727]).

3. UAs are the generators and consumers of the UUI data. Proxies and other intermediaries may route based on the presence of a User-to-User header field or a particular package tag but do not otherwise consume or generate the UUI data.

4. There are no privacy issues associated with the information being transported (e.g., geolocation or emergency-related information are examples of inappropriate UUI data).

5. The UUI data is not being utilized for User-to-User Remote Procedure Calls (RPCs).

UUI packages define the semantics for a particular application usage of UUI data. The content defines the syntax of the UUI data, while the encoding defines the encoding of the UUI data for the content. Each content is defined as a stream of octets, which allows multiple encodings of that content. For example, packages may define:

1. The SIP methods and responses in which the UUI data may be present.

2. The maximum number of UUI data elements that may be inserted into a request or response. The default is one per encoding. Note that a UA may still receive a request with more than this maximum number due to redirection. The package needs to define how to handle this situation.

3. The default values for content and encoding if they are not present. If the same UUI data may be inserted multiple times with different encodings, the package needs to state this. A package may support and define multiple contents and their associated encodings and reuse contents defined by other packages.

4. Any size limitations on the UUI data. Size needs to be specified in terms of the octet stream output of the content, since the size of the resulting uui-data element will vary depending on the encoding scheme.

A package MUST define a "purpose" header field value to identify the package in the coding. A package MUST describe the new application that is utilizing the UUI data and provide some use case examples. The default "content" value MUST be defined or referenced in another document for the package. Additional allowed contents MAY also be defined or referenced. Any restrictions on the size of the UUI data MUST be described. In addition, a package MAY define a media feature tag per [RFC3840] to indicate support for this UUI package. For example, the media feature tag "sip.uui-pk1" could be defined to indicate support for a UUI package named pk1. The definition of a new SIP option tag solely to identify support for a UUI package is NOT RECOMMENDED unless there are additional SIP behaviors needed to implement this feature.

For an example UUI package definition, see [RFC7434].

5.1. Extensibility

New "content" values MUST describe the semantics of the UUI data and valid encodings, and give some example use cases. A previously defined UUI content value can be used in a new package. In this case, the semantics and usage of the content by the new package is defined within the new package. New UUI content types cannot be added to existing packages -- instead, a new package would need to be defined. New content values that are defined are added to the IANA registry with a Standards Track RFC, which needs to discuss the issues in this section. If no new encoding value is defined for a content, the encoding defaults to "hex" as defined in this document. In this case, the "hex" value will be explicitly stated via the encoding parameter as the encoding for the content.

New "encoding" values associated with a new content MUST reference a specific encoding scheme (such as "hex", which is defined in this specification) or define the new encoding scheme. A previously defined UUI encoding value can be used with a newly defined content. In this case, the usage of the encoding is defined by the content

definition. New UUI encodings cannot be added to existing contents -- instead, a new content would need to be defined. Newly defined encoding values are added to the IANA registry with a Standards Track RFC, which needs to discuss the issues in this section.

6. IANA Considerations

6.1. Registration of User-to-User Header Field

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

The following row has been added to the "Header Fields" section of the SIP parameter registry:

Header Name	Compact Form	Reference
User-to-User		[RFC7433]

6.2. Registration of User-to-User 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 have been 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	Yes	[RFC7433]
User-to-User	content	No	[RFC7433]
User-to-User	purpose	No	[RFC7433]

6.3. Registration of UUI Packages

This specification establishes the "UUI Packages" subregistry under <http://www.iana.org/assignments/sip-parameters>.

The descriptive text for this subregistry is:

UUI packages provide information about the usage of the UUI data in a User-to-User header field [RFC7433].

The registration policy for this registry is "Standards Action" as defined in [RFC5226].

Package	Description	Reference

6.4. Registration of UUI Content Parameters

This specification establishes the "UUI Content Parameters" subregistry under <http://www.iana.org/assignments/sip-parameters>.

The descriptive text for this subregistry is:

UUI content provides information about the content of the UUI data in a User-to-User header field [RFC7433].

The registration policy for this registry is "Standards Action" as defined in [RFC5226].

Content	Description	Reference

6.5. Registration of UUI Encoding Parameters

This specification establishes the "UUI Encoding Parameters" subregistry under <http://www.iana.org/assignments/sip-parameters> and initiates its population with the table below.

The descriptive text for this subregistry is:

UUI encoding provides information about the encoding of the UUI data in a User-to-User header field [RFC7433].

The registration policy for this registry is "Standards Action" as defined in [RFC5226].

Encoding	Description	Reference
hex	The UUI data is encoded using hexadecimal	[RFC7433]

6.6. 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.	[RFC7433]

7. Security Considerations

UUI data can potentially carry sensitive information that might require confidentiality protection for privacy or integrity protection from third parties that may wish to read or modify the UUI data. The three security models described in [RFC6567] may be applicable for the 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, applications are encouraged to use their own integrity and/or encryption mechanisms before passing it to the SIP layer.

The second 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. To preserve multi-hop or end-to-end confidentiality and integrity of UUI data, approaches using S/MIME or IPsec can be used, as discussed in the review of REQ-13 and REQ-14 in Section 3 of this document. However, the lack of deployment of these mechanisms means that applications cannot in general rely on them being present.

The third 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. Standard deployed SIP security mechanisms such as TLS transport offer privacy and integrity protection properties on a hop-by-hop basis at the SIP layer.

If the UUI data was included by the UA originator of the SIP request or response, normal SIP mechanisms can be used to determine the identity of the inserter of the UUI data. If the UUI data was included by a UA that was not the originator of the request, a History-Info header field can be used to determine the identity of the inserter of the UUI data. UAs can apply policy based on the origin of the UUI data using this information. In short, the UUI data included in an INVITE can be trusted as much as the INVITE itself can be trusted.

Note that it is possible that this mechanism could be used as a covert communication channel between UAs, conveying information unknown to the SIP network.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[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, <http://www.rfc-editor.org/info/rfc3261>.

[RFC3515] Sparks, R., "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, April 2003, <http://www.rfc-editor.org/info/rfc3515>.

[RFC3840] Rosenberg, J., Schulzrinne, H., and P. Kyzivat, "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)", RFC 3840, August 2004, <http://www.rfc-editor.org/info/rfc3840>.

[RFC3891] Mahy, R., Biggs, B., and R. Dean, "The Session Initiation Protocol (SIP) "Replaces" Header", RFC 3891, September 2004, <http://www.rfc-editor.org/info/rfc3891>.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006, <http://www.rfc-editor.org/info/rfc4474>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006, <http://www.rfc-editor.org/info/rfc4648>.

[RFC4916] Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)", RFC 4916, June 2007, <http://www.rfc-editor.org/info/rfc4916>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

[RFC7044] Barnes, M., Audet, F., Schubert, S., van Elburg, J., and C. Holmberg, "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 7044, February 2014, <http://www.rfc-editor.org/info/rfc7044>.

[RFC7434] Drage, K. and A. Johnston, "Interworking ISDN Call Control User Information with SIP", RFC 7434, January 2015, <http://www.rfc-editor.org/info/rfc7434>.

8.2. Informative References

[Q1980] ITU-T, "The Narrowband Signalling Syntax (NSS) - Syntax Definition", ITU-T Recommendation Q.1980.1, <http://www.itu.int/itudoc/itu-t/aap/sg11aap/history/q1980.1/q1980.1.html>.

[Q763] ITU-T, "Signalling System No. 7 - ISDN User Part formats and codes", ITU-T Recommendation Q.763, <http://www.itu.int/rec/T-REC-Q.763-199912-I/en>.

[Q931] ITU-T, "ISDN user-network interface layer 3 specification for basic call control", ITU-T Recommendation Q.931, <http://www.itu.int/rec/T-REC-Q.931-199805-I/en>.

[RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002, <http://www.rfc-editor.org/info/rfc3325>.

[RFC3372] Vemuri, A. and J. Peterson, "Session Initiation Protocol for Telephones (SIP-T): Context and Architectures", BCP 63, RFC 3372, September 2002, <http://www.rfc-editor.org/info/rfc3372>.

[RFC4475] Sparks, R., Hawrylyshen, A., Johnston, A., Rosenberg, J., and H. Schulzrinne, "Session Initiation Protocol (SIP) Torture Test Messages", RFC 4475, May 2006, <http://www.rfc-editor.org/info/rfc4475>.

[RFC5727] Peterson, J., Jennings, C., and R. Sparks, "Change Process for the Session Initiation Protocol (SIP) and the Real-time Applications and Infrastructure Area", BCP 67, RFC 5727, March 2010, <http://www.rfc-editor.org/info/rfc5727>.

[RFC6086] Holmberg, C., Burger, E., and H. Kaplan, "Session Initiation Protocol (SIP) INFO Method and Package Framework", RFC 6086, January 2011, <http://www.rfc-editor.org/info/rfc6086>.

[RFC6567] Johnston, A. and L. Liess, "Problem Statement and Requirements for Transporting User-to-User Call Control Information in SIP", RFC 6567, April 2012, <http://www.rfc-editor.org/info/rfc6567>.

Appendix A. Other Possible Mechanisms

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

A.1. Why INFO is Not Used

Since the INFO method [RFC6086] was developed for ISDN User Part (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 [RFC6567] show, the information is related to an attempt to establish a session and needs to 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.

A.2. Why Other Protocol Encapsulation UUI Mechanisms Are Not Used

Other protocols have the ability to transport UUI data. For example, consider the ITU-T Recommendation Q.931 User-user information element [Q931] and the ITU-T Recommendation Q.763 User-to-User information parameter [Q763]. In addition, the Narrowband Signalling System (NSS) [Q1980] is also able to transport UUI data. Should one of these protocols be in use, and present in both User Agents, then utilizing these other protocols to transport UUI data 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 data; it is encapsulating another protocol, and that protocol is transporting the UUI data. Once a mechanism to transport that other protocol using SIP exists, the UUI data transport function is essentially obtained without any additional effort or work.

However, the CUSS working group believes, consistent with its charter, that SIP needs to have its own native UUI data 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 data transport service. Of course, this work does not preclude anyone from using other protocols with SIP to transport UUI data.

A.3. MIME Body Approach

One method of transport is to use a MIME body. This is in keeping with the Session Initiation Protocol for Telephones (SIP-T) architecture [RFC3372] in which MIME bodies are used to transport ISUP information. Since the INVITE will normally have a Session

Description Protocol (SDP) message body, the resulting INVITE with SDP and UUI data 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 included as well? And, what if the included Content-Length does not agree with the included body?

Since proxies cannot remove a body from a request or response, it is not 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 "Securing MIME bodies", Section 23.3 of RFC 3261. Alternatively, this could be achieved using [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>
```

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.

A.4. URI Parameter

Another proposed approach is to encode the UUI data 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 response that does not have a Request-URI, or in BYE requests or responses.

```
<allOneLine>
Contact: <sip:+12125551212@gateway.example.com;uui=ZeGl9i2icVqaNVailT
6F5iJ90m6mvuTS4OK05M0vDk0Q4Xs>
</allOneLine>
```

An INVITE sent to this Contact URI would contain UUI data 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 [RFC6567]. 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.

Acknowledgments

Joanne McMillen was a major contributor and coauthor of earlier versions of this document. Thanks to Paul Kyzivat for his contribution of hex encoding rules. Thanks to Spencer Dawkins, Keith Drage, Vijay Gurbani, and Laura Liess for their review of the document. The authors wish to thank Roland Jesske, Celine Serrut-Valette, Francois Audet, Denis Alexeitsev, Paul Kyzivat, Cullen Jennings, and Mahalingam Mani for their comments. Thanks to Scott Kelly and Joel Halpern for their reviews.

Authors' Addresses

Alan Johnston
Avaya
St. Louis, MO 63124
United States

EMail: alan.b.johnston@gmail.com

James Rafferty
Human Communications
Norfolk, MA 02056
United States

EMail: jay@humancomm.com