Internet Engineering Task Force
Internet Draft
draft-ietf-sip-isup-mime-00.txt
January 2000
Expires: July 2000

Eric Zimmerer
ipVerse, Inc.
Aparna Vemuri
Level 3 Communications
L. Ong
M. Zonoun
M. Watson
Nortel Networks

MIME media types for ISUP and QSIG Objects

Status of this Memo

Abstract

This document describes MIME types for application/ISUP and application/QSIG objects for use in SIP applications, according to the rules defined in RFC 2048 [1]. These types can be used to identify ISUP and QSIG objects within a SIP message such as INVITE or INFO, as might be implemented when using SIP between legacy systems.

1. Introduction

ISUP (ISDN User part) defined in the ITU-T recommendations Q.761-4 is a signaling protocol used between telephony switches. There exists a need to transport ISUP-encoded signaling information between SIP entities as part of the payload of SIP [2] messages, in order to access ISUP-based legacy service logic. For example, this may be implemented when using SIP to control sessions between two systems that support legacy telephony services or gateway between legacy systems.

QSIG is the analogous signaling protocol used between private branch exchanges to support calls within private telephony networks. There is a similar need to transport QSIG-encoded signaling information between SIP entities to support legacy services or gateway between legacy systems.

The following discussion is specific to this usage and would not apply to the transportation of ISUP or QSIG messages in other applications. These media types are intended for ISUP or QSIG application information that is used within the context of a SIP session, and not as general purpose transport of SCN signaling.

The definition of media types for ISUP and QSIG application information does not address fully how the entities exchanging messages determine or negotiate compatibility. It is assumed that this is addressed by alternative means such as configuration or routing protocols.

It is assumed in this document that the processing of ISUP and QSIG information is in addition to the standard SIP processing, and that no interworking of SIP and ISUP or QSIG signaling is required.

This is intended to be an IETF approved MIME type, and to be defined through an RFC. NOTE: usage of Q.SIG within SIP is neither endorsed nor recommended as a result of this MIME registration.

3. Proposed new media types

ISUP and QSIG messages are composed of arbitrary binary data that is transparent to SIP processing. The best way to encode these is to use binary encoding. This is in conformance with the restrictions imposed on the use of binary data for MIME (RFC 2045 [3]). It should be noted that the rules mentioned in the RFC 2045 apply to Internet mail messages and not to SIP messages. Binary has been preferred over Base64 encoding because the latter would only result in adding bulk to the encoded messages and possibly be more costly in terms of processing power.

3.1 ISUP Media Type

This media type is defined by the following information:

Media type name: application

Media subtype name: ISUP
Required parameters: none
Optional parameters: version, compatibility, spec
Encoding scheme: binary
Security considerations: See section 5.

Note: It is mandatory for SoftSwitches to specify the 'version' of the ISUP message. Proxies, redirect servers, etc., have no need to process/specify this information.

The use of the 'version' parameter allows differentiation between different base ISUP variants. This enables the SoftSwitch (also known as a Media Gateway Controller) to

---

recognize and parse the message correctly, or (possibly) to reject the message if the particular ISUP variant is not supported. The idea here is to allow to specify a preference of version, so that the following scenarios are possible: "I only like application/isup;version=lcd" or "I accept application/isup (but don't really know the details; I just pass them on to some other tool that displays/munges them)". If not specified, the default version is assumed to be ITU-T ISUP.

'compatibility' indicates whether or not the version of ISUP supports the forward compatibility mechanism that is defined in ITU-T White Book specifications and later issues of ISUP. If present, its value is either yes or no.

The 'spec' parameter provides more detailed identification of the ISUP specification being sent, if this is available. This may be used, for example, to identify a particular national specification.

The following is how a typical header would look:

```
Content-Type: application/ISUP; version=etsi;
    compatibility=yes; spec=uk21
Content-Transfer-Encoding: binary
```

Table 1 is a partial list of protocol versions supported by the 'application/ISUP' media type.

version	compatibility	protocol

itu-t	no	ITU-T Q.761-4 (1988)
itu-t	yes	ITU-T Q.761-4 (1992)
ansi	no	ANSI T1.113-1988
etsi	no	ETSI 300 121
etsi	yes	ETSI 300 356
gr317	no	BELLCORE GR-317

3.2 QSIG Media Type

The application/QSIG media type is defined by the following information:

Media type name: application
Media subtype name: QSIG
Required parameters: none
Optional parameters: version
Encoding scheme: binary
Security considerations: See section 5.

The use of the 'version' parameter allows identification of different QSIG variants. This enables the terminating Connection Server to

---

recognize and parse the message correctly, or (possibly) to reject the message if the particular QSIG variant is not supported.

The following is how a typical header would look:-

```
Content-Type: application/QSIG; version=iso
Content-Transfer-Encoding: binary
```

Table 2 is a list of protocol versions supported by the 'application/QSIG' media type.

version	protocol
etsi93	ETSI 1993 version
iso	ISO/IEC 11572 (equiv. to ETSI 1995)

4. Illustrative examples

4.1 ISUP

SIP message format requires a Request line followed by Header lines followed by a CRLF separator followed by the message body. To illustrate the use of the 'application/ISUP' media type, below is an INVITE message which has the originating SDP information and

an encapsulated ISUP IAM.

Note that the two payloads are demarcated by the boundary parameter (specified in RFC 2046 [4]) which in the example has the value "unique-boundary-1". This is part of the specification of MIME multipart and is not related to the 'application/ISUP' media type.

```
INVITE sip:13039263142@Den1.level3.com SIP/2.0
From: sip:13034513355@den3.level3.com
To: sip:13039263142@Den1.level3.com
Call-ID: DEN123199902171209550099@Den1.level3.com
Content-Length: 448
Content-Type: multipart/mixed; boundary=unique-boundary-1
MIME-Version: 1.0


--unique-boundary-1
Content-Type: application/SDP; charset=ISO-10646

v=0
o=ezimmerer 2890844526 2890842807 IN IP4 126.16.64.4
s=SDP seminar
c=IN IP4 MG122.level3.com
t= 2873397496   2873404696
m=audio 9092 RTP/AVP 0 3 4
```



```
--unique-boundary-1
Content-type:application/ISUP; version=etsi;
compatibility=yes; spec=uk21
Content-Transfer-Encoding: binary

e1 f9 28 85 43 1e 05 44 1e 05 00 6e 0a 01 00
00 00 00 03 06 0d 03 80 90 a2 07 03 10 03 63
53 00 10 0a 07 03 10 27 80 88 03 00 00 89 8b
0e 95 1e 1e 1e 06 26 05 0d f5 01 06 10 04 00
--unique-boundary-1--
```

Note:
Since binary encoding is used for the ISUP payload, each byte is encoded as a byte, and not as a two-character hex representation. Hex digits were used in the draft because a literal encoding of those bytes would have been confusing and unreadable.

4.2 QSIG

To illustrate the use of the 'application/QSIG' media type, below is an INVITE message which has the originating SDP information and an encapsulated QSIG SETUP message.

Note that the two payloads are demarcated by the boundary parameter (specified in RFC 2046 [4]) which in the example has the value "unique-boundary-1". This is part of the specification of MIME multipart and is not related to the 'application/QSIG' media type.

```
INVITE sip:14084955072@sc1.nortelnetworks.com SIP/2.0
From: sip:14085655675@sc10.nortelnetworks.com
To: sip:14084955072@sc1.nortelnetworks.com
Call-ID: 12319990217120955009990sc12.nortelnetworks.com
Content-Length: 393
Content-Type: multipart/mixed; boundary=unique-boundary-1
MIME-Version: 1.0

--unique-boundary-1
Content-Type: application/SDP; charset=ISO-10646

v=0
o=audet 2890844526 2890842807 5 IN IP4 134.177.64.4
s=SDP seminar
c=IN IP4 MG141.nortelnetworks.com
t= 2873397496 2873404696
m=audio 9092 RTP/AVP 0 3 4

--unique-boundary-1
Content-type:application/QSIG; version=iso
Content-Transfer-Encoding: binary

08 02 55 55 05 04 02 90 90 18 03 a1 83 01
70 0a 89 31 34 30 38 34 39 35 35 30 37 32


--unique-boundary-1--
```


---

5. Security considerations

ISUP and QSIG objects may have security considerations due to customer-related information contained in the objects. However, the security mechanisms described in RFC 2543 (SIP - Session Initiation Protocol) are sufficient to support security of the

encapsulated ISUP or QSIG information. No new security considerations are thought necessary.

6. Authors

Eric Zimmerer
ipVerse, Inc.
1901 Landings Drive
Mountain View, CA 94043, USA
Phone: 650-919-0648
Email: ericz@ipverse.com

L. Ong
M. Zonoun
Nortel Networks
Santa Clara, CA 95054
long@nortelnetworks.com
mzonoun@nortelnetworks.com

Aparna Vemuri
Level 3 Communications
Louisville, CO, USA
Phone: 303-926-3768
EMail: aparna.vemuri@level3.com

M. Watson
Nortel Networks
Maidenhead, UK
mwatson@nortelnetworks.com

7. References

[1] Freed, Klensin, Postel, "Multipart Internet Mail Extensions (MIME) Part Four: Registration Procedures" RFC 2048, Internet Engineering Task Force, November 1996.

[2] Handley, Schulzrinne, Schooler and Rosenberg, "Session Initiation Protocol (SIP)" RFC 2543, Internet Engineering Task Force, March 1999.

[3] Freed, Borenstein, "Multipart Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies" RFC 2045, Internet Engineering Task Force, November 1996.

[4] Freed, Borenstein, "Multipart Internet Mail Extensions (MIME) Part Two: Media Types" RFC 2046, Internet Engineering Task Force, November 1996.