

Internet Engineering Task Force  
Internet Draft  
[draft-ietf-sip-isup-mime-01.txt](http://www.ietf.org/drafts/ietf-sip-isup-mime-01.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

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#). Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

### 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: version

Optional parameters: base

Encoding scheme: binary

Security considerations: See [section 5](#).

Note: It is mandatory for clients 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 a client such as a SoftSwitch/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 1992.

The 'base' parameter provides identification of a base regional variant of ISUP that can be used to process the ISUP body. This may be used, for example, to identify that the message can be processed using ITU-T 1992 ISUP processing, including support of the forward compatibility mechanism.

The following is how a typical header would look:

```
Content-Type: application/ISUP; version=uk21;
             base=etsi121
Content-Transfer-Encoding: binary
```

Table 1 is a partial list of protocol base versions supported by the 'application/ISUP' media type, and whether they support the forward compatibility mechanism defined in later versions of ISUP.

base	protocol	compatibility
itu-t88	ITU-T Q.761-4 (1988)	no
itu-t92+	ITU-T Q.761-4 (1992)	yes
ansi88	ANSI T1.113-1988	no
etsi121	ETS 300 121	no
etsi356	ES 300 356	yes
gr317	BELLCORE GR-317	no

### [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. The ISUP message is encapsulated beginning with the ISUP Message Type Code (i.e., omitting Routing Label and Circuit Identification Code).

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: DEN1231999021712095500999@Den1.level3.com
Content-Length: 420
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=uk21;
base=etsi121
Content-Transfer-Encoding: binary
```

```
01 00 49 00 00 03 02 00 07 04 10 00 33 63 21
43 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: 1231999021712095500999@sc12.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--

Zimmerer, Vemuri [draft-ietf-sip-isup-mime-01.txt](#)

[Page 5]

## 5. Security considerations

Information contained in ISUP and QSIG bodies may include sensitive customer information, potentially requiring use of encryption. Security mechanisms are provided in [RFC 2543](#) (SIP - Session Initiation Protocol) and should be used as appropriate for both the SIP message and the encapsulated ISUP or QSIG body.

## 6. Authors

Eric Zimmerer	L. Ong
ipVerse, Inc.	M. Zonoun
<a href="#">1901</a> Landings Drive	Nortel Networks
Mountain View, CA 94043, USA	Santa Clara, CA 95054
Phone: 650-919-0648	long@nortelnetworks.com
Email: ericz@ipverse.com	mzonoun@nortelnetworks.com

Aparna Vemuri	M. Watson
Level 3 Communications	Nortel Networks
Louisville, CO, USA	Maidenhead, UK
Phone: 303-926-3768	mwatson@nortelnetworks.com
EMail: aparna.vemuri@level3.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.

This Internet Draft expires July 2000