The SIP ISUP/MIME type

1. Abstract

This document proposes the definition of an application/ISUP media type, according to the rules defined in RFC 2048 [1].

2. 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 messages between SoftSwitches as being part of the payload of SIP [2] messages. The following discussion is specific to this usage and would not apply to the transportation of ISUP messages in other applications.

3. The application/ISUP media type

The ISUP messages are composed of arbitrary binary data. The best way to encode these would be to use binary encoding. This is in conformance with the restrictions imposed on the use of binary data.
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 as well as prove costly in terms of processing power. This media type is defined by the following information:

Media type name: application
Media subtype name: ISUP
Required parameters: none
Optional parameters: version
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 ISUP variants. This enables the terminating SoftSwitch (also known as media gateway) 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)".

The following is how a typical header would look:-

```
Content-Type: application/ISUP; Version=ETSI1
Content-Transfer-Encoding: binary
```

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANSI</td>
<td>ANSI ISUP</td>
</tr>
<tr>
<td>ETSI1</td>
<td>ETSI ISUP v1</td>
</tr>
<tr>
<td>ETSI2</td>
<td>ETSI ISUP v2</td>
</tr>
<tr>
<td>GR317</td>
<td>Bellcore ISUP GR-317</td>
</tr>
</tbody>
</table>

Zimmerer, Vemuri  draft-zimmerer-sip-isup-mime-00.txt  [Page 2]
4. Illustrative example

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: DEN1231999021712095500999@Den1.level3.com
Content-Length: 377
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=ETSI1
Content-Transfer-Encoding: binary

89 8b 0e 95 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.

5. Security considerations

The security mechanisms described in RFC 2543 (SIP - Session Initiation Protocol) should suffice. 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

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

7. References


