



**Implementation Agreement for a  
SIP-T Profile for a CA/MGC**

**MSF-IA-SIP-T.001.02-FINAL**

# Multiservice Switching Forum Implementation Agreement

**Contribution Number:** MSF2004.030

**Document Filename:** MSF-IA-SIP-T.001.02-FINAL

**Working Group:** Protocol & Control

**Title:** Implementation Agreement for a SIP-T Profile for a CA/MGC

**Editors:** Wayne Cutler (wayne.cutler@marconi.com)

**Working Group Chairperson:** Chris Gallon (c.gallon@ftel.co.uk)

**Date:** 28<sup>th</sup> September 2004

**Abstract:** This document describes a SIP-T profile for a CA/MGC.

**Keywords:** SIP, SIP-T, GMI2004

The goal of the MSF is to promote multi-vendor interoperability as part of a drive to accelerate the deployment of next generation networks. To this end the MSF looks to adopt pragmatic solutions in order to maximize the chances for early deployment in real world networks.

To date the MSF has defined a number of detailed Implementation Agreements and detailed Test Plans for the signaling protocols between network components and is developing additional Implementation Agreements and Test Plans addressing some of the other technical issues such as QoS and Security to assist vendors and operators in deploying interoperable solutions.

In 2002, the MSF held a "Global MSF Interoperability 2002" (GMI 2002) event that tested interoperability between next generation network elements situated in Asia, Europe and North America. GMI 2002 validated the MSF release 1 architectural framework and Implementation Agreements by subjecting them to interoperability testing based on realistic network scenarios.

Following the success of GMI 2002 the MSF work program continues to address the key technical barriers to next generation network deployments. Global MSF Interoperability 2004 (GMI 2004) will demonstrate a deployable and operationally ready IP telephony network with Network Management, enhanced Quality-of-Service (QoS) and security features. GMI2004 will also demonstrate a service layer with application server, media server, and service broker functionality. This will enable the MSF to demonstrate a full end-to-end customer ready deployable network.

It is envisaged that GMI2004 will provide an industry showcase that will:

- Assist carriers achieve their goal: to deploy flexible, best of breed products.
- Assist vendors achieve their goal: to market products more cost effectively.
- Display the global interoperability of the MSF architecture as referenced in the Release 2 architecture document.
- Demonstrate a network scenario that can be managed to specific quality standards.

The MSF welcomes feedback and comment and would encourage interested parties to get involved in this work program. Information about the MSF and membership options can be found on the MSF website <http://www.msforum.org/>

## DISCLAIMER

The information in this publication is believed to be accurate as of its publication date. Such information is subject to change without notice and the Multiservice Switching Forum is not responsible for any errors or omissions. The Multiservice Switching Forum does not assume any responsibility to update or correct any

information in this publication. Notwithstanding anything to the contrary, neither the Multiservice Switching Forum nor the publisher make any representation or warranty, expressed or implied, concerning the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind whether based on theories of tort, contract, strict liability or otherwise, shall be assumed or incurred by the Multiservice Switching Forum, its member companies, or the publisher as a result of reliance or use by any party upon any information contained in this publication. All liability for any implied or express warranty of merchantability or fitness for a particular purpose is hereby disclaimed. The receipt or any use of this document or its contents does not in any way create by implication or otherwise:

Any express or implied license or right to or under any Multiservice Switching Forum member company's patent, copyright, trademark or trade secret rights which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor

Any warranty or representation that any Multiservice Switching Forum member companies will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor

Any commitment by a Multiservice Switching Forum company to purchase or otherwise procure any product(s) and/or service(s) that embody any or all of the ideas, technologies, or concepts contained herein; nor

Any form of relationship between any Multiservice Switching Forum member companies and the recipient or user of this document.

Implementation or use of specific Multiservice Switching Forum Implementation Agreements, Architectural Frameworks or recommendations and Multiservice Switching Forum specifications will be voluntary, and no company shall agree or be obliged to implement them by virtue of participation in the Multiservice Switching Forum.

For addition information contact:

Multiservice Switching Forum  
39355 California Street, Suite 307, Fremont, CA 94538  
(510) 608-5922  
(510) 608-5917 (fax)  
[info@msforum.org](mailto:info@msforum.org)  
<http://www.msforum.org>

<b>1</b>	<b>MULTISERVICE SWITCHING FORUM</b>	<b>6</b>
<b>2</b>	<b>APPLICABILITY AND SCOPE</b>	<b>7</b>
<b>3</b>	<b>SIP-T PROFILE</b>	<b>8</b>
3.1	Identifications	8
3.2	Base specifications	8
3.3	Optional specifications	8
3.4	Configuration	8
3.5	Transport	8
3.6	RTP stream and SDP description	8
3.7	Encapsulated Protocol	9
3.8	URL	10
3.9	SIP Protocol	10
3.9.1	SIP Request Headers	10
3.9.2	SIP Response Headers	11
3.10	SDP	12
3.10.1	SDP Usage	12
3.10.2	Basic Call Bearer Connection	12
3.10.3	Mid Call Bearer Change	13
3.11	Start of Day Processing	13
3.12	Reliable Provisional Responses	14
3.13	SIP Session Timer	14
<b>4</b>	<b>VOICE CODECS</b>	<b>15</b>
<b>5</b>	<b>ECHO CONTROL</b>	<b>16</b>
<b>6</b>	<b>MODEM, FAX AND TTY SUPPORT</b>	<b>17</b>
<b>7</b>	<b>DTMF DIGITS AND TELEPHONY TONES</b>	<b>18</b>
<b>8</b>	<b>NAT &amp; FIREWALL TRAVERSAL</b>	<b>19</b>

<b>9</b>	<b>QOS ASPECTS</b>	<b>20</b>
<b>10</b>	<b>SECURITY ASPECTS</b>	<b>21</b>
<b>11</b>	<b>REDUNDANCY &amp; RESILIENCE</b>	<b>22</b>
<b>12</b>	<b>MANAGEMENT INFORMATION MODEL</b>	<b>23</b>
<b>12.1</b>	<b>SIP-T Route/Interface</b>	<b>23</b>
<b>13</b>	<b>REFERENCES</b>	<b>23</b>
<b>14</b>	<b>ACKNOWLEDGEMENTS</b>	<b>25</b>

# 1 Multiservice Switching Forum

The goal of the MSF is to promote multi-vendor interoperability as part of a drive to accelerate the deployment of next generation networks. To this end the MSF looks to adopt pragmatic solutions in order to maximize the chances for early interoperability in real world networks.

To date the MSF has defined a number of detailed Implementation Agreements and detailed Test Plans for the signaling protocols between network components and is developing additional Implementation Agreements and Test Plans addressing some of the other technical issues such as QoS and Security to assist vendors and operators in deploying interoperable solutions.

In 2002, the MSF held a “Global MSF Interoperability 2002” (GMI 2002) event that tested interoperability between next generation network elements situated in Asia, Europe and North America. GMI 2002 validated the MSF release 1 architectural framework and Implementation Agreements by subjecting them to interoperability testing based on realistic network scenarios.

Following the success of GMI 2002 the MSF work program continues to address the key technical barriers to next generation network deployments. Global MSF Interoperability 2004 (GMI 2004) will demonstrate a deployable and operationally ready IP telephony network with Network Management, enhanced Quality-of-Service (QoS) and security features. GMI2004 will also demonstrate a service layer with application server, media server, and service broker functionality. This will enable the MSF to demonstrate a full end-to-end customer ready deployable network.

It is envisaged that GMI2004 will provide an industry showcase that will:

- Assist carriers achieve their goal: to deploy flexible, best of breed products.
- Assist vendors achieve their goal: to market products more cost effectively.
- Display the global interoperability of the MSF architecture as referenced in the Release 2 architecture document.
- Demonstrate a network scenario that can be managed to specific quality standards.

The MSF welcomes feedback and comment and would encourage interested parties to get involved in this work program. Information about the MSF and membership options can be found on the MSF website <http://www.msforum.org/>

## 2 Applicability and Scope

This Implementation Agreement covers the interface between two Media Gateway Controllers / Call Agents using SIP-T as a signaling protocol in preparation for GMI 2004. This profile is an updated version of the SIP-T Profile for GMI2002 Event (see [1]).

Figure 1 shows the MSF architecture diagram for GMI 2004 and highlights the applicable interfaces for this IA.

The overall end to end Network Architecture for GMI 2004 is shown in figure 1 below.

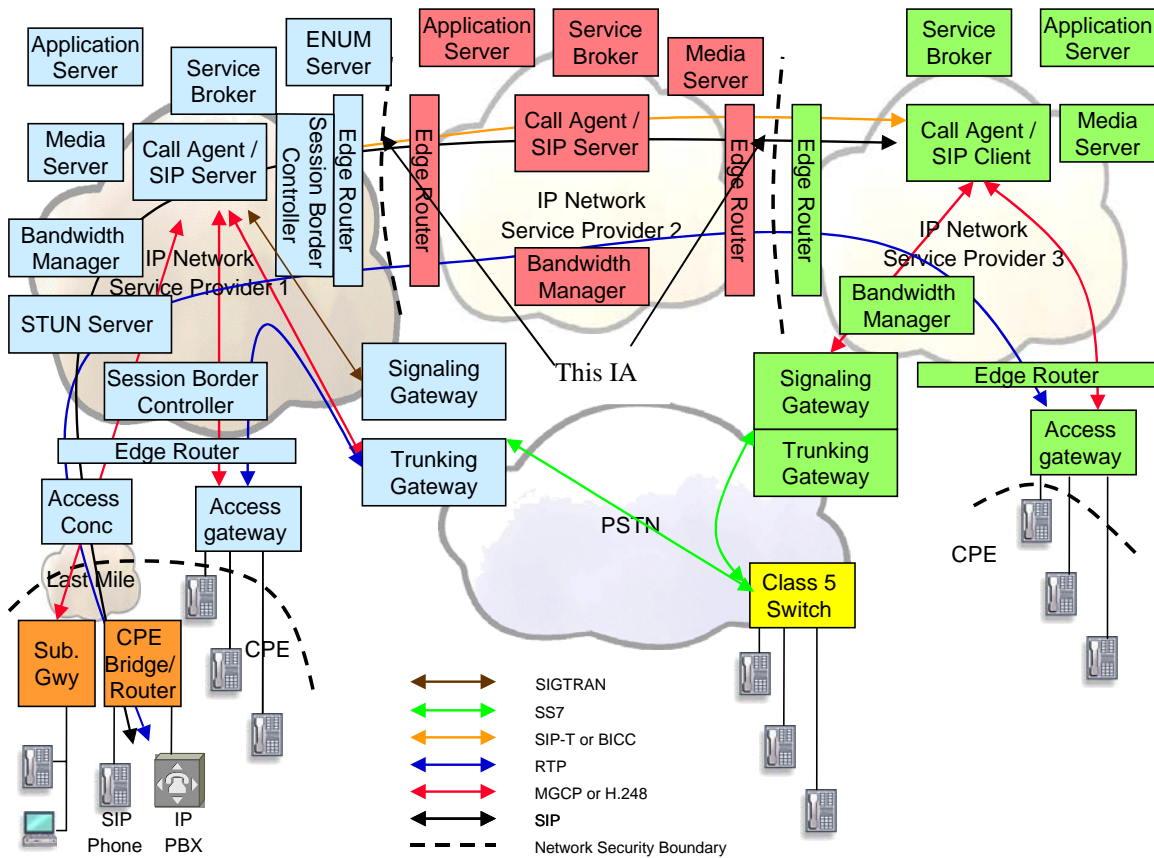


Figure 1: Architecture diagram indicating applicable interfaces for this IA in Service Provider 2

This interface is used to enable peer-peer signalling between MGCs/Call Agents. SIP-T (SIP for Telephones) is a mechanism that uses SIP to facilitate the interconnection of the PSTN with packet networks. SIP-T is characterized by the encapsulation of legacy signalling in the SIP body for feature transparency, translation of ISUP information into the SIP header for routability, and use of the INFO method for mid-call signalling. This profile is concerned solely with the encapsulation of ISUP signalling and corresponds to the ITU-T standard ([11] for SIP-I Profile C. This profile ought to be read in conjunction with the MSF Core SIP Profile ([14]).

## 3 SIP-T Profile

### 3.1 Identifications

This profile shall be entitled “MSF SIP-T Controller Profile”. The version number shall be 1.

### 3.2 Base specifications

A conforming MGC shall implement the following specifications:

- IETF RFC 3261, "TEL: Session Initiation Protocol"
- IETF RFC 2976, "The SIP INFO Method"
- IETF RFC 3204, "MIME media types for ISUP and QSIG Objects"
- IETF RFC 3372, "SIP for Telephones (SIP-T): Context and Architectures"
- IETF RFC 3262, "Reliability of Provisional Responses in SIP"
- IETF RFC 3311, “The SIP Update Method”
- IETF RFC 3264, “An Offer / Answer Model with SDP”
- ITU-T Q.1912.5, “Inter-working between SIP and BICC/ISUP”

### 3.3 Optional specifications

A conforming MGC shall optionally implement the following specifications:

- IETF draft draft-ietf-sip-session-timers-13.txt, “Session Timers in SIP”
- IETF RFC 3326, “The Reason Header field for SIP”
- IETF RFC 3325, “Private Extensions to SIP for Asserted Identity within trusted networks”
- IETF RFC 3312, “Integration of Resource Management & SIP”.

Note that RFCs 3326 and 3325 are regarded as mandatory in [11] for SIP-I Profile C.

### 3.4 Configuration

Routing information to peer MGCs shall be provisioned in the MGC.

An MGC shall know that it should use SIP-T across an interface to a peer node via provisioning for this version of the profile.

### 3.5 Transport

RFC 3261 [13] allow SIP requests to be sent using reliable or unreliable protocols: UDP, TCP, or SCTP.

Where the SIP-T interface crosses a trust boundary, the MSF architecture mandates the use of TLS as described in the SIP Signaling Security IA. This requires support for TCP and optionally SCTP as a transport protocol.

Thus, a conforming MGC shall support UDP for signalling to a trusted peer and TCP for signalling to an untrusted peer. SCTP MAY also be supported in the latter case.

When UDP is used, only unicast support is required.

### 3.6 RTP stream and SDP description

A conforming MGC shall support unicast for RTP streams. Multicast may be supported.

SDP shall be exchanged according to the rules of RFC 3264 [7].

### 3.7 Encapsulated Protocol

This profile applies to the encapsulation of ISUP only. The ISUP message is encapsulated beginning with the Message Type Code (i.e., omitting Routing Label and Circuit Identification Code).

In the context of GMI2004, the relevant ISUP versions are UK-ISUP, Japanese ISUP, ANSI ISUP and ITU-T ISUP. A MGC shall support the encapsulation of ITU-T ISUP and may support one or more of the other ISUP versions. The encapsulated ISUP must be explicitly tagged (as described in [3]) to enable a recipient MGC to be able to recognize and parse the encapsulated ISUP. To this end, it is proposed that a conformant MGC support the minimum set of headers, namely :-

```
Media type name: "application"  
Media subtype name: "ISUP"  
ISUP Version : set to "uk", "us", "jp" or "itu"
```

In addition, the Content-Disposition header shall be supported in order to explicitly tag whether the handling of the ISUP is optional or required.

An example encapsulated ISUP message would look something like :-

```
--unique-boundary-1  
Content-Type: application/ISUP; version=uk;  
Content-Disposition: signal; handling=mandatory  
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--
```

The sending MGC may send either national or ITU variants of ISUP. It is recommended that ITU ISUP be tagged as optional and national versions are tagged as mandatory. The recipient MGC will respond in the following ways :-

- If the encapsulated ISUP is marked as "optional" then it will be processed (if understood) and ignored if not.
- If the encapsulated ISUP is marked as required and the egress MGC does not understand either the variant of ISUP or it does not understand ISUP at all then it shall respond with 415, "Unsupported Media Type".

On receipt of a 415 response, a MGC may then either reject the call or re-send the invite. If the MGC chooses to re-send the invite and in the case where it first encapsulated national version of ISUP, then it may choose to encapsulate international ISUP. In this case, the handling is marked as "optional". This approach aids inter-operability since (in the general case) a recipient MGC may not understand ITU ISUP but would still permit the call to proceed.

In terms of the GMI2004 event, it is expected that all MGCs will be provisioned with data to enable them to encapsulate the correct version of ISUP on a given interface.

Within the packet network SIP servers do not understand encapsulated ISUP, and do not modify or look at the encapsulated message.

A conforming recipient MGC shall ensure that the SIP headers take precedence over the ISUP. This is based on the possibility that the contents of SIP headers may be updated by an intermediate SIP server within the IP network.

For this profile, en-bloc working shall be applicable (i.e. end of dialling determination applied by the originating CA).

### 3.8 URL

A conforming entity shall support tel-URLs and SIP-URLs. SIPS URLs shall also be supported if TLS is to be used (see section 3.5).

Passwords in the userinfo field are not recommended and are to be ignored if present.

### 3.9 SIP Protocol

#### (1) Supported methods

A conforming MGC shall support all the methods defined in the base specifications (section 3.2), and may support ones in the optional specifications (section 3.3).

*Currently, INVITE, ACK, BYE, CANCEL, PRACK, INFO and UPDATE are mandatory for a conforming MGC.*

#### (2) Message body in 1xx and 300 and greater responses

*A conforming MGC should support text/plain type and may support text/html.*

#### (3) Compact Form

A conforming MGC shall use only non-compact forms.

#### 3.9.1 SIP Request Headers

All SIP requests shall support the following headers :- REQ-URI, TO, FROM, CALL-ID, CSEQ & CONTENT-LENGTH.

In addition, the following table describes the salient headers which are supported in the various requests:-

Header	INVITE	ACK	PRACK	CANCEL	BYE	INFO	UPDATE
Content Type	C	O	O	O	O	M	M
Contact	M	O	O	N/A	N/A	O	N/A
Supported	M	N/A	O	O	O	O	N/A
Rack	N/A	N/A	M	N/A	N/A	N/A	N/A
Require	M	N/A	N/A	N/A	N/A	N/A	N/A
Content Disposition	C	N/A	N/A	N/A	N/A	N/A	M
Record Route	M	N/A	N/A	N/A	N/A	N/A	N/A
Route	O	O	N/A	O	O	O	O
Session Expires	O	N/A	N/A	N/A	N/A	N/A	O
Min-SE	O	N/A	N/A	N/A	N/A	N/A	N/A
Allow	M (note)	N/A	N/A	N/A	N/A	N/A	N/A

Resource Priority	O	O	O	O	O	O	O
Accept Resource Priority	O	O	O	O	O	O	O

Note – Used to advertise support of UPDATE.

Key :- M – Mandatory, O – Optional, C – Conditional (i.e. if message body not empty, then M), N/A – Not applicable.

Embedded ISUP messages may be present in the following Methods :-

Method Name	Corresponding ISUP Message	Comments
INVITE	IAM	Always present.
ACK	None	Never present
BYE	REL	Always present
CANCEL	REL	Always present
PRACK	None	PRACK used to acknowledge early bearer info (e.g. in 18X).
INFO	RES, SUS	
UPDATE	None	UPDATE used for mid call bearer change or session timer update.
None	SAM	N/A since en-bloc working assumed.

### 3.9.2 SIP Response Headers

All SIP 1XX responses support the following headers :- TO, FROM, VIA, CALL-ID, CSEQ & CONTENT-LENGTH. The following table details which additional headers are carried in specific 1XX responses :-

Header	100	18X
Content Type	N/A	O
Contact	O	M
Supported	O	O
RSeq	N/A	C
Require	O	O
Content Disposition	N/A	C
Session Expires	O	O
Record-Route	N/A	O
Allow	O	O

Note :- M – Mandatory, O – Optional, C – Conditional (i.e. if SDP present, then M), N/A – Not applicable.

All 2XX responses other than 200 response are treated as for a 200 response for the corresponding transaction.

A 200 OK response will be sent to INVITE,PRACK,INFO,BYE, CANCEL& UPDATE if the request is properly processed. It may contain a body to exchange the callee’s capabilities. The 200 OK response to a BYE or CANCEL may carry an embedded ISUP RLC message. Note that since CANCEL is hop-by-hop, there is no guarantee that the contents of a 200 OK CANCEL will reach a remote CA.

The 200 OK response always contains the following :- TO, FROM, VIA, CALL-ID, CSEQ, CONTACT & CONTENT-LENGTH. In addition, the following headers may be present :- CONTENT-TYPE (if SDP / encapsulated ISUP present), REQUIRE, SUPPORTED, SESSION-EXPIRES, RECORD-ROUTE, CONTENT-DISPOSITION (if encapsulated ISUP present) & ALLOW (to enable advertising of UPDATE support).

Any SIP failure reason (3XX, 4XX, 5XX, 6XX) should be allowed in the profile.

3XX responses will contain the following headers :- TO, FROM, VIA, CALL\_ID, CSEQ, CONTENT-LENGTH & CONTACT. It is assumed that a 3XX response will cause the call to be released (i.e. redirection shall be done via ISUP call forwarding).

4XX/5XX/6XX responses will contain the following headers :- TO, FROM, VIA, CALL\_ID, CSEQ, & CONTENT-LENGTH.

In general, the headers identified in this section are intended to be a minimum set to support the encapsulation of ISUP signalling with appropriate session control.

Embedded ISUP messages may be present in the following responses :-

Response Type	Corresponding ISUP Message	Comments
100 Trying	None	Never present
180 Ringing	ACM, CPG	Always present
18X (i.e. other than 180)	ACM, CPG	Always present
200	ANM, CON	Always present for 200 response to INVITE

### 3.10 SDP

SDP shall be supported as defined in RFC 2327 [6] and RFC 3264 [7].

This profile shall support mid-call bearer change. It is recommended that this is performed via the UPDATE method.

#### 3.10.1 SDP Usage

SDP usage shall conform to [4].

#### 3.10.2 Basic Call Bearer Connection

For the initial / basic call bearer connection, a single block of SDP shall be exchanged as described in [7]. The typical sequence shall be:-

- An INVITE containing an originating side SDP Offer,
- A 18X message (typically 180 Alerting) containing the terminating side SDP Answer,

- A 200 OK message containing the (repeated) terminating side SDP Answer.

Note that [7] mandates that the same SDP Time (t=) Line must appear in both blocks. In addition, there must be identical numbers of Media (m=) Lines in each SDP block.

### 3.10.3 Mid Call Bearer Change

Mid call bearer change is realized according to [7]. It is recommended that UPDATE be used ([12]) to convey the SDP change although re-INVITE shall also be supported.

[7] mandates that the same number of Media (m=) lines must be present. This raises an issue where a media stream is to be disconnected and thus must be disabled. There are a number of ways in which to disable a stream :-

- By setting the IP address to 0.0.0.0 (this is currently widely supported but is deprecated in [7]),
- By setting the cstream media attribute to inactive,
- By setting the port number to zero.

For this profile, to facilitate inter-operability, it is recommended that all three mechanisms are used to disable a media stream, e.g. compare the following SDP blocks :-

#### Active

```
v=0
s=-
t=0 0
o=- 0 0 IN IP4 128.96.63.25
c=IN IP4 128.96.63.25
m=audio 3456 RTP/AVP 0, 100
a=recvonly
a=rtpmap:100 G729D
a=ptime:20
```

#### Inactive

```
v=0
s=-
t=0 0
o=- 0 0 IN IP4 128.96.63.25
c=IN IP4 0.0.0.0
m=audio 0 RTP/AVP 0, 100
a=inactive
a=rtpmap:100 G729D
a=ptime:20
```

A new stream (i.e. bearer redirection) may be enabled via exchanging a new address and port in the Connection and Media Lines respectively – i.e. the contents of existing Media & Connection Lines can be altered as desired (e.g. to change address / port / media format / codec list).

## 3.11 Start of Day Processing

A Call Agent, on restart shall listen on its pre-configured port for receipt of signalling from a peer Call Agent.

A Call Agent shall run application level timers to terminate calls in the event of message loss / lack of response from a peer Call Agent.

### 3.12 Reliable Provisional Responses

Due to the fact that encapsulated ISUP messages are carried in provisional responses, support of RFC 3262 ([9]) is mandatory for this profile.

A confirming Call Agent shall advertise its requirement of provisional reliable responses via a REQUIRE header containing the tag "100Rel".

When sending a response in the range 101-199 (i.e. 100 is never sent reliably), a conformant Call Agent shall include a REQUIRE header with tag "100rel".

On receipt of a response in the range 101-199, a conformant Call Agent shall check to see that a REQUIRE header is present with tag "100Rel". If so, then a PRACK is generated.

See the appendix for a message flow example that uses 100rel.

### 3.13 SIP Session Timer

Support of session timer ([10]) is optional in this profile.

A confirming Call Agent MAY advertise support of session timer via a SUPPORTED header containing the tag "timer". In this case, the Call Agent MAY also include a SESSION-EXPIRES header. A period of 3 minutes (180) is recommended. The rules governing which ends performs the refresh are as [10].

When the refresher timer expires, it is recommended for this profile that the UPDATE method ([12]) be used to perform the refresh.

## **4 Voice Codecs**

This profile describes an inter-Call Agent SIP-T interface. Therefore, the supported voice codecs are dependent on the capabilities of the distant endpoints (e.g. a RGW or SIP Phone). This profile should not inhibit any media inter-working between the relevant endpoints. Codec negotiation is performed across this interface as described in [4].

## **5 Echo Control**

Not applicable to this IA. Echo control is performed at the distant endpoints (e.g. RGW or SIP Phone).

## 6 Modem, Fax and TTY Support

Not applicable to this IA. Modem/faxes are handled at the distant endpoints.

Even though the n/w preferred codec for the GMI2004 event is G711, the occurrence of fax/modem tones on a call MAY still result in a re-Offer/Answer sequence across the SIP-T interface in order to convey modified SDP blocks (e.g. additional media attribute lines such as *ecan* or *silencesupp*).

## **7 DTMF Digits and Telephony Tones**

DTMF Digits may be transparently passed between the endpoints using RFC 2833 or else signalled out of band via a SIP INFO message.

## 8 NAT & Firewall traversal

Dependent on trust / operator boundaries, it is possible for there to be a network side NAT/FW present at a SIP-T interface. In addition, it is also possible for there to be a SIP-T interface between a pair of Call Agents in the same Operator network in which case there would not necessarily be a NAT/FW. For GMI2004, the presence of NAT/FW for this IA shall be optional.

If a NAT/FW is present, then suitable signalling and media PHs must be controlled and the SDP (conveyed in the SIP) appropriately modified. Such a FW device could be realized via a separate NAT/FW controlled by a discrete protocol such as the ETSI Gate Control Profile ([5]) or MSF Gate Control Profile ([16]) or else via a SIP enabled ALG device.

## 9 QoS Aspects

The overall solution for QoS is described in the MSF Quality of Service for next generation VoIP networks solution framework ([8]). This solution framework uses DiffServ to provide differential service to VoIP traffic and data traffic. VoIP traffic is marked using DSCP (Differentiated Services Code Points) in the IP header, it can then be given priority by routers in the IP network.

If a NAT/FW is present between peer Call Agents, then the signalling/media packets (on entering the Operator's network) must be marked appropriately via DSCP. In general, Operators may wish to allocate the DSCP values within their network and therefore the DSCP actually used shall be configurable both for SIP-T signaling traffic and RTP/RTCP media.

## 10 Security Aspects

Generic SIP security requirements are provided in [15].

SIP-T can be employed as an inter-domain or intra-domain signalling mechanism. In the former case, it may be subject to pre-existing trust relationships between different administrative domains. The level of security required is dependent on the level of trust between the peer Call Agents. Examples of this are :-

- Authentication is based upon the known FQDN and potentially the IP address (peer Call Agents are likely to be given a fixed provisioned address).
- Use of HTTP digest to provide authentication between peer Call Agents (i.e. each end independently authenticates its peer).
- . Use of TLS and/or S/MIME.

For this IA, the first option shall be mandatory whilst the others are optional.

## 11 Redundancy & Resilience

The Call Agent must support redundancy. This is required to match the existing PSTN five-nine's level of reliability. In general, there are two ways to implement a redundant Call Agent :-

- Implement a primary and secondary Call Agent as separate components in the network
  - Primary and backup Call Agents have different domain names
- Implement a Call Agent with no single point of failure and full redundancy

To support the first scheme, peer Call Agents must support fail over to a secondary peer Call Agent if it detects a failure of the primary peer Call Agent.

In the second scheme, the Call Agent has its own redundant components that share the same Domain name or IP address and the peer Call Agents will be unaware that a failover has occurred.

Since the REGISTER event is not used in this profile, it is recommended that the second scheme be used for compliant Call Agents.

## 12 Management Information Model

### 12.1 SIP-T Route/Interface

The following items must be configurable on the Call Agent:-

- Fully Qualified Domain Name
- DHCP or fixed IP address (typically, MGC would have a provisioned IP address)
- If DHCP is not used
  - IP address
  - Subnet mask
  - Default IP gateway
- UDP Port to receive SIP-T signaling from peer Call Agents (default 5060)
- DSCP (TOS) byte value for SIP-T signaling traffic (applicable if FW present)
- DSCP (TOS) byte value for RTP voice traffic (applicable if FW present)
- Shared secret for digest authentication (if HTTP digest used)
- TLS Root Certificates (if TLS used)
- Maximum number of permitted calls/sessions (if policing is required)
- The trust status of the interface (trusted/untrusted)
- For the peer Call Agent
  - Domain Name or IP address
  - UDP Port to send SIP-T signalling (default 5060)

## 13 References

[1]	MSF-IA-SIP-T.001-FINAL – Implementation Agreement for SIP-T Profile for Media Gateway Controllers, June 2002
[2]	Not Used
[3]	IETF RFC 3204, "MIME media types for ISUP and QSIG Objects" December 2001
[4]	MSF2003.059.03 Implementation Agreement for SDP Usage & Codec Negotiation for GMI2004, February 2004
[5]	TS 102 333 v1.1.2 ETSI Gate Control Profile, June 2004
[6]	IETF – RFC 2327 SDP: Session Description Protocol, April 1998
[7]	IETF RFC 3264 An Offer / Answer Model with SDP, June 2002
[8]	MSF2003.105.00 QOS for Next generation VoIP Networks Solution Framework, October 2003
[9]	IETF RFC 3262, "Reliability of Provisional Responses in SIP", June 2002
[10]	IETF draft draft-ietf-sip-session-timers-13.txt, Session Timers in SIP, January 2004.
[11]	ITU-T Q1912.5, Inter-working between SIP and BICC/ISUP
[12]	IETF RFC 3311, "The SIP UPDATE Method", September 2002
[13]	IETF RFC 3261, "Session Initiation Protocol", June 2002
[14]	MSF2004.035.00, "IA for Core SIP Profile for VoIP"
[15]	MSF2003.016.03, "SIP Signalling Security for GMI2004"

[16]

MSF2004.032.01, "MSF IA for Gate Control using H248"

## **14 Acknowledgements**

The author would like to thank Takumi Ohba (NTT) who was the editor of [1] & Shinsaku Ogasawar (NTT) who provided updates to [1] based on GMI2002 experience. This document reproduces much of the content of [1].



F1

172.17.2.29 (5060) ---- INVITE(Encapsulated IAM) ----> 172.30.1.5 (5060)

INVITE tel:9724411111@172.30.1.5 SIP/2.0  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21478 INVITE  
Contact: tel:2143302105@172.17.2.29  
Session-Expires: 180  
Require: 100rel  
Supported: timer  
Record-Route: <sip: 172.17.2.29;lr>  
Allow: UPDATE  
Content-Length: xxx  
Content-Type: multipart/mixed; boundary=unique-boundary-1  
MIME-Version: 1.0

--unique-boundary-1  
Content-Type: application/SDP

(SDP contents)  
--unique-boundary-1  
Content-Type: application/ISUP; version=uk  
Content-Disposition: signal; handling=required

(Encapsulated IAM contents)  
--unique-boundary-1--

-----  
F2

172.30.1.5 (5060) ---- 100 Trying ----> 172.17.2.29 (5060)

SIP/2.0 100 Trying  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>  
Date: Sat, 01 Jan 2000 01:41:27 GMT  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21478 INVITE  
Content-Length: 0

-----  
F3

172.30.1.5 (5060) ---- 180 Ringing(Encapsulated ACM) ----> 172.17.2.29 (5060)

SIP/2.0 180 Ringing  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Date: Sat, 01 Jan 2000 01:41:27 GMT  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21478 INVITE  
Require: 100rel  
RSeq: 360

Contact: <tel:9724411111@172.30.1.5:5060>  
Allow: UPDATE  
Content-Length: xxx  
MIME-Version: 1.0  
Content-Type: multipart/mixed; boundary=unique-boundary-1  
MIME-Version: 1.0

--unique-boundary-1  
Content-Type: application/SDP

(SDP octets )  
--unique-boundary-1  
Content-Type: application/ISUP; version=uk  
Content-Disposition: signal; handling=required

(Encapsulated ACM)  
--unique-boundary-1--

-----  
F4  
172.17.2.29 (5060) ---- PRACK ----> 172.30.1.5 (5060)

PRACK tel:9724411111@172.30.1.5:5060 SIP/2.0  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21479 PRACK  
Content-Length: 0  
Contact: tel:2143302105@172.17.2.29  
RAck: 360 21478 INVITE

-----  
F5  
172.30.1.5 (5060) ---- 200 OK ----> 172.17.2.29 (5060)

SIP/2.0 200 OK  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Date: Sat, 01 Jan 2000 01:41:27 GMT  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21479 PRACK  
Content-Length: 0

-----  
F6  
172.30.1.5 (5060) ---- 200 OK(Encapsulated ANM) ----> 172.17.2.29 (5060)

SIP/2.0 200 OK  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Date: Sat, 01 Jan 2000 01:41:27 GMT  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29

CSeq: 21478 INVITE  
Contact: <tel:9724411111@172.30.1.5:5060>  
Record-Route: <sip: 172.17.2.29;lr>  
Allow: UPDATE  
Supported: timer  
Require: timer  
Session-Expires: 3600;refresher=uas  
Content-Length: xxx  
Content-Type: multipart/mixed; boundary=unique-boundary-1  
MIME-Version: 1.0

--unique-boundary-1  
Content-Type: application/SDP

(SDP)  
--unique-boundary-1  
Content-Type: application/ISUP; version=uk  
Content-Disposition: signal; handling=required

(Encapsulated ANM)  
--unique-boundary-1--

-----  
F7  
172.17.2.29 (5060) ---- ACK ----> 172.30.1.5 (5060)

ACK tel:9724411111@172.30.1.5:5060 SIP/2.0  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21478 ACK  
Content-Length: 0  
Contact: tel:2143302105@172.17.2.29

-----  
F8  
172.17.2.29 (5060)---- BYE(Encapsulated REL) ----> 172.30.1.5 (5060)

BYE tel:9724411111@172.30.1.5:5060 SIP/2.0  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Date: Sat, 01 Jan 2000 01:41:29 GMT  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
Max-Forwards: 6  
Timestamp: 946690894  
CSeq: 101 BYE  
Content-Length: xxx  
Content-Type: application/ISUP; version=uk  
Content-Disposition: signal; handling=required

(Encapsulated REL)

-----  
F9  
172.30.1.5 (5060) ---- 200 OK (Encapsulated RLC)----> 172.17.2.29 (5060)

SIP/2.0 200 OK  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 101 BYE  
Contact: <tel:9724411111@172.30.1.5:5060>  
Content-Length: xxx  
Content-Type: application/ISUP; version=uk  
Content-Disposition: signal; handling=required

(Encapsulated RLC)  
-----

## A.2 Suspend / Resume

A call is set up to supervision as in Appendix A.1 from CA#1 (172.17.2.19) to CA #2(172.30.1.5)..

Subsequently, the terminating party (e.g. H248 / MGCP line) goes on-hook which causes the call to be suspended. It is assumed that the Calling Party Clearing program would be operation.

Subsequently, the terminating party (e.g. H248 / MGCP line) goes off-hook which causes the call to be resumed.

172.17.2.29] [172.30.1.5]

### *CA#1 initiates the session*

F1 |---- INVITE(Encapsulated IAM) ---->|  
F2 |<----- 100 Trying -----|

### *Call is in ringing.*

F3 |<-- 180 Ringing(Encapsulated ACM) --|  
F4 |----- PRACK ----->|  
F5 |<----- 200 OK -----|

### *Call is answered.*

F6 |<---- 200 OK(Encapsulated ANM) ----|  
F7 |----- ACK ----->|

### *Call is connected.*

### *Call is suspended.*

F8 |<---- INFO(Encapsulated SUS) ----|  
F9 |----- 200 OK ----->|

### *Call is resumed.*

F10 |<---- INFO(Encapsulated RES) ----|  
F11 |----- 200 OK ----->|

### *Call in supervision.*

=====  
F1-F7 as appendix A.1.

-----  
F8  
172.17.2.29 (5060) ---- INFO (SUS) ----> 172.30.1.5 (5060)

INFO tel:9724411111@172.30.1.5:5060 SIP/2.0  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21480 INFO  
Content-Length: xxx  
Content-Type: application/ISUP; version=uk  
Content-Disposition: signal; handling=required

(Encapsulated SUS)  
-----

F9  
172.30.1.5 (5060) ---- 200 OK ----> 172.17.2.29 (5060)

SIP/2.0 200 OK  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Date: Sat, 01 Jan 2000 01:41:27 GMT  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21480 INFO  
Content-Length: 0

-----  
F10  
172.17.2.29 (5060) ---- INFO (RES) ----> 172.30.1.5 (5060)

INFO tel:9724411111@172.30.1.5:5060 SIP/2.0  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21481 INFO  
Content-Length: xxx  
Content-Type: application/ISUP; version=uk  
Content-Disposition: signal; handling=required

(Encapsulated RES)

-----  
F11  
172.30.1.5 (5060) ---- 200 OK ----> 172.17.2.29 (5060)

SIP/2.0 200 OK  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Date: Sat, 01 Jan 2000 01:41:27 GMT  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21481 INFO  
Content-Length: 0

---

---

## A.3 Mid Call Bearer Change

A call is set up to supervision as in Appendix A.1 from CA#1 (172.17.2.19) to CA #2(172.30.1.5)..

Subsequently, the terminating party (e.g. H248 / MGCP line) initiates a feature which causes a mid-call bearer change (e.g. moving the connection from one media endpoint to another) . It is assumed that the UPDATE method is used to convey the bearer change.

Note that each UPDATE/200 exchange is an Offer/Answer and there may be multiple such exchanges in either direction during a given call/session.

172.17.2.29] [172.30.1.5]

***CA#1 initiates the session***

F1 |---- INVITE(Encapsulated IAM) ---->|  
F2 |<----- 100 Trying -----|

***Call is in ringing.***

F3 |<-- 180 Ringing(Encapsulated ACM) ---|  
F4 |----- PRACK ----->|  
F5 |<----- 200 OK -----|

***Call is answered.***

F6 |<---- 200 OK(Encapsulated ANM) -----|  
F7 |----- ACK ----->|

***Call is connected.***

***Connection is modified (disconnected).***

F8 |<---- UPDATE(Encapsulated SDP) ----|  
F9 |----- 200 OK ----->|

***Connection is modified (new connection).***

F10 |<---- UPDATE (Encapsulated SDP) ---|  
F11 |----- 200 OK ----->|

=====  
F1-F7 as appendix A.1.

-----  
F8  
172.17.2.29 (5060) ---- UPDATE (SDP) ----> 172.30.1.5 (5060)

INFO tel:9724411111@172.30.1.5:5060 SIP/2.0  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21480 UPDATE  
Content-Length: xxx  
Content-Type: application/SDP

(SDP Octets)

-----  
F9

172.30.1.5 (5060) ---- 200 OK (SDP)----> 172.17.2.29 (5060)

SIP/2.0 200 OK  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Date: Sat, 01 Jan 2000 01:41:27 GMT  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21480 INFO  
Content-Length: xxx  
Content-Type: application/SDP

(SDP Octets)

-----  
F10  
172.17.2.29 (5060) ---- UPDATE (SDP) ----> 172.30.1.5 (5060)

INFO tel:9724411111@172.30.1.5:5060 SIP/2.0  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21481 UPDATE  
Content-Length: xxx  
Content-Type: application/SDP

(SDP Octets)

-----  
F11  
172.30.1.5 (5060) ---- 200 OK(SDP) ----> 172.17.2.29 (5060)

SIP/2.0 200 OK  
Via: SIP/2.0/UDP 172.17.2.29:5060  
From: <tel:2143302105@172.17.2.29>;tag=0E1D.8099  
To: <tel:9724411111@172.30.1.5>;tag=5CEE58-2187  
Date: Sat, 01 Jan 2000 01:41:27 GMT  
Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21481 UPDATE  
Content-Length: xxx  
Content-Type: application/SDP

(SDP Octets)

---



Call-ID: 0800.20CE.A152.3C5B.0E1D.8099@172.17.2.29  
CSeq: 21480 UPDATE  
Supported: timer  
Session-Expires: 3600  
Content-Length: 0  
-----