Why SIP-I?

A Switching Core Protocol Recommendation for GSM/UMTS Operators

August 2007

3G americas

TABLE OF CONTENTS

1. Abstract

The purpose of this white paper is to recommend that the wireless industry adopt a single session control protocol which will inter-work with the PSTN and support the creation, modification, and termination of packetized voice sessions in a GSM/UMTS network. The recommendation will be made based on comparison and analyses of three (3) candidate session control protocols that can inter-work with the PSTN: BICC, SIP-I, and SIP-T.

2. Introduction to Session Control

This section provides an introduction to the concept of sessions and session control.

Session control refers to the process used to create, modify, and terminate IP based communication sessions. A session can include two-way voice communication, multimedia (text, audio, or video) conference collaboration, instant messaging, application sharing, and other contemplated but not yet fully specified services. Session control is accomplished through signaling between various network elements and endpoints using a session control protocol. Examples of session control protocols include BICC, SIP, SIP-I, SIP-T, and H.323.

SIP (Session Initiation Protocol) is one of the more widely known examples of a session control protocol. It was defined by the IETF (Internet Engineering Task Force) and is used to create, modify, and terminate sessions with one or more participants. SIP is a peer-to-peer signaling protocol; it creates, terminates, and modifies sessions between peers.

According to RFC 3261 “SIP: Session Initiation Protocol”,

> “Session Initiation Protocol (SIP) [is] an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.
>
> “SIP invitations used to create sessions carry session descriptions that allow participants to agree on a set of compatible media types. SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide features to users. SIP also provides a registration function that allows users to upload their current locations for use by proxy servers. SIP runs on top of several different transport protocols.”

When the SIP protocol was originally created, the IETF community in general believed that the optimal future vision for communication services delivery would consist of a simple core network that primarily provided transparent transport and possibly call routing services. The IETF did not attempt to replicate the feature-rich services of the

PSTN. Instead, the SIP protocol was architected on the principle that most intelligence would move to the edge of the network and into the hands of end-users who would be free to innovate and implement their own services in the form of SIP clients.

The Next Generation Network (NGN) vision which has emerged in many parts of the telecommunications industry is not fully aligned with the original IETF SIP concept of a transparent transport network with most of the intelligence at the edge. One of the key drivers for NGN and network evolution in general is the ability for network operators to rapidly and cost-effectively develop new value-added services, and realize an appropriate and rewarding revenue stream for deploying, operating, and supporting these new services.

The SIP community must be credited with initially developing a robust protocol and architectural concept which has been easily adapted to support operators' requirements for their NGN and network evolution. Indeed, SIP signaling has been formally adopted as the Session Control Protocol by both 3GPP and 3GPP2 for IMS. In addition, SIP clients are now commonly used to deliver and extend services to wireline networked PCs, WLAN devices, mobile and fixed terminals, enterprise desksets, and a large number of other types of communication endpoints.

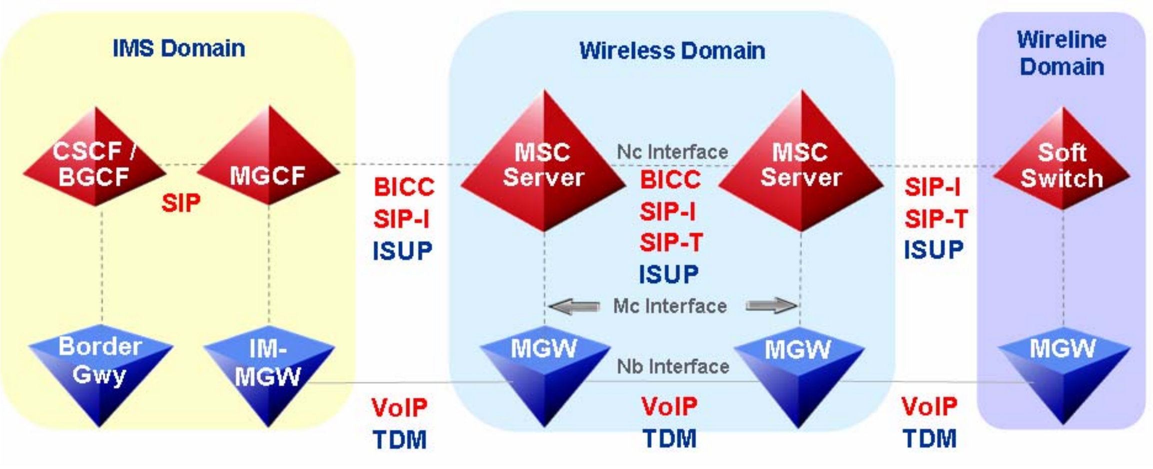
There are limitations of SIP, however. One of the key limitations of SIP is that it does not provide any method of directly interworking with the PSTN. The reason for this is that the IETF did not create SIP with the intention of full backward compatibility with legacy PSTN signaling mechanisms.

The lack of full SIP/PSTN interworking has many technical causes, primary among those being that the call signaling protocol used in the legacy PSTN (i.e. ISUP) is based on a fundamentally different call model than SIP. Under many circumstances, the ISUP call model requires a particular sequence of messaging for which no corresponding SIP message or messages have been defined. There are also cases in which the rich feature set available on the PSTN and facilitated by ISUP cannot be easily developed using SIP due to lack of corresponding SIP functionality. There are other cases in which regulatory requirements are most easily and immediately fulfilled by retaining an ability to deliver ISUP services as opposed to trying to meet complex regulatory mandates with a new SIP implementation.

The necessity of protocol interworking between networks based on SIP and ISUP was recognized by both the ITU and IETF who independently developed alternative methods for SIP with ISUP encapsulation referred to as SIP-I and SIP-T, respectively. The technical differences between the two methods of ISUP encapsulation are dealt with in detail later in the paper.

An alternative to SIP-T and SIP-I is BICC which was standardized by the ITU-T in 2000. BICC was developed to provide ISUP-like services over broadband connections. It can be used to create, modify, and terminate packetized voice calls between switches. This paper will also discuss reasons why SIP with ISUP encapsulation is preferred to BICC as the basis for evolution of GSM/UMTS networks.

The diagram on the next page shows where these session control protocols can be used in a GSM/UMTS core network.

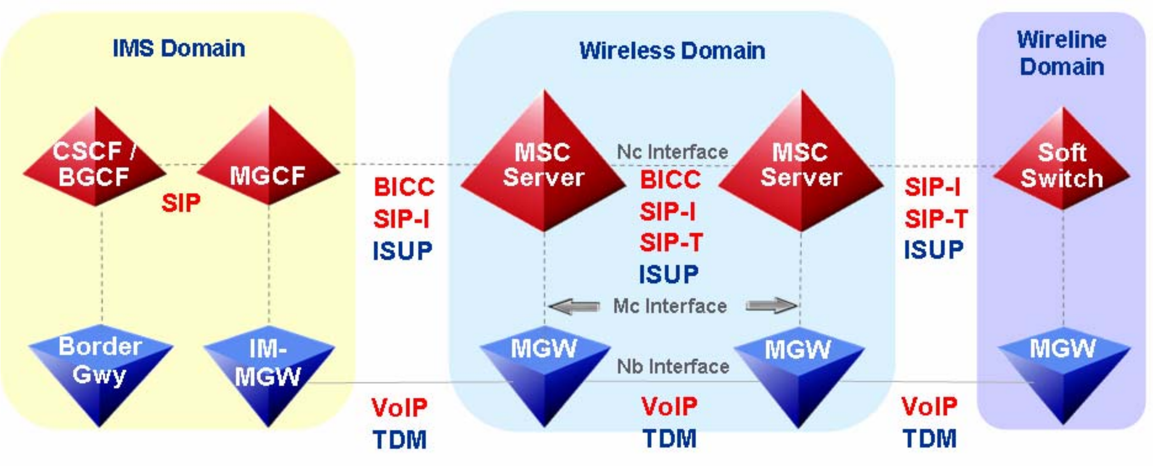


3. Executive Summary

There are three (3) session control protocols that interwork with the PSTN and can set up packetized voice calls (i.e. VoATM or VoIP) between switches in a GSM/UMTS network:

- Bearer Independent Call Control (BICC)
- SIP-T
- SIP-I

BICC was standardized by the International Telecommunication Union Standardization Sector (ITU-T), SIP-T by the IETF, and SIP-I by ITU-T and then ANSI. The diagram below shows where these three (3) protocols can be used in a GSM/UMTS core network.



BICC is a network level call control signaling protocol based on the existing narrowband ISUP specifications. It inherits the message and parameter set of ISUP and can therefore support the same services as ISUP. The Third Generation Partnership Project (3GPP) adopted BICC in the Universal Mobile Telecommunications Service (UMTS) Release 4 (2001) standard, a decision that was ahead of its time when compared to some of the other broadly adopted cellular standards of the day.

Defined by the IETF in 2002, Session Initiation Protocol (SIP) for Telephones (SIP-T) provides an extension to the standard SIP protocol to transport ISUP messages across a SIP network as attachments to the SIP messages. Defined by the ITU-T in 2004 and adopted by ANSI, Session Initiation Protocol (SIP) with encapsulated ISUP (SIP-I) also provides an extension to the standard SIP protocol to transport ISUP messages across a SIP network as attachments to the SIP messages.

These three (3) specifications all include an architectural context for interworking, mappings for specific parameters, and a mechanism for encapsulating ISUP messages. There are important technical differences between SIP-I and SIP-T, as well as between BICC and SIP with ISUP encapsulation, however.

At a high level, although BICC is the current session control protocol standardized in the 3GPP R4 architecture and deployed in some networks today, BICC is not an optimal choice for on-going evolution because it has been limited to, and is predicted to remain limited to, operation within a GSM/UMTS context. It does not appear that BICC was ever intended to, and currently being extended to, address domains beyond GSM/UMTS; as a result, BICC does not automatically offer the future level of flexibility of continued development and evolution that would occur by selecting one of the SIP with ISUP encapsulation variants (i.e. either SIP-T or SIP-I).

In comparing and contrasting the two (2) SIP technologies with ISUP encapsulation variants, the recommended direction for evolution is SIP-I based on a detailed technical analysis of capabilities existing within the two standards in their current form and considering as well the methods used to develop and evolve each standard. The two (2) standards differ in ways which can be linked to the differences between IETF and ITU in terms of operational practices, operating objectives, and underlying assumptions on industry dynamics and future industry evolution. The differences are highlighted next.

There are four (4) areas where SIP-I is better suited for a GSM/UMTS environment than SIP-T:

- Assumptions regarding the trust and security environment
- Encapsulation procedures & message mapping
- Support of RFCs
- User plane interoperability

In SIP-I, it is assumed that it is possible to provision trust domains and that any message received from an entity within the trust domain can be treated as if it had come from a valid network node. On the other hand, SIP-T assumes that trust can never be assumed on the basis of network location. The assumptions regarding trust domains form a core on top of which the protocols were developed, and as such leads directly to increased operational complexity in the case where it is assumed that trust domains do not exist. Appendix A, Section 7.1 covers this in more detail.

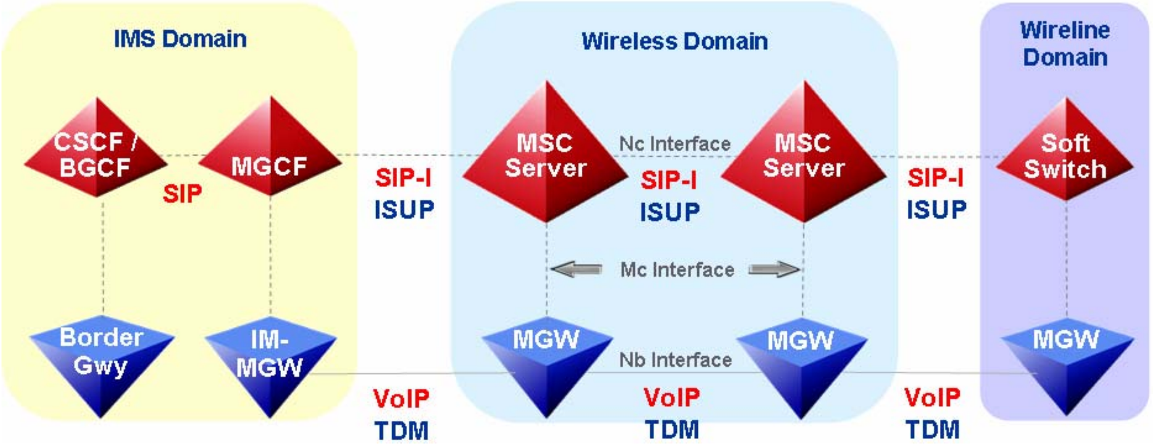
SIP-T is largely underspecified with regard to encapsulation procedures and message mapping as compared with SIP-I. The implication is that there is a higher degree of risk and uncertainty for initial SIP-T implementations which could be addressed with an increased emphasis on comprehensive interoperability testing of products at the end of the development cycle. Appendix A, Section 7.2 covers this in more detail.

The list of RFCs supported by SIP-I and SIP-T differ. For example, SIP-I provides a normative list of RFCs, whereas SIP-T provides mostly inferences. The implication is that there is a higher degree of risk and uncertainty associated with initial SIP-T implementations which could also be addressed with an increased emphasis on interoperability testing. Appendix A, Section 7.3 covers this in more detail.

SIP-T does not give any attention to interoperability of the user plane or define any media profile. SIP-I, however, defines a media profile and provides a normative list of RFCs which are required. Similar comments apply about the increased risks and uncertainties with initial SIP-T implementations. Appendix A, Section 7.3 covers this in more detail.

It is therefore recommended that all GSM/UMTS network operators put SIP-I on their network evolution roadmap as the session control protocol and evolve to it over time as operational requirements and/or service delivery requirements emerge. It is recognized that SIP-I/SIP-T adaptors or translators may be required to interface with some minor subset of networks or network elements, but this does not invalidate or change the main conclusion that SIP-I is the optimal session control protocol for GSM/UMTS networks.

The diagram below shows the recommendation from this white paper where the SIP-I protocol should be used in a GSM/UMTS core network. (Note: ISUP is still supported for TDM connections).



4. Session Control Protocols

There are three (3) session control protocols that support PSTN interworking and can set-up packetized voice calls between MSCs in a wireless network:

- Bearer Independent Call Control (BICC)
- SIP-T
- SIP-I

BICC was standardized by the International Telecommunication Union Standardization Sector (ITU-T), SIP-T by the IETF, and SIP-I by ITU-T and then ANSI.

This section briefly describes all three (3) session control protocols.

4.1. Bearer Independent Call Control (BICC)

The Bearer Independent Call Control (BICC) is a network level call control signaling protocol based on the existing narrowband ISUP specifications. BICC extends ISUP to allow BICC to provide the same set of ISDN services over a broadband backbone network that ISUP provides for TDM networks.

The first capability set of BICC was specified by the International Telecommunication Union Standardization Sector (ITU-T) in recommendation Q.1901 in 2000. BICC CS1 provided BICC call control an ATM bearer network. BICC was extended with capability set 2 (CS2) in recommendation Q.1902 in 2001. BICC CS 2 added the BCP (Bearer Control Protocol), the ability to control an IP bearer network, and the ability to perform codec negotiation and modification. The ITU-T BICC specification has not changed significantly since the CS2 publication.

BICC separates call control and bearer connection control, transporting BICC signaling independently of bearer establishment signaling. The signaling and call control can be centralized in a Call Service Function (CSF) Call Control Unit (CCU) while the bearer may be managed by one or more Media Control Function (MCF) Media Control Units (MCUs) or Media Gateways (MGWs). The bearer establishment may be initiated from either the originating or terminating side of a call. While BICC, like ISUP, establishes pair-wise links between nodes, BICC negotiates codecs on an end-to-end basis. The bearer codecs are negotiated through the exchange of BICC specific call establishment and mid-call signaling. The bearer control may use signaling outside of BICC, e.g., AAL2, or tunnel the bearer parameters within the BICC signaling as is done for IP using the IP Bearer Control Protocol (IPBCP).

BICC inherits the message and parameter set of ISUP and can therefore support the same services as ISUP. This also allows a natural interworking between ISUP and BICC without loss of ISUP service functionality. BICC maintains the separation established by ISUP of being a network call control protocol separate from access protocols.

The Third Generation Partnership Project (3GPP) adopted BICC CS2 in the Universal Mobile Telecommunications Service (UMTS) release 4 (2001). 3GPP specification TS 29.205 provides the application of the ITU-T specifications to the 3GPP network with additional 3GPP specifications in 23.205 and 23.153. 3GPP

BICC uses of the IuFP (Iu Framing Protocol), to carry the negotiated codec media packets between media gateways. This is the same framing as is used in the Radio Access Network (RAN).

4.2. SIP for Telephones (SIP-T)

Defined by the IETF in 2002, Session Initiation Protocol (SIP) for Telephones (SIP-T) provides an extension to the standard SIP protocol as defined by RFC 3261 to transport ISUP messages across a SIP network as attachments to the SIP messages.

SIP-T is defined by the four (4) IETF RFCs listed below. It should be noted that additional RFCs are referenced in these documents (e.g. RFC 3261 SIP: Session Initiation Protocol, and RFC 2976 – SIP Info Method), but are not explicitly identified here.

- RFC 3204 “MIME media types for ISUP and QSIG Objects” specifies the rules for encapsulating the ISUP messages within the SIP signaling messages.
- RFC 3372 “Session Initiation Protocol for Telephones (SIP-T): Context and Architectures” describes the architecture for interworking between ISUP and SIP-T.
- RFC 3398 “Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping” provides explicit rules for interworking between ISUP and SIP.
- RFC 3578 “Mapping of Integrated Services Digital Network (ISDN) User Part (ISUP) Overlap Signaling to the Session Initiation Protocol (SIP)” adds a discussion of the handling of overlap signaling. Note: Overlap signaling is not a concern for networks using ANSI ISUP.

SIP-T uses the Session Description Protocol (RFC 3264 “An Offer/Answer Model with SDP”) to provide media specific information for sessions that are being set up. SDP is attached to the SIP message and indicates the type of transport to be used for the media. In the case of audio packets, RTP/AVP transport and associated IETF framing (which is different from the IuPF framing used in 3GPP BICC) are used as defined by RFC 3550, 3551, and various codec specific RFCs. While SIP and SDP have mainly been developed to support IP networks, extensions to SDP have been defined to support ATM as well. The use of SIP for ATM networks has not seen wide deployment, however.

The SIP-T architecture as defined in RFC 3372 specifies two general network configurations: gateway and bridging.

In the gateway case, the Interworking Unit (IWU) performs the interworking between ISUP and SIP and manages the encapsulated ISUP messages. Signaling will occur between the IWU and a SIP client, e.g., a subscriber terminal. If the SIP client does not understand the encapsulated ISUP, ISUP services cannot be expected to be supported end to end as only the information mapped to SIP headers will be available to the SIP end point.

In the “bridging” case, SIP-T is used to connect PSTN exchanges through a SIP network. In the bridging case the encapsulated ISUP is used to carry additional ISUP service information, some of which cannot be reflected by SIP headers, across the SIP based packet network so that services may continue to be supported end to end without loss of functionality.

Since SIP-T provided the only standardized means to support ISUP services across a packet network at the time of publication (2002), it was quickly adopted by some network providers; however, it has not gained acceptance by the telecommunication standardization bodies. Instead, they later published their own solution – SIP-I.

4.3. SIP with encapsulated ISUP (SIP-I)

Session Initiation Protocol (SIP) with encapsulated ISUP (SIP-I) provides an extension to the standard SIP protocol, as defined by RFC 3261, to transport ISUP messages across a SIP network as attachments to the SIP messages. Both ITU-T and ANSI have standardized SIP-I and from this point on the term “SIP-I” will refer to both of these ISUP encapsulation scenarios.

SIP-I was standardized by ITU-T in 2004 in ITU-T Q.1912.5. The specification covers SIP interworking with ISUP (Q.761-Q.764) and BICC (Q.1902.1-Q.1902.4) and uses RFC 3402 for the encapsulation specification. It specifies actions for three profiles, A, B, and C. These profiles cover key interworking scenarios.

- Profile A specifically addresses 3GPP SIP requirements as documented in 3GPP TS 24.229 where encapsulated ISUP is not used. It also makes simplifying assumptions that are guaranteed to apply when interworking to a 3GPP network. The Media Gateway Control Function (MGCF) function in the 3GPP reference architecture uses this profile, with a few minor differences noted in an appendix of 3GPP TS 29.163. Profile A can only support ISUP services to the degree that can be provided through the information mapped into SIP headers.

- Profile B is a pure SIP solution which generalizes the 3GPP specific details of profile A to cover interworking with a range of ISUP networks. For example, it allows the option of overlap signaling propagation through the SIP network where Profile A does not (because mobile networks never generate overlap signaling).

  Profile B is also used in the gateway configuration when interworking between ISUP and SIP. Profile B is very similar to Profile A in that no ISUP encapsulation is provided, but the ISUP interworking default mappings are slightly different to accommodate interworking with PSTN networks. Profile B differs from SIP-T’s use in a gateway configuration in that Profile B does not provide encapsulated ISUP. Profile B can only support ISUP services to the degree that can be provided through the information mapped into SIP headers.

- Profile C, also known as SIP-I, is the same as Profile B with the addition of ISUP encapsulation. This is applicable where ISUP islands are interconnected via a SIP backbone. The encapsulated ISUP is used to meet regulatory requirements that are not yet supported by SIP. It can also be used to support key legacy services where SIP does not provide any equivalent functionality.

ITU-T Q.1912.5 is similar to the combination of the IETF RFCs 3398 and 3372, except that there are differences in both the interworking and encapsulation rules. Q.1912.5 went on to specify the interworking rules for the ISUP services where this was left unspecified by IETF. Similar to SIP-T, the SIP headers take precedence over any encapsulated information that may be present, with limited exceptions. The interworking rules are applied even when the ISUP message is not encapsulated.

ITU-T Q.1912.5 will also use the RTP/AVP transport and framing as specified by RFC 3550, 3551 and various codec specific RFCs. SIP-I explicitly references the SDP offer/answer rules as specified by IETF RFC 3264 (there is no explicit reference to these procedures by SIP-T).

ANSI T1.679 also covers SIP interworking with ISUP (T1.113-2000) and BICC (T1.673-2002). T1.679 is based upon Q.1912.5 and is intended to be compatible with that recommendation. However, it uses “network options” (ISUP encapsulation, SIP preconditions, etc.) instead of SIP profiles (e.g. Profile A, B or C). There are also some other minor differences between what these two (2) specifications consider to be part of their respective scopes. However, as outlined in this document, this specification is largely in alignment with its ITU predecessor.

Once standardized by ITU-T, SIP-I was incorporated by other standardization bodies, specifically ETSI and ANSI, and generally embraced by the industry as a more complete specification as compared to SIP-T. Most recently, 3GPP has untaken an effort to incorporate the use of SIP-I into the 3GPP specifications as an alternative to BICC for the Nc interface and as an outward facing protocol from the IMS MGCF. It is expected that the full technical specification of the SIP-I based Nc protocol will be provided during the 3GPP Release 8 timeframe.

4.4. Session Control Protocols Summary

These specifications for BICC, SIP-T and SIP-I include an architectural context for the interworking, mappings for specific parameters, and a mechanism for encapsulating ISUP messages. There are important technical differences between SIP-I and SIP-T, as well as between BICC and SIP with ISUP encapsulation. These differences will be described in the following section.

5. Session Control Protocol Comparison

5.1. BICC and SIP with ISUP Encapsulation

There are two (2) general reasons why SIP with ISUP encapsulation is preferred to BICC. First, there does not appear to be any enhancement work being done to BICC in any standards forum, implying that BICC will be limited to the capabilities it currently supports today with no apparent path forward for evolution and improvement. Second, there are concerns about the degree of interoperability with BICC across domains other than GMS/UMTS.

3GPP chose to standardize IMS around SIP, not BICC, which implies that the 3GPP does not view BICC as a long-term solution. While BICC is supported in IMS, interworking is required through the use of the MGCF and I-MGW. The MGCF provides SIP/BICC interworking while the I-MGW provides Nb/Mb conversion.

In addition, there does not appear to be any major enhancements being made either in the ITU or 3GPP for BICC. For example, there are no known plans to modify BICC so that it can easily create, modify, and terminate multimedia services as currently available in SIP.

There are concerns about the degree of interoperability with BICC between different types of network domains.

First, there are two versions of BICC: ITU standard Q.1902.1-6 and a modified version from 3GPP. The 3GPP version is not used in any wireline deployment; therefore, it would be difficult for a wireless operator using 3GPP BICC to peer with a wireline operator. This scenario can be avoided by use of SIP with encapsulated ISUP because these protocols are standardized for both wireline and wireless networks.

Second, there are few, if any, known cases in which BICC is used to peer between wireless and wireline carriers or between wireline carriers. BICC was standardized by 3GPP to serve as a method for carrying packetized voice between GSM/UMTS call servers within a single operator’s network, and when used for that function it performs as intended. Any attempt to extend BICC deployment to tasks beyond its originally envisaged and relatively narrow scope without a corresponding and supporting evolution of the protocol itself would present significant technical challenges.

Third, the media packet framing protocols used by BICC and SIP are different. BICC uses the 3GPP specific IuFP framing protocol while SIP framing is based on IETF specifications. Since IuFP is specific to 3GPP BICC, it is not as widely deployed as IETF based framing. Even the ITU version of BICC uses the IETF framing.

The IuFP framing used by BICC introduces a protocol layer above the RTP which duplicates some of the RTP functions; as a result, the IuFP framing is not as efficient as strict IETF. Furthermore, IuFP framing is not supported by SIP; therefore, when interworking between existing SIP networks (e.g., IMS or NGN), additional media resources are required to provide the framing conversion. In contrast, when IETF framing is used in both peering networks, it becomes possible to eliminate the media gateway at the interworking point.

5.2. SIP-I and SIP-T

There are five (5) areas where SIP-I and SIP-T differ:

- Trust and Security
- Encapsulation Procedures & Message Mapping
- Support of RFCs
- User Plane Interoperability
- Support of Forking

In SIP-I (and in the ITU-T and ANSI in general), it is assumed that it is possible to provision trust domains and that any message received from an entity within the trust domain can be treated as if it had come from a valid network node – i.e. a “trusted” node. In practice, the trust domain would be established by provisioning a private (or virtual private) secure network to connect all trusted nodes. This is deemed to be practical because the number of ISUP nodes in the SIP network will be relatively small.

On the other hand, SIP-T (and IETF in general) assumes that trust can never be assumed on the basis of network location (or apparent location). The IETF position is that it is always necessary to use cryptography at the application level to verify identity, establish trust, and to secure communication. This follows from the SIP architecture where any computer on the IP network could be a SIP node.

See Appendix A, Section 7.1 for a more detailed analysis on trust models.

SIP-T is largely underspecified with regard to encapsulation procedures and message mapping as compared with SIP-I. For example,

- SIP-T often does not provide the same level of detail on ISUP-SIP mappings,
- SIP-T barely considers non-call related messages unlike SIP-I which provides rules on how every ISUP message should be handled,
- SIP-T does not mention BICC interworking at all, which is covered by SIP-I, and
- SIP-T does not describe in detail interworking with Continuity procedures, whereas SIP-I provides detailed procedures for all scenarios (ISUP and BICC).

See Appendix A, Section 7.2 for a more detailed analysis of the difference in encapsulation procedures and message mapping.

The list of RFCs supported by SIP-I and SIP-T differ. For example, SIP-I provides a normative list of RFCs whereas SIP-T provides mostly inferences. In addition, several RFCs are considered optional by both, adding further IOT risk. Appendix A, Section 7.3 describes the differences in supported RFCs in much greater detail.

SIP-T does not give any attention to interoperability of the user plane or define any media profile. SIP-I, however, defines a media profile and provides a normative list of RFCs which are required. See Appendix A, Section 7.4 for more information.

SIP-I does not specify the procedures which would be required to handle forking in the SIP network, and note that forking is for further study. SIP-T has no restriction on forking, and RFC 3578 has explicit procedures to deal with it.

6. Conclusion and Recommendations

This white paper examined the relative merits of three (3) alternative session control protocols that can interwork with the PSTN and set up packetized voice calls between distributed architecture voice switches (i.e. softswitches, call servers, etc.) in a GSM/UMTS network.

The three (3) primary protocols examined in this paper were

- BICC,
- SIP-T, and
- SIP-I.

At a high level, it was determined that whereas BICC is the current session control protocol standardized in the 3GPP R4 architecture and deployed in some networks today, BICC is not an optimal choice for future evolution because it has been limited to, and is predicted to remain limited to, operation within a GSM/UMTS context. BICC is not being extended to address other domains, and as such does not offer the future level of flexibility and continued development and evolution that would occur by selecting one of the SIP with ISUP encapsulation variants (i.e. either SIP-T or SIP-I).

In comparing and contrasting the two (2) SIP with ISUP encapsulation variants, the recommended direction for evolution is SIP-I based on a detailed technical analysis of capabilities existing within the two (2) standards in their current form and considering as well the methods used to develop and evolve each standard. The two (2) standards differ in ways which can be linked to the differences between IETF and ITU in terms of operational practices, operating objectives, and underlying assumptions on industry dynamics and future industry evolution.

To summarize, there are four (4) areas where SIP-I is better suited for a GSM/UMTS environment than SIP-T:

- Assumptions on trust and security environment
- Encapsulation procedures & message mapping
- Support of RFCs
- User plane interoperability

In SIP-I, it is assumed that it is possible to provision trust domains and that any message received from an entity within the trust domain can be treated as if it had come from a valid network node. On the other hand, SIP-T assumes that trust can never be assumed on the basis of network location. Appendix A, Section 7.1 covers this in more detail.

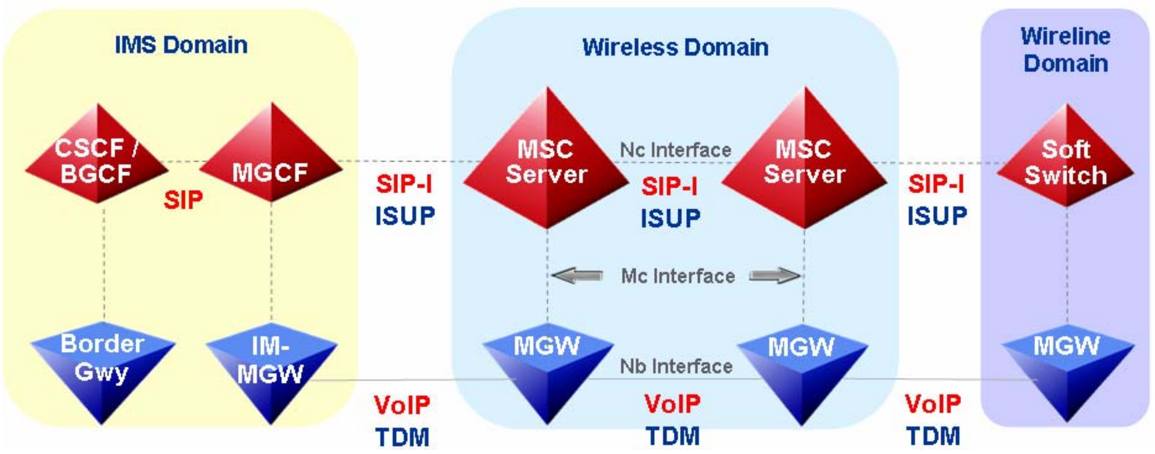
SIP-T is largely underspecified with regard to encapsulation procedures and message mapping as compared with SIP-I. Appendix A, Section 7.2 covers this in more detail.

The list of RFCs supported by SIP-I and SIP-T differ. For example, SIP-I provides a normative list of RFCs whereas SIP-T provides mostly inferences. Appendix A, Section 7.3 covers this in more detail.

SIP-T does not give any attention to interoperability of the user plane or define any media profile. SIP-I, however, defines a media profile and provides a normative list of RFCs which should be required. Appendix A, Section 7.3 covers this in more detail.

It is therefore recommended that the session control protocol for all future GSM/UMTS networks be defined to be SIP-I, and that all GSM/UMTS networks develop plans to evolve and migrate in a SIP-I direction over time. SIP-I should be fully incorporated into the 3GPP specifications in the Release 8 timeframe. It is recognized, however, that SIP-I/SIP-T adaptors or translators may be required to interface with some minor subset of networks or network elements, but this does not invalidate or change the main conclusion that SIP-I is the optimal session control protocol for GSM/UMTS networks.

The diagram below shows the recommendation from this white paper where the SIP-I protocol should be used in a GSM/UMTS core network. (Note: ISUP is still supported for TDM connections).



7. Appendix A: SIP-I vs. SIP-T

7.1. Trust Models

In SIP-I (and in the ITU-T and ANSI in general), it is assumed that it is possible to provision trust domains and that any message received from an entity within the trust domain can be treated as if it had come from a valid network node – i.e. a “trusted” node. In practice, the trust domain would be established by provisioning a private (or virtual private) secure network to connect all trusted nodes. This is deemed to be practical because the number of ISUP nodes in the SIP network will be relatively small.

On the other hand, SIP-T (and IETF in general) assumes that trust can never be assumed on the basis of network location (or apparent location). The IETF position is that it is always necessary to use cryptography at the application level to verify identity, establish trust, and to secure communication. This follows from the SIP architecture where any computer on the IP network could be a SIP node.

This difference in philosophy explains numerous differences between SIP-T and SIP-I. Several of the specific differences are highlighted below.

- The RFCs assume that it is not possible to know in advance whether the peer UA to a gateway is trusted or untrusted. In consequence, SIP-T recommends encryption of ISUP bodies, and includes authentication so that the receiver can determine whether the ISUP came from a legitimate source. SIP-I does not preclude the use of encryption as specified in RFC 3372, but it does leave security issues out of scope.
- Q.1912.5 and T1.679 assume a trust relationship between a gateway and its peer UA. This trust relationship means that:
    - Trust policy is configured. The gateway is required to filter the information it sends to the SIP network based on its configured trust policy,
    - Trust can be inferred. The remote peer is assumed to be a trusted source of subscriber identity information if a P-Asserted-Identity header field is present in incoming signaling.

Detailed security requirements are outside the scope of these specifications.

7.2. Encapsulation Procedures

This section identifies the specific differences in message mapping and encapsulation procedures between SIP-T and SIP-I.

7.2.1. BICC/ISUP Message Mapping and Encapsulation

7.2.1.1. Non-call-Related Messages

RFCs 3398/3578: Maintenance messages dealing with PSTN trunks are treated only as far as they affect the control of an ongoing call. Messages indicating error or congestion situations in the PSTN (MTP-3) and the recovery mechanisms used such as User Part Available and User Part Test ISUP messages are out of scope.

Q.1912.5: Provides a complete tabulation of ISUP messages, indicating which are encapsulated transparently, which are inter-worked, and which are terminated at the gateway.

T1.679: Aligns with Q.1912.5.

7.2.1.2. Generation of 183 Session Progress

RFC 3398: If INVITE contained an IAM, 183 Session Progress is withheld until an ACM is received. The RFC states that there are "known problems" with SIP bridging (i.e. SIP-I), although it does not elaborate on what these problems are.

Q.1912.5: Sending of IAM may be deferred until SIP precondition procedure is completed. This implies that there could be a return of 183 Session Progress and exchange of other messages even before IAM is sent.

T1.679: Aligns with Q.1912.5.

7.2.1.3. Overlap/SAM (Subsequent Address Message)

There is general agreement between RFC 3578 and Q.1912.5 on the procedures for overlap signaling, with the following exceptions:

RFC 3578: SAMs are encapsulated along with IAM in subsequent INVITEs.

Q.1912.5: subsequent INVITEs contain only the IAM (Request-URI contains all digits received to this point). Outgoing side uses interworking timers rather than ISUP timer T10.

T1.679: Not discussed as T1.113 does not support overlap signaling.

7.2.1.4. Early ACM

RFC 3398: States that early ACM SHOULD be interworked to 183 Session Progress.

Q.1912.5: Aligned with RFC 3398 with the additional definition of interworking timers (T_{IOW1} and T_{IOW2}) at the outgoing gateway which can generate early ACM independently of upstream activity.

T1.679: Aligned with Q.1912.5 except that only one timer (T_{IOW2}) is defined.

7.2.1.5. ACM with Cause

This applies when an ISDN terminal is sending back its own announcement or tone.

RFC 3398: Specifies that ACM with Cause interworks to 183 Session Progress "to cut through early media" and use of an interworking timer to end the call.

Q.1912.5: Specifies that ACM with Cause is not interworked other than by encapsulation (SIP-I). ISUP timers protect against indefinite prolongation of the call.

T1.679-2004: Aligns with Q.1912.5.

7.2.1.6. CPG (Call Progress)

RFC 3398: Contains the blanket statement that if the CPG “suggests that in-band information is available, the gateway SHOULD begin to transmit early media and cut through the unidirectional backwards media path.” For SIP bridging (i.e. SIP-I) it specifies mappings of ISUP event codes to SIP provisional responses. Also specifies interworking of Call Forward indications to provisional response 181 Call Is Being Forwarded.

Q.1912.5: For SIP-I the mappings of ISUP event codes to SIP provisional responses align with RFC 3398 except that there is no mention of the mappings for CPGs with Call Forward indications. Instead, it is stated that call forwarding in the PSTN requires no additional interworking beyond the use of ISUP encapsulation.

T1.679: Aligns with Q.1912.5.

7.2.1.7. SUS/RES (Suspend / Resume)

RFC 3398: Provides options for handling this. It allows re-INVITE for both media control and encapsulation or INFO for encapsulation only.

Q.1912.5: ITU-T considers SUS/RES to be a purely ISUP-side procedure for profiles A and B, and hence SUS is not interworked. For profile C, the INFO is used to encapsulate.

T1.679: Aligns with Q.1912.5, interworking is only valid with SIP-I, in which case the INFO is used for encapsulation.

7.2.1.8. RLC (Release Complete)

RFC 3398: This message is not interworked.

Q.1912.5: This is encapsulated in 200 OK (BYE) when the BYE contained an encapsulated REL. Specific requirements are also provided for interworking to satisfy the ISUP state machine in circumstances where RLC cannot be received.

T1.679: Aligns with Q.1912.5.

7.2.1.9. Continuity Procedures

RFC 3398: Devotes only a short section towards this, basically stating that when an IAM is received with the Continuity Check Indicator flag set, the gateway must not send the INVITE until continuity check has been finished.

Q.1912.5: Detailed procedures are defined for all cases. These are coordinated with SIP precondition procedure when latter is used.

T1.679: Aligns with Q.1912.5.

7.2.1.10. CFN (Confusion) on SIP side (presupposes encapsulation)

RFC 3398: Allow ISUP procedures to attempt recovery, and invoke SIP error procedures (call failure) only after repeated failure of ISUP procedures.

Q.1912.5: Allow ISUP procedures to attempt recovery or encapsulate in 183 Session Progress or INFO. There is no mention of SIP error procedures being invoked to take down the call; this is left up to ISUP.

T1.679: Aligns with Q.1912.5.

7.2.1.11. Miscellaneous ISUP Error Procedures on SIP Side

RFC 3398: Unspecified.

Q.1912.5: If encapsulation is used and normal ISUP would send RSC, send REL instead. Q.1912.5 also disables a number of ISUP procedures on SIP side, as represented by specified ISUP timers, to ensure correct interworking.

T1.679: Aligns with Q.1912.5.

7.2.2. SIP-to-ISUP Parameter Mapping

This section identifies differences in the way that SIP parameters (either initiated in the SIP network, or previously mapped to SIP from ISUP) are mapped into ISUP.

7.2.2.1. Called Party Number

In all cases, the Called Party Number is taken from the Request-URI.

RFC 3398: Request-URI can be either a SIP URI with the user=phone parameter (user info encoded as per RFC 2806 for a telephone-subscriber) or a tel: URI. SIP-T defines procedures for LNP (checks for “npdi” parameter) and transit network selection. Internal Network Number Indicator is unspecified.

Q.1912.5: Request-URI is assumed to be a SIP URI with the user=phone parameter (user info encoded as per RFC 2806 telephone-subscriber). The specific argument that a gateway will never receive tel: URIs in the Request-

URI because proxies will change them for routing purposes was accepted by SG 11. LNP and TNS are unspecified by Q.1912.5 because they are national matters. The Internal Network Number Indicator within the Called Party Number ISUP parameter must be set to "*routing to internal network number not allowed*".

T1.679: Same as Q.1912.5 except that LNP support is specified (“npdi” support). The Internal Network Number Indicator is not mentioned.

7.2.2.2. Calling Party's Category

RFC 3398: Defaults to "Ordinary calling subscriber" unless different value received in encapsulated ISUP.

Q.1912.5: Specifies the same procedure as RFC 3398.

T1.679: Defaults to “Calling party’s category unknown” unless different value received in encapsulated ISUP.

7.2.2.3. Nature of Connection Indicators

RFC 3398: Does not specify defaults for these indicators. Instead, RFC3398 states that the defaults for these indicators are to be configured by the operator.

Q.1912.5:

- Defaults specified for Satellite Indicator. SIP network is treated as a satellite hop (except for Profile C).
- Continuity check is set only if precondition negotiation is in progress.
- Profile A specifies as default that outgoing echo control is activated. No default for Profiles B or C.

T1.679: Aligns with Q.1912.5.

7.2.2.4. Forward Call Indicators

RFC 3398: Strongly recommends that if encapsulated ISUP is not available, the FCI values indicate "no interworking" and "ISUP used all the way" so as not to unduly limit feature interworking. This is based on the assumption that native SIP can provide features that are equivalent to any features supported by ISUP, and therefore the ISUP network can act as if there were “ISUP all the way.”

Q.1912.5: Profile A is more pessimistic in these settings, indicating in all respects that the SIP network is non-ISDN. Profile B leaves the settings to local policy and call information, while Profile C takes the settings from the encapsulated ISUP.

T1.679: Aligns with Q.1912.5 with additional guidance on setting of the M bit for LNP. For ISUP encapsulation, the FCI information is taken from the ISUP message. If no ISUP is encapsulated, the FCI values align with Q.1912.5 profile B (interworking encountered, ISUP *not* used all the way).

7.2.2.5. Backward Call Indicators

RFC 3398: Provides a complete specification.

Q.1912.5: Differences are similar to those for Forward Call Indicators.

T1.679: Aligns with Q.1912.5.

7.2.2.6. Transmission Medium Requirement / User Service Information / Application Transport

RFC 3398: Does not specify defaults for these indicators. Instead, RFC3398 states that the defaults for these indicators are to be configured by the operator. Interworking of SDP and BICC is not addressed.

Q.1912.5: Rules are specified for offers of G.711 -- require u-law networks to offer both u-law and A-law encoding in the initial offer. Default mapping rules between SDP and TMR/USI/HLC specified for the particular case where the gateway is not capable of transcoding. Otherwise SDP is a matter of local policy, but TMR and Access Transport Information received in encapsulated ISUP must be propagated to the BICC/ISUP network. Interworking of SDP and BICC (APP with BAT) is covered in an Appendix.

T1.679: Mostly aligns with Q.1912.5. Interworking of SDP and BICC is not addressed.

7.2.2.7. Calling Party Number

RFC 3398: Derived from the “From” header field if available in a suitable form.

Q.1912.5: Derived from P-Asserted-Identity if present, otherwise uses a network-provided number. The expectation is that P-Asserted-Identity has telephone number in the form "+" CC NDC SN. APRI set to "presentation restricted" if Privacy header field with value other than "none" is present. If Privacy header is absent, presentation is allowed. Mentions the scenario where the P-Asserted-Identity header contains both a tel: URI and a SIP URI, indicating this is for further study.

T1.679: Aligns with Q.1912.5.

7.2.2.8. Generic Number (Additional / Supplemental Calling Party Number)

RFC 3398: Only specified with respect to ANSI LNP procedures.

Q.1912.5: Derived from the From header field if present in suitable form. Inclusion may require a "special arrangement" with the SIP network. Same APRI as Calling Party Number. Screening Indicator is "user provided not verified".

T1.679: Aligns with Q.1912.5 (From header) as well as RFC 3398 (LNP scenario).

7.2.2.9. Hop Counter

RFC 3398: not specified.

Q.1912.5: For Profile C, taken from encapsulated ISUP. SIP network counts as one hop. For other profiles, this maps to/from Max-Forwards, with the intent of ensuring successive transits of an IWU decrease the Hop Counter. This requires engineering and application on a per source-destination basis as well as knowledge of network topology.

T1.679: Aligns with Q.1912.5.

7.2.2.10. Cause Value

RFC 3398: Encapsulated REL takes priority. Status code mapping attempts to take account of the semantics of the status code. SIP-specific concerns mapped to 127 Interworking. Location is set by default as "user" for 6xx and "network" for 4xx and 5xx.

Q.1912.5: Populated from encapsulated REL, Reason header field, or SIP status code in descending order of priority. To minimize potential impact of SIP terminals on ISUP network operations, most cause values not related to services are mapped to 127 Interworking. Derivation from Reason header field is a matter of local policy.

T1.679: Aligns with Q.1912.5.

7.2.2.11. Application transport (BAT) – BICC only

RFC 3398: Not specified.

Q.1912.5: Interworking is covered in Annex A.

T1.679: Not covered.

7.2.3. ISUP-to-SIP Parameter Mapping

Most differences of approach are consistent with the ISUP to SIP parameter mapping in the previous section, and are therefore not restated here.

7.3. RFC Support

This section shows the level of RFC support specified in SIP-T and SIP-T (both ITU-T Q.1912.5 and ANSI T1.679) with some clarifications following the table. Blank cells (N/A) imply that the issue is not discussed in that particular body of specifications.

RFC Support

Reference	SIP-I (ITU-T Q.1912.5)	SIP- I (ANSI T1.679)	SIP-T
RFC 2046 Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types	Required	Required	Required
RFC 2327 SDP: Session Description Protocol	Required	Required	Required
RFC 2633 S/MIME v3 (Note 1)	N/A	N/A	Recommended
RFC 2806 URLs for Telephone Calls (Note 2)	Required	Required	Required
RFC 2916 ENUM (Note 3)	N/A	N/A	Allowed
RFC 2976 The SIP INFO Method	Required by Profile C (SIP-I)	Required with SIP-I	Required
RFC 3204 MIME media types for ISUP Objects	Required by Profile C (SIP-I)	Required with SIP-I	Required
RFC 3219 TRIP (Note 3)	N/A	N/A	Allowed
RFC 3261 SIP: Session Initiation Protocol	Required	Required	Required
RFC 3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP) (Note 4)	Required by Profile A, optional with Profiles B and C	Optional	Optional
RFC 3264 An Offer/Answer Model with the Session Description Protocol (SDP) (Note 5)	Required	Required	Support implied by support of RFC 3261

Reference	SIP-I (ITU-T Q.1912.5)	SIP- I (ANSI T1.679)	SIP-T
RFC 3311 The Session Initiation Protocol UPDATE Method (Note 6)	Required with COT and SIP preconditions	Required with COT and SIP preconditions	Mentioned only in context of early media
RFC 3312 Integration of Resource Management and Session Initiation Protocol (SIP)	Required with SIP preconditions	Required with SIP preconditions	Optional
RFC 3323 Privacy	Optional, only relevant if Anonymous URIs are supported	Optional, only relevant if Anonymous URIs are supported	Optional, only relevant if Anonymous URIs are supported
RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks (Note 7)	Optional	Optional	N/A
RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP)	Optional	Optional	Optional

Note 1: The use of RFC 2633 S/MIME v3 to secure ISUP bodies is a recommendation in the text of RFC 3372, although it is shown as a normative reference. Q.1912.5 and T1.679 do not talk about security, considering this to be a matter of SIP-side procedures rather than interworking.

Note 2: SIP-T allows only SIP:URIs with user=phone while SIP-T allows SIP:URIs and Tel:URLs.

Note 3: The use of this RFC is a "MAY" in the text of RFC 3398, although it is shown as a normative reference. Q.1912.5 would consider this to be a matter of SIP-side procedures rather than interworking.

Note 4: RFC 3398 cites RFC 3262 as one option to achieve reliable delivery of provisional responses. The requirement is reliable delivery, not RFC 3262 itself. Q.1912.5 has taken the same attitude for profiles B and C, but profile A (3GPP) specifically mandates support of RFC 3262. T1.679 is ambiguous on this point but does not position RFC 3262 as mandatory.

Note 5: RFC 3264 Offer Answer is implicit for RFCs 3372/3398/3578, since it is a normative reference in RFC 3261. Q.1912.5 and T1.679 discuss this in the context of interworking call HOLD to SIP networks. While first mentioning that SIP-I handles this interworking via the encapsulated GPC message only, the specifications go on to show that the SDP actions defined in RFC 3261 are required.

Note 6: Q.1912.5 and T1.679 show interworking between SIP preconditions and continuity check in the PSTN, where RFC 3398 does not mention the procedure. (3GPP explicitly mandates support of RFC 3312 Preconditions.)

Note 7: RFC 3325 represents a key difference in philosophy between the IETF and the ITU-T/ANSI. Q.1912.5 and T1.679 show use the private extension to SIP defined in RFC 3325, which assumes a trusted network. The IETF, on the other hand, has tried to avoid reliance on provisioned trust agreements amongst SIP network entities. It is worth nothing that Q.1912.5 and T1.679 both define behaviors in to be followed when RFC 3325 is not used.

7.4. Media Support

The media profile (below) is an ITU-T idea (leveraged by ANSI T1.679) to ensure a minimum level of interoperability between gateways. It does not strictly relate to interworking. The specifications below are listed as normative requirements to the ITU-T Q.1912.5 and ANSI T1.679 recommendations. The IETF does not specify media profiles, but has specified RFC 2833 support as an alternative to carrying DTMF in INFO requests. Otherwise the media aspects are left unspecified, as a purely SIP concern.

Table X: Media Profile Comparison

Reference	SIP-I (ITU-T and ANSI)	SIP-T
RFC 2833 DTMF payload	Mandatory	Mandatory
RFC 3267 AMR and AMR-WB	Mandatory	Unspecified
RFC 3389 Comfort noise	Mandatory	Unspecified
RFC 3550 RTP	Mandatory	Unspecified
RFC 3551 Audio-video profile	Mandatory	Unspecified
ITU-T Rec. T.38	Mandatory	Unspecified

Acknowledgements

The mission of 3G Americas is to promote and facilitate the seamless deployment throughout the Americas of GSM and its evolution to 3G and beyond. 3G Americas' Board of Governor members include Alcatel-Lucent, Andrew Corporation, AT&T, Cable & Wireless, Ericsson, Gemalto, HP, Motorola, Nortel Networks, Nokia, Openwave, Research in Motion (RIM), Rogers (Canada), T-Mobile USA, Telcel (Mexico), Telefónica, and Texas Instruments.

We would like to recognize the significant project leadership and important contributions of Dave Brewer of Nortel Networks, W. Cooper Chastain of AT&T and James Calme of Alcatel-Lucent, as well as the other member companies from 3G Americas’ Board of Governors who participated in the development of this white paper.