Network Working Group
Request for Comments: 4497
BCP: 117
Category: Best Current Practice

J. Elwell
Siemens
F. Derks
NEC Philips
P. Mourot
O. Rousseau
Alcatel

May 2006

Interworking between the Session Initiation Protocol (SIP) and QSIG

Status of This Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This document specifies interworking between the Session Initiation Protocol (SIP) and QSIG within corporate telecommunication networks (also known as enterprise networks). SIP is an Internet application-layer control (signalling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include, in particular, telephone calls. QSIG is a signalling protocol for creating, modifying, and terminating circuit-switched calls (in particular, telephone calls) within Private Integrated Services Networks (PISNs). QSIG is specified in a number of Ecma Standards and published also as ISO/IEC standards.

Table of Contents

1. Introduction

This document specifies signalling interworking between QSIG and the Session Initiation Protocol (SIP) in support of basic services within a corporate telecommunication network (CN) (also known as enterprise network).

QSIG is a signalling protocol that operates between Private Integrated Services eXchanges (PINX) within a Private Integrated Services Network (PISN). A PISN provides circuit-switched basic services and supplementary services to its users. QSIG is specified in Ecma Standards; in particular, [2] (call control in support of basic services), [3] (generic functional protocol for the support of supplementary services), and a number of standards specifying individual supplementary services.

NOTE: The name QSIG was derived from the fact that it is used for signalling at the Q reference point. The Q reference point is a point of demarcation between two PINXs.

SIP is an application-layer protocol for establishing, terminating, and modifying multimedia sessions. It is typically carried over IP [15], [16]. Telephone calls are considered a type of multimedia session where just audio is exchanged. SIP is defined in [10].

As the support of telephony within corporate networks evolves from circuit-switched technology to Internet technology, the two technologies will coexist in many networks for a period, perhaps several years. Therefore, there is a need to be able to establish, modify, and terminate sessions involving a participant in the SIP network and a participant in the QSIG network. Such calls are supported by gateways that perform interworking between SIP and QSIG.

This document specifies SIP-QSIG signalling interworking for basic services that provide a bi-directional transfer capability for speech, DTMF, facsimile, and modem media between a PISN employing QSIG and a corporate IP network employing SIP. Other aspects of interworking, e.g., the use of RTP and SDP, will differ according to the type of media concerned and are outside the scope of this specification.

Call-related and call-independent signalling in support of supplementary services is outside the scope of this specification, but support for certain supplementary services (e.g., call transfer, call diversion) could be the subject of future work.

Interworking between QSIG and SIP permits a call originating at a user of a PISN to terminate at a user of a corporate IP network, or a call originating at a user of a corporate IP network to terminate at a user of a PISN.

Interworking between a PISN employing QSIG and a public IP network employing SIP is outside the scope of this specification. However, the functionality specified in this specification is in principle applicable to such a scenario when deployed in conjunction with other relevant functionality (e.g., number translation, security functions, etc.).

This specification is applicable to any interworking unit that can act as a gateway between a PISN employing QSIG and a corporate IP network employing SIP.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [4] and indicate requirement levels for compliant SIP implementations.

3. Definitions

For the purposes of this specification, the following definitions apply.

3.1. External Definitions

The definitions in [2] and [10] apply as appropriate.

3.2. Other definitions

3.2.1. Corporate Telecommunication Network (CN)

Sets of privately-owned or carrier-provided equipment that are located at geographically dispersed locations and are interconnected to provide telecommunication services to a defined group of users.

NOTE: A CN can comprise a PISN, a private IP network (intranet), or a combination of the two.

3.2.2. Gateway

An entity that performs interworking between a PISN using QSIG and an IP network using SIP.

3.2.3. IP Network

A network (unless otherwise stated, a corporate network) offering connectionless packet-mode services based on the Internet Protocol (IP) as the network-layer protocol.

3.2.4. Media Stream

Audio or other user information transmitted in UDP packets, typically containing RTP, in a single direction between the gateway and a peer entity participating in a session established using SIP.

NOTE: Normally a SIP session establishes a pair of media streams, one in each direction.

3.2.5. Private Integrated Services Network (PISN)

A CN or part of a CN that employs circuit-switched technology.

3.2.6. Private Integrated Services Network Exchange (PINX)

A PISN nodal entity comprising switching and call handling functions and supporting QSIG signalling in accordance with [2].

4. Acronyms

DNS	Domain Name Service
IP	Internet Protocol
PINX	Private Integrated services Network eXchange
PISN	Private Integrated Services Network
RTP	Real-time Transport Protocol
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TU	Transaction User
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol

5. Background and Architecture

During the 1980s, corporate voice telecommunications adopted technology similar in principle to Integrated Services Digital Networks (ISDN). Digital circuit switches, commonly known as Private Branch eXchanges (PBX) or more formally as Private Integrated services Network eXchanges (PINX) have been interconnected by digital transmission systems to form Private Integrated Services Networks (PISN). These digital transmission systems carry voice or other payload in fixed-rate channels, typically 64 Kbit/s, and signalling in a separate channel. A technique known as common channel signalling is employed, whereby a single signalling channel potentially controls a number of payload channels or bearer channels. A typical arrangement is a point-to-point transmission facility at T1 or E1 rate providing a 64 Kbit/s signalling channel and 23 or 30 bearer channels, respectively. Other arrangements are possible and have been deployed, including the use of multiple transmission facilities for a signalling channel and its logically associated bearer channels. Also, arrangements involving bearer channels at sub-64 Kbit/s have been deployed, where voice payload requires the use of codecs that perform compression.

QSIG is the internationally-standardized message-based signalling protocol for use in networks as described above. It runs in a signalling channel between two PINXs and controls calls on a number of logically associated bearer channels between the same two PINXs. The signalling channel and its logically associated bearer channels are collectively known as an inter-PINX link. QSIG is independent of the type of transmission capabilities over which the signalling channel and bearer channels are provided. QSIG is also independent of the transport protocol used to transport QSIG messages reliably over the signalling channel.

QSIG provides a means for establishing and clearing calls that originate and terminate on different PINXs. A call can be routed over a single inter-PINX link connecting the originating and terminating PINX, or over several inter-PINX links in series with switching at intermediate PINXs known as transit PINXs. A call can originate or terminate in another network, in which case it enters or leaves the PISN environment through a gateway PINX. Parties are identified by numbers, in accordance with either [17] or a private numbering plan. This basic call capability is specified in [2]. In addition to basic call capability, QSIG specifies a number of further capabilities supporting the use of supplementary services in PISNs.

More recently, corporate telecommunications networks have started to exploit IP in various ways. One way is to migrate part of the network to IP using SIP. This might, for example, be a new branch office with a SIP proxy and SIP endpoints instead of a PINX. Alternatively, SIP equipment might be used to replace an existing PINX or PINXs. The new SIP environment needs to interwork with the QSIG-based PISN in order to support calls originating in one environment and terminating in the other. Interworking is achieved through a gateway.

Interworking between QSIG and SIP at gateways can also be used where a SIP network interconnects different parts of a PISN, thereby allowing calls between the different parts. A call can enter the SIP network at one gateway and leave at another. Each gateway would behave in accordance with this specification.

Another way of connecting two parts of a PISN would be to encapsulate QSIG signalling in SIP messages for calls between the two parts. This is outside the scope of this specification but could be the subject of future work.

This document specifies signalling protocol interworking aspects of a gateway between a PISN employing QSIG signalling and an IP network employing SIP signalling. The gateway appears as a PINX to other PINXs in the PISN. The gateway appears as a SIP endpoint to other SIP entities in the IP network. The environment is shown in Figure 1.

```
        +------+   IP network                  PISN
        |      |
        |SIP   |                                             +------+
        |Proxy |                                            /|      |
        |      |                                           / |PINX  |
        +---+--+             *-----------+                /  |      |
            |                |           |        +-----+/   +------+
            |                |           |        |     |
            |                |           |        |PINX |
   ---+-----+-------+--------+  Gateway  +--------|     |
      |             |        |           |        |     |\
      |             |        |           |        +-----+ \
      |             |        |           |                 \ +------+
      |             |        |           |                  \|      |
   +--+---+      +--+---+    *-----------+                   |PINX  |
   |SIP   |      |SIP   |                                    |      |
   |End-  |      |End-  |                                    +------+
   |point |      |point |
   +------+      +------+
```

Figure 1: Environment

In addition to the signalling interworking functionality specified in this specification, it is assumed that the gateway also includes the following functionality:

- one or more physical interfaces on the PISN side supporting one or more inter-PINX links, each link providing one or more constant bit rate channels for media streams and a reliable layer 2 connection (e.g., over a fixed rate physical channel) for transporting QSIG signalling messages; and

- one or more physical interfaces on the IP network side supporting, through layer 1 and layer 2 protocols, IP as the network layer protocol and UDP [6] and TCP [5] as transport layer protocols, these being used for the transport of SIP signalling messages and, in the case of UDP, also for media streams;

- optionally the support of TLS [7] and/or SCTP [9] as additional transport layer protocols on the IP network side, these being used for the transport of SIP signalling messages; and

- a means of transferring media streams in each direction between the PISN and the IP network, including as a minimum packetization of media streams sent to the IP network and de-packetization of media streams received from the IP network.

NOTE: [10] mandates support for both UDP and TCP for the transport of SIP messages and allows optional support for TLS and/or SCTP for this same purpose.

The protocol model relevant to signalling interworking functionality of a gateway is shown in Figure 2.

```
   +-----------------------------------------------------------+
   |                   Interworking function                   |
   |                                                           |
   +-----------------------+---------+-----------------------+
   |                       |         |                       |
   |        SIP            |         |                       |
   |                       |         |                       |
   +-----------------------+         |                       |
   |                       |         |                       |
   |  UDP/TCP/TLS/SCTP     |         |        QSIG           |
   |                       |         |                       |
   +-----------------------+         |                       |
   |                       |         |                       |
   |        IP             |         |                       |
   |                       |         |                       |
   +-----------------------+         +-----------------------+
   |    IP network         |         |        PISN           |
   |    lower layers       |         |    lower layers       |
   |                       |         |                       |
   +-----------------------+         +-----------------------+
```

Figure 2: Protocol model

In Figure 2, the SIP box represents SIP syntax and encoding, the SIP transport layer, and the SIP transaction layer. The Interworking function includes SIP Transaction User (TU) functionality.

6. Overview

The gateway maps received QSIG messages, where appropriate, to SIP messages and vice versa and maintains an association between a QSIG call and a SIP dialog.

A call from QSIG to SIP is initiated when a QSIG SETUP message arrives at the gateway. The QSIG SETUP message initiates QSIG call establishment, and an initial response message (e.g., CALL PROCEEDING) completes negotiation of the bearer channel to be used for that call. The gateway then sends a SIP INVITE request, having translated the QSIG called party number to a URI suitable for inclusion in the Request-URI. The SIP INVITE request and the resulting SIP dialog, if successfully established, are associated with the QSIG call. The SIP 2xx response to the INVITE request is mapped to a QSIG CONNECT message, signifying answer of the call. During establishment, media streams established by SIP and SDP are connected to the bearer channel.

A call from SIP to QSIG is initiated when a SIP INVITE request arrives at the gateway. The gateway sends a QSIG SETUP message to initiate QSIG call establishment, having translated the SIP Request-URI to a number suitable for use as the QSIG called party number. The resulting QSIG call is associated with the SIP INVITE request and with the eventual SIP dialog. Receipt of an initial QSIG response message completes negotiation of the bearer channel to be used, allowing media streams established by SIP and SDP to be connected to that bearer channel. The QSIG CONNECT message is mapped to a SIP 200 OK response to the INVITE request.

Appendix A gives examples of typical message sequences that can arise.

7. General Requirements

In order to conform to this specification, a gateway SHALL support QSIG in accordance with [2] as a gateway and SHALL support SIP in accordance with [10] as a UA. In particular, the gateway SHALL support SIP syntax and encoding, the SIP transport layer, and the SIP transaction layer in accordance with [10]. In addition, the gateway SHALL support SIP TU behaviour for a UA in accordance with [10] except where stated otherwise in Sections 8, 9, and 10 of this specification.

NOTE: [10] mandates that a SIP entity support both UDP and TCP as transport layer protocols for SIP messages. Other transport layer protocols can also be supported.

The gateway SHALL also support SIP reliable provisional responses in accordance with [11] as a UA.

NOTE: [11] makes provision for recovering from loss of provisional responses (other than 100) to INVITE requests when using unreliable transport services in the IP network. This is important for ensuring delivery of responses that map to essential QSIG messages.

The gateway SHALL support SDP in accordance with [8] and its use in accordance with the offer/answer model in [12].

Section 9 also specifies optional use of the Privacy header in accordance with [13] and the P-Asserted-Identity header in accordance with [14].

The gateway SHALL support calls from QSIG to SIP and calls from SIP to QSIG.

SIP methods not defined in [10] or [11] are outside the scope of this specification but could be the subject of other specifications for interworking with QSIG, e.g., for interworking in support of supplementary services.

As a result of DNS lookup by the gateway in order to determine where to send a SIP INVITE request, a number of candidate destinations can be attempted in sequence. The way in which this is handled by the gateway is outside the scope of this specification. However, any behaviour specified in this document on receipt of a SIP 4xx or 5xx final response to an INVITE request SHOULD apply only when there are no more candidate destinations to try or when overlap signalling applies in the SIP network (see 8.2.2.2).

8. Message Mapping Requirements

8.1. Message Validation and Handling of Protocol Errors

The gateway SHALL validate received QSIG messages in accordance with the requirements of [2] and SHALL act in accordance with [2] on detection of a QSIG protocol error. The requirements of this section for acting on a received QSIG message apply only to a received QSIG message that has been successfully validated and that satisfies one of the following conditions:

-the QSIG message is a SETUP message and indicates a destination in the IP network and a bearer capability for which the gateway is able to provide interworking; or

-the QSIG message is a message other than SETUP and contains a call reference that identifies an existing call for which the gateway is providing interworking between QSIG and SIP.

The processing of any valid QSIG message that does not satisfy any of these conditions is outside the scope of this specification. Also, the processing of any QSIG message relating to call-independent signalling connections or connectionless transport, as specified in [3], is outside the scope of this specification.

If segmented QSIG messages are received, the gateway SHALL await receipt of all segments of a message and SHALL validate and act on the complete reassembled message.

The gateway SHALL validate received SIP messages (requests and responses) in accordance with the requirements of [10] and SHALL act in accordance with [10] on detection of a SIP protocol error.

Requirements of this section for acting on a received SIP message apply only to a received message that has been successfully validated and that satisfies one of the following conditions:

- the SIP message is an INVITE request that contains no tag parameter in the To header field, does not match an ongoing transaction (i.e., is not a merged request; see Section 8.2.2.2 of [10]), and indicates a destination in the PISN for which the gateway is able to provide interworking; or

- the SIP message is a request that relates to an existing dialog representing a call for which the gateway is providing interworking between QSIG and SIP; or

- the SIP message is a CANCEL request that relates to a received INVITE request for which the gateway is providing interworking with QSIG but for which the only response sent is informational (1xx), no dialog having been confirmed; or

- the SIP message is a response to a request sent by the gateway in accordance with this section.

The processing of any valid SIP message that does not satisfy any of these conditions is outside the scope of this specification.

NOTE: These rules mean that an error detected in a received message will not be propagated to the other side of the gateway. However, there can be an indirect impact on the other side of the gateway, e.g., the initiation of call clearing procedures.

The gateway SHALL run QSIG protocol timers as specified in [2] and SHALL act in accordance with [2] if a QSIG protocol timer expires. Any other action on expiry of a QSIG protocol timer is outside the scope of this specification, except that if it results in the clearing of the QSIG call, the gateway SHALL also clear the SIP call in accordance with Section 8.4.5.

The gateway SHALL run SIP protocol timers as specified in [10] and SHALL act in accordance with [10] if a SIP protocol timer expires. Any other action on expiry of a SIP protocol timer is outside the scope of this specification, except that if it results in the clearing of the SIP call, the gateway SHALL also clear the QSIG call in accordance with Section 8.4.5.

8.2. Call Establishment from QSIG to SIP

8.2.1. Call Establishment from QSIG to SIP Using En Bloc Procedures

The following procedures apply when the gateway receives a QSIG SETUP message containing a Sending Complete information element or the gateway receives a QSIG SETUP message and is able to determine that the number in the Called party number information element is complete.

NOTE: In the absence of a Sending Complete information element, the means by which the gateway determines the number to be complete is an implementation matter. It can involve knowledge of the numbering plan and/or use of inter-digit timer expiry.

8.2.1.1. Receipt of QSIG SETUP Message

On receipt of a QSIG SETUP message containing a number that the gateway determines to be complete in the Called party number information element, or containing a Sending complete information element and a number that could potentially be complete, the gateway SHALL map the QSIG SETUP message to a SIP INVITE request. The gateway SHALL also send a QSIG CALL PROCEEDING message.

The gateway SHALL generate the SIP Request-URI, To, and From fields in the SIP INVITE request in accordance with Section 9. The gateway SHALL include in the INVITE request a Supported header containing option tag 100rel, to indicate support for [11].

The gateway SHALL include SDP offer information in the SIP INVITE request as described in Section 10. It SHOULD also connect the incoming media stream to the user information channel of the inter-PINX link, to allow the caller to hear in-band tones or announcements and prevent speech clipping on answer. Because of forking, the gateway may receive more than one media stream, in which case it SHOULD select one (e.g., the first received). If the gateway is able to correlate an unselected media stream with a particular early dialog established using a reliable provisional response, it MAY use the UPDATE method [19] to stop that stream and then use the UPDATE method to start that stream again if a 2xx response is received on that dialog.

On receipt of a QSIG SETUP message containing a Sending complete information element and a number that the gateway determines to be incomplete in the Called party number information element, the gateway SHALL initiate QSIG call clearing procedures using cause value 28, "invalid number format (address incomplete)".

If information in the QSIG SETUP message is unsuitable for generating any of the mandatory fields in a SIP INVITE request (e.g., if a Request-URI cannot be derived from the QSIG Called party number information element) or for generating SDP information, the gateway SHALL NOT issue a SIP INVITE request and SHALL initiate QSIG call clearing procedures in accordance with [2].

8.2.1.2. Receipt of SIP 100 (Trying) Response to an INVITE Request

A SIP 100 response SHALL NOT trigger any QSIG messages. It only serves the purpose of suppressing INVITE request retransmissions.

8.2.1.3. Receipt of SIP 18x provisional response to an INVITE request

The gateway SHALL map a received SIP 18x response to an INVITE request to a QSIG PROGRESS or ALERTING message based on the following conditions.

- If a SIP 180 response is received and no QSIG ALERTING message has been sent, the gateway SHALL generate a QSIG ALERTING message. The gateway MAY supply ring-back tone on the user information channel of the inter-PINX link, in which case the gateway SHALL include progress description number 8 in the QSIG ALERTING message. Otherwise the gateway SHALL NOT include progress description number 8 in the QSIG ALERTING message unless the gateway is aware that in-band information (e.g., ring-back tone) is being transmitted.

- If a SIP 181/182/183 response is received, no QSIG ALERTING message has been sent, and no message containing progress description number 1 has been sent, the gateway SHALL generate a QSIG PROGRESS message containing progress description number 1.

NOTE: This will ensure that QSIG timer T310 is stopped if running at the Originating PINX.

In all other scenarios, the gateway SHALL NOT map the SIP 18x response to a QSIG message.

If the SIP 18x response contains a Require header with option tag 100rel, the gateway SHALL send back a SIP PRACK request in accordance with [11].

8.2.1.4. Receipt of SIP 2xx Response to an INVITE Request

If the gateway receives a SIP 2xx response as the first SIP 2xx response to a SIP INVITE request, the gateway SHALL map the SIP 2xx response to a QSIG CONNECT message. The gateway SHALL also send a SIP ACK request to acknowledge the 2xx response. The gateway SHALL

NOT include any SDP information in the SIP ACK request. If the gateway receives further 2xx responses, it SHALL respond to each in accordance with [10], SHOULD issue a BYE request for each, and SHALL NOT generate any further QSIG messages.

Media streams will normally have been established in the IP network in each direction. If so, the gateway SHALL connect the media streams to the corresponding user-information channel on the inter-PINX link if it has not already done so and stop any local ring-back tone.

If the SIP 2xx response is received in response to the SIP PRACK request, the gateway SHALL NOT map this message to any QSIG message.

NOTE: A SIP 2xx response to the INVITE request can be received later on a different dialog as a result of a forking proxy.

8.2.1.5. Receipt of SIP 3xx Response to an INVITE Request

On receipt of a SIP 3xx response to an INVITE request, the gateway SHALL act in accordance with [10].

NOTE: This will normally result in sending a new SIP INVITE request.

Unless the gateway supports the QSIG Call Diversion Supplementary Service, no QSIG message SHALL be sent. The definition of Call Diversion Supplementary Service for QSIG to SIP interworking is beyond the scope of this specification.

8.2.2. Call Establishment from QSIG to SIP Using Overlap Procedures

SIP uses en bloc signalling, and it is strongly RECOMMENDED to avoid using overlap signalling in a SIP network. A SIP/QSIG gateway dealing with overlap signalling SHOULD perform a conversion from overlap to en bloc signalling method using one or more of the following mechanisms:

- timers;

- numbering plan information;

- the presence of a Sending complete information element in a received QSIG INFORMATION message.

If the gateway performs a conversion from overlap to en bloc signalling in the SIP network, then the procedures defined in Section 8.2.2.1 SHALL apply.

However, for some applications it might be impossible to avoid using overlap signalling in the SIP network. In this case, the procedures defined in Section 8.2.2.2 SHALL apply.

8.2.2.1. En Bloc Signalling in SIP Network

8.2.2.1.1. Receipt of QSIG SETUP Message

On receipt of a QSIG SETUP message containing no Sending complete information element and a number in the Called party number information element that the gateway cannot determine to be complete, the gateway SHALL send back a QSIG SETUP ACKNOWLEDGE message, start QSIG timer T302, and await further number digits.

8.2.2.1.2. Receipt of QSIG INFORMATION Message

On receipt of each QSIG INFORMATION message containing no Sending complete information element and containing a number that the gateway cannot determine to be complete, QSIG timer T302 SHALL be restarted. When QSIG timer T302 expires or a QSIG INFORMATION message containing a Sending complete information element is received, the gateway SHALL send a SIP INVITE request as described in Section 8.2.1.1. The Request-URI and To fields (see Section 9) SHALL be generated from the concatenation of information in the Called party number information element in the received QSIG SETUP and INFORMATION messages. The gateway SHALL also send a QSIG CALL PROCEEDING message.

8.2.2.1.3. Receipt of SIP Responses to INVITE Requests

SIP responses to INVITE requests SHALL be mapped as described in 8.2.1.

8.2.2.2. Overlap Signalling in SIP Network

The procedures below for using overlap signalling in the SIP network are in accordance with the principles described in [18] for using overlap sending when interworking with ISDN User Part (ISUP). In [18], there is discussion of some potential problems arising from the use of overlap sending in the SIP network. These potential problems are applicable also in the context of QSIG-SIP interworking and can be avoided if overlap sending in the QSIG network is terminated at the gateway, in accordance with Section 8.2.2.1. The procedures below should be used only where it is not feasible to use the procedures of Section 8.2.2.1.

8.2.2.2.1. Receipt of QSIG SETUP Message

On receipt of a QSIG SETUP message containing no Sending complete information element and a number in the Called party number information element that the gateway cannot determine to be complete, the gateway SHALL send back a QSIG SETUP ACKNOWLEDGE message and start QSIG timer T302. If the QSIG SETUP message contains the minimum number of digits required to route the call in the IP network, the gateway SHALL send a SIP INVITE request as specified in Section 8.2.1.1. Otherwise, the gateway SHALL wait for more digits to arrive in QSIG INFORMATION messages.

8.2.2.2.2. Receipt of QSIG INFORMATION Message

On receipt of a QSIG INFORMATION message, the gateway SHALL handle the QSIG timer T302 in accordance with [2].

NOTE: [2] requires the QSIG timer to be stopped if the INFORMATION message contains a Sending complete information element or to be restarted otherwise.

Further behaviour of the gateway SHALL depend on whether or not it has already sent a SIP INVITE request. If the gateway has not sent a SIP INVITE request and it now has the minimum number of digits required to route the call, it SHALL send a SIP INVITE request as specified in Section 8.2.2.1.2. If the gateway still does not have the minimum number of digits required, it SHALL wait for more QSIG INFORMATION messages to arrive.

If the gateway has already sent one or more SIP INVITE requests, whether or not final responses to those requests have been received, it SHALL send a new SIP INVITE request in accordance with Section 3.2 of [18]. The updated Request-URI and To fields (see Section 9) SHALL be generated from the concatenation of information in the Called party number information element in the received QSIG SETUP and INFORMATION messages.

NOTE: [18] requires the new request to have the same Call-ID and the same From header (including tag) as in the previous INVITE request. [18] recommends that the CSeq header should contain a value higher than that in the previous INVITE request.

8.2.2.2.3. Receipt of SIP 100 (Trying) Response to an INVITE Request

The requirements of Section 8.2.1.2 SHALL apply.

8.2.2.2.4. Receipt of SIP 18x Provisional Response to an INVITE Request

The requirements of Section 8.2.1.3 SHALL apply.

8.2.2.2.5. Receipt of SIP 2xx Response to an INVITE Request

The requirements of Section 8.2.1.4 SHALL apply. In addition, the gateway SHALL send a SIP CANCEL request in accordance with Section 3.4 of [18] to cancel any SIP INVITE transactions for which no final response has been received.

8.2.2.2.6. Receipt of SIP 3xx Response to an INVITE Request

The requirements of Section 8.2.1.5 SHALL apply.

8.2.2.2.7. Receipt of a SIP 4xx, 5xx, or 6xx Final Response to an INVITE Request

On receipt of a SIP 4xx, 5xx, or 6xx final response to an INVITE request, the gateway SHALL send back a SIP ACK request. Unless the gateway is able to retry the INVITE request to avoid the problem (e.g., by supplying authentication in the case of a 401 or 407 response), the gateway SHALL also send a QSIG DISCONNECT message (8.4.4) if no further QSIG INFORMATION messages are expected and final responses have been received to all transmitted SIP INVITE requests.

NOTE: Further QSIG INFORMATION messages will not be expected after QSIG timer T302 has expired or after a Sending complete information element has been received.

In all other cases, the receipt of a SIP 4xx, 5xx, or 6xx final response to an INVITE request SHALL NOT trigger the sending of any QSIG message.

NOTE: If further QSIG INFORMATION messages arrive, these will result in further SIP INVITE requests being sent, one of which might result in successful call establishment. For example, initial INVITE requests might produce 484 (Address Incomplete) or 404 (Not Found) responses because the Request-URIs derived from incomplete numbers cannot be routed, yet a subsequent INVITE request with a routable Request-URI might produce a 2xx final response or a more meaningful 4xx, 5xx, or 6xx final response.

8.2.2.2.8. Receipt of Multiple SIP Responses to an INVITE Request

Section 3.3 of [18] applies.

8.2.2.2.9. Cancelling Pending SIP INVITE Transactions

As stated in Section 3.4 of [18], when a gateway sends a new SIP INVITE request containing new digits, it SHOULD NOT send a SIP CANCEL request to cancel a previous SIP INVITE transaction that has not had a final response. This SIP CANCEL request could arrive at an egress gateway before the new SIP INVITE request and trigger premature call clearing.

NOTE: Previous SIP INVITE transactions can be expected to result in SIP 4xx class responses, which terminate the transaction. In Section 8.2.2.2.5, there is provision for cancelling any transactions still in progress after a SIP 2xx response has been received.

8.2.2.2.10. QSIG Timer T302 Expiry

If QSIG timer T302 expires and the gateway has received 4xx, 5xx, or 6xx responses to all transmitted SIP INVITE requests, the gateway SHALL send a QSIG DISCONNECT message. If T302 expires and the gateway has not received 4xx, 5xx, or 6xx responses to all transmitted SIP INVITE requests, the gateway SHALL ignore any further QSIG INFORMATION messages but SHALL NOT send a QSIG DISCONNECT message at this stage.

NOTE: A QSIG DISCONNECT request will be sent when all outstanding SIP INVITE requests have received 4xx, 5xx, or 6xx responses.

8.3. Call Establishment from SIP to QSIG

8.3.1. Receipt of SIP INVITE Request for a New Call

On receipt of a SIP INVITE request for a new call, if a suitable channel is available on the inter-PINX link, the gateway SHALL generate a QSIG SETUP message from the received SIP INVITE request. The gateway SHALL generate the Called party number and Calling party number information elements in accordance with Section 9 and SHALL generate the Bearer capability information element in accordance with Section 10. If the gateway can determine that the number placed in the Called party number information element is complete, the gateway MAY include the Sending complete information element.

NOTE: The means by which the gateway determines the number to be complete is an implementation matter. It can involve knowledge of the numbering plan and/or use of the inter-digit timer.

The gateway SHOULD send a SIP 100 (Trying) response.

If information in the SIP INVITE request is unsuitable for generating any of the mandatory information elements in a QSIG SETUP message (e.g., if a QSIG Called party number information element cannot be derived from SIP Request-URI field) or if no suitable channel is available on the inter-PINX link, the gateway SHALL NOT issue a QSIG SETUP message and SHALL send a SIP 4xx, 5xx, or 6xx response. If no suitable channel is available, the gateway should use response code 503 (Service Unavailable).

If the SIP INVITE request does not contain SDP information and does not contain either a Required header or a Supported header with option tag 100rel, the gateway SHOULD still proceed as above, although an implementation can instead send a SIP 488 (Not Acceptable Here) response, in which case it SHALL NOT issue a QSIG SETUP message.

NOTE: The absence of SDP offer information in the SIP INVITE request means that the gateway might need to send SDP offer information in a provisional response and receive SDP answer information in a SIP PRACK request (in accordance with [11]) in order to ensure that tones and announcements from the PISN are transmitted. SDP offer information cannot be sent in an unreliable provisional response because SDP answer information would need to be returned in a SIP PRACK request. The recommendation above still to proceed with call establishment in this situation reflects the desire to maximise the chances of a successful call. However, if important in-band information is likely to be denied in this situation, a gateway can choose not to proceed.

NOTE: If SDP offer information is present in the INVITE request, the issuing of a QSIG SETUP message is not dependent on the presence of a Required header or a Supported header with option tag 100rel.

On receipt of a SIP INVITE request relating to a call that has already been established from SIP to QSIG, the procedures of 8.3.9 SHALL apply.

8.3.2. Receipt of QSIG CALL PROCEEDING Message

The receipt of a QSIG CALL PROCEEDING message SHALL NOT result in any SIP message being sent.

8.3.3. Receipt of QSIG PROGRESS Message

A QSIG PROGRESS message can be received in the event of interworking on the remote side of the PISN or if the PISN is unable to complete the call and generates an in-band tone or announcement. In the latter case, a Cause information element is included in the QSIG PROGRESS message.

The gateway SHALL map a received QSIG PROGRESS message to a SIP 183 (Session Progress) response to the INVITE request. If the SIP INVITE request contained either a Require header or a Supported header with option tag 100rel, the gateway SHALL include in the SIP 183 response a Require header with option tag 100rel.

NOTE: In accordance with [11], inclusion of option tag 100rel in a provisional response instructs the UAC to acknowledge the provisional response by sending a PRACK request. [11] also specifies procedures for repeating a provisional response with option tag 100rel if no PRACK is received.

If the QSIG PROGRESS message contained a Progress indicator information element with Progress description number 1 or 8, the gateway SHALL connect the media streams to the corresponding user information channel of the inter-PINX link if it has not already done so, provided that SDP answer information is included in the transmitted SIP response to the INVITE request or has already been sent or received. Inclusion of SDP offer or answer information in the 183 provisional response SHALL be in accordance with Section 8.3.5.

If the QSIG PROGRESS message is received with a Cause information element, the gateway SHALL either wait until the tone/announcement is complete or has been applied for sufficient time before initiating call clearing, or wait for a SIP CANCEL request. If call clearing is initiated, the cause value in the QSIG PROGRESS message SHALL be used to derive the response to the SIP INVITE request in accordance with Table 1.

8.3.4. Receipt of QSIG ALERTING Message

The gateway SHALL map a QSIG ALERTING message to a SIP 180 (Ringing) response to the INVITE request. If the SIP INVITE request contained either a Require header or a Supported header with option tag 100rel, the gateway SHALL include in the SIP 180 response a Require header with option tag 100rel.

NOTE: In accordance with [11], inclusion of option tag 100rel in a provisional response instructs the UAC to acknowledge the provisional response by sending a PRACK request. [11] also specifies procedures for repeating a provisional response with option tag 100rel if no PRACK is received.

If the QSIG ALERTING message contained a Progress indicator information element with Progress description number 1 or 8, the gateway SHALL connect the media streams to the corresponding user information channel of the inter-PINX link if it has not already done so, provided that SDP answer information is included in the transmitted SIP response or has already been sent or received. Inclusion of SDP offer or answer information in the 180 provisional response SHALL be in accordance with Section 8.3.5.

8.3.5. Inclusion of SDP Information in a SIP 18x Provisional Response

When sending a SIP 18x provisional response to the INVITE request, if a QSIG message containing a Progress indicator information element with progress description number 1 or 8 has been received the gateway SHALL include SDP information. Otherwise, the gateway MAY include SDP information. If SDP information is included, it shall be in accordance with the following rules.

If the SIP INVITE request contained a Required or Supported header with option tag 100rel, and if SDP offer and answer information has already been exchanged, no SDP information SHALL be included in the SIP 18x provisional response.

If the SIP INVITE request contained a Required or Supported header with option tag 100rel, and if SDP offer information was received in the SIP INVITE request but no SDP answer information has been sent, SDP answer information SHALL be included in the SIP 18x provisional response.

If the SIP INVITE request contained a Required or Supported header with option tag 100rel, and if no SDP offer information was received in the SIP INVITE request and no SDP offer information has already been sent, SDP offer information SHALL be included in the SIP 18x provisional response.

NOTE: In this case, SDP answer information can be expected in the SIP PRACK.

If the SIP INVITE request contained neither a Required nor a Supported header with option tag 100rel, SDP answer information SHALL be included in the SIP 18x provisional response.

NOTE: Because the provisional response is unreliable, SDP answer information needs to be repeated in each provisional response and in the final SIP 2xx response.

NOTE: If the SIP INVITE request contained no SDP offer information and neither a Required nor a Supported header with option tag 100rel, it should have been rejected in accordance with Section 8.3.1.

8.3.6. Receipt of QSIG CONNECT Message

The gateway SHALL map a QSIG CONNECT message to a SIP 200 (OK) final response for the SIP INVITE request. The gateway SHALL also send a QSIG CONNECT ACKNOWLEDGE message.

If the SIP INVITE request contained a Required or Supported header with option tag 100rel, and if SDP offer and answer information has already been exchanged, no SDP information SHALL be included in the SIP 200 response.

If the SIP INVITE request contained a Required or Supported header with option tag 100rel, and if SDP offer information was received in the SIP INVITE request but no SDP answer information has been sent, SDP answer information SHALL be included in the SIP 200 response.

If the SIP INVITE request contained a Required or Supported header with option tag 100rel, and if no SDP offer information was received in the SIP INVITE request and no SDP offer information has already been sent, SDP offer information SHALL be included in the SIP 200 response.

NOTE: In this case, SDP answer information can be expected in the SIP ACK.

If the SIP INVITE request contained neither a Required nor a Supported header with option tag 100rel, SDP answer information SHALL be included in the SIP 200 response.

NOTE: Because the provisional response is unreliable, SDP answer information needs to be repeated in each provisional response and in the final 2xx response.

NOTE: If the SIP INVITE request contained no SDP offer information and neither a Required nor a Supported header with option tag 100rel, it may have been rejected in accordance with Section 8.3.1.

The gateway SHALL connect the media streams to the corresponding user information channel of the inter-PINX link if it has not already done so, provided that SDP answer information is included in the transmitted SIP response or has already been sent or received.

8.3.7. Receipt of SIP PRACK Request

The receipt of a SIP PRACK request acknowledging a reliable provisional response SHALL NOT result in any QSIG message being sent. The gateway SHALL send back a SIP 200 (OK) response to the SIP PRACK request.

If the SIP PRACK contains SDP answer information and a QSIG message containing a Progress indicator information element with progress description number 1 or 8 has been received, the gateway SHALL connect the media streams to the corresponding user information channel of the inter-PINX link.

8.3.8. Receipt of SIP ACK Request

The receipt of a SIP ACK request SHALL NOT result in any QSIG message being sent.

If the SIP ACK contains SDP answer information, the gateway SHALL connect the media streams to the corresponding user information channel of the inter-PINX link if it has not already done so.

8.3.9. Receipt of a SIP INVITE Request for a Call Already Being Established

A gateway can receive a call from SIP using overlap procedures. This should occur when the UAC for the INVITE request is a gateway from a network that employs overlap procedures (e.g., an ISUP gateway or another QSIG gateway) and the gateway has not absorbed overlap.

For a call from SIP using overlap procedures, the gateway will receive multiple SIP INVITE requests that belong to the same call but have different Request-URI and To fields. Each SIP INVITE request belongs to a different dialog.

A SIP INVITE request is considered to be for the purpose of overlap sending if, compared to a previously received SIP INVITE request, it has:

- the same Call-ID header;
- the same From header (including the tag);
- no tag in the To header;

- an updated Request-URI from which can be derived a called party number with a superset of the digits derived from the previously received SIP INVITE request;

and if

- the gateway has not yet sent a final response other than 484 to the previously received SIP INVITE request.

If a gateway receives a SIP INVITE request for the purpose of overlap sending, it SHALL generate a QSIG INFORMATION message using the call reference of the existing QSIG call instead of a new QSIG SETUP message and containing only the additional digits in the Called party number information element. It SHALL also respond to the SIP INVITE request received previously with a SIP 484 Address Incomplete response.

If a gateway receives a SIP INVITE request that meets all of the conditions for a SIP INVITE request for the purpose of overlap sending except the condition concerning the Request-URI, the gateway SHALL respond to the new request with a SIP 485 (Ambiguous) response.

8.4. Call Clearing and Call Failure

8.4.1. Receipt of a QSIG DISCONNECT, RELEASE, or RELEASE COMPLETE Message

On receipt of QSIG DISCONNECT, RELEASE, or RELEASE COMPLETE message as the first QSIG call clearing message, gateway behaviour SHALL depend on the state of call establishment.

1) If the gateway has sent a SIP 200 (OK) response to a SIP INVITE request and received a SIP ACK request, or if it has received a SIP 200 (OK) response to a SIP INVITE request and sent a SIP ACK request, the gateway SHALL send a SIP BYE request to clear the call.

2) If the gateway has sent a SIP 200 (OK) response to a SIP INVITE request (indicating that call establishment is complete) but has not received a SIP ACK request, the gateway SHALL wait until a SIP ACK is received and then send a SIP BYE request to clear the call.

3) If the gateway has sent a SIP INVITE request and received a SIP provisional response but not a SIP final response, the gateway SHALL send a SIP CANCEL request to clear the call.

NOTE 1: In accordance with [10], if after sending a SIP CANCEL request a SIP 2xx response is received to the SIP INVITE request, the gateway will need to send a SIP BYE request.

4) If the gateway has sent a SIP INVITE request but received no SIP response, the gateway SHALL NOT send a SIP message. If a SIP final or provisional response is subsequently received, the gateway SHALL then act in accordance with 1, 2, or 3 above, respectively.

5) If the gateway has received a SIP INVITE request but not sent a SIP final response, the gateway SHALL send a SIP final response chosen according to the cause value in the received QSIG message as specified in Table 1. SIP response 500 (Server internal error) SHALL be used as the default for cause values not shown in Table 1.

NOTE 2: It is not necessarily appropriate to map some QSIG cause values to SIP messages because these cause values are meaningful only at the gateway. A good example of this is cause value 44, "Requested circuit or channel not available", which signifies that the channel number in the transmitted QSIG SETUP message was not acceptable to the peer PINX. The appropriate behavior in this case is for the gateway to send another SETUP message indicating a different channel number. If this is not possible, the gateway should treat it either as a congestion situation (no channels available; see Section 8.3.1) or as a gateway failure situation (in which case the default SIP response code applies).

In all cases, the gateway SHALL also disconnect media streams, if established, and allow QSIG and SIP signalling to complete in accordance with [2] and [10], respectively.

Table 1: Mapping of QSIG Cause Value to SIP 4xx-6xx responses to an INVITE request

QSIG Cause value	SIP response
1 Unallocated number	404 Not found
2 No route to specified transit network	404 Not found
3 No route to destination	404 Not found
16 Normal call clearing	(NOTE 3)
17 User busy	486 Busy here
18 No user responding	408 Request timeout
19 No answer from the user	480 Temporarily unavailable
20 Subscriber absent	480 Temporarily unavailable
21 Call rejected	603 Decline, if location field in Cause information element indicates user. Otherwise: 403 Forbidden
22 Number changed	301 Moved permanently, if information in diagnostic field of Cause information element is suitable for generating a SIP Contact header. Otherwise: 410 Gone
23 Redirection to new destination	410 Gone
27 Destination out of order	502 Bad gateway
28 Address incomplete	484 Address incomplete
29 Facility rejected	501 Not implemented
31 Normal, unspecified	480 Temporarily unavailable
34 No circuit/channel available	503 Service unavailable
38 Network out of order	503 Service unavailable
41 Temporary failure	503 Service unavailable
42 Switching equipment congestion	503 Service unavailable
47 Resource unavailable, unspecified	503 Service unavailable
55 Incoming calls barred within CUG	403 Forbidden
57 Bearer capability not authorized	403 Forbidden
58 Bearer capability not presently available	503 Service unavailable
65 Bearer capability not implemented	488 Not acceptable here (NOTE 4)
69 Requested facility not implemented	501 Not implemented

70 Only restricted digital information available	488 Not acceptable here (NOTE 4)
79 Service or option not implemented, unspecified	501 Not implemented
87 User not member of CUG	403 Forbidden
88 Incompatible destination	503 Service unavailable
102 Recovery on timer expiry	504 Server time-out

NOTE 3: A QSIG call clearing message containing cause value 16 will normally result in the sending of a SIP BYE or CANCEL request. However, if a SIP response is to be sent to the INVITE request, the default response code should be used.

NOTE 4: The gateway may include a SIP Warning header if diagnostic information in the QSIG Cause information element allows a suitable warning code to be selected.

8.4.2. Receipt of a SIP BYE Request

On receipt of a SIP BYE request, the gateway SHALL send a QSIG DISCONNECT message with cause value 16 (normal call clearing). The gateway SHALL also disconnect media streams, if established, and allow QSIG and SIP signalling to complete in accordance with [2] and [10], respectively.

NOTE: When responding to a SIP BYE request, in accordance with [10], the gateway is also required to respond to any other outstanding transactions, e.g., with a SIP 487 (Request Terminated) response. This applies in particular if the gateway has not yet returned a final response to the SIP INVITE request.

8.4.3. Receipt of a SIP CANCEL Request

On receipt of a SIP CANCEL request to clear a call for which the gateway has not sent a SIP final response to the received SIP INVITE request, the gateway SHALL send a QSIG DISCONNECT message with cause value 16 (normal call clearing). The gateway SHALL also disconnect media streams, if established, and allow QSIG and SIP signalling to complete in accordance with [2] and [10], respectively.

8.4.4. Receipt of a SIP 4xx-6xx Response to an INVITE Request

Except where otherwise specified in the context of overlap sending (8.2.2.2), on receipt of a SIP final response (4xx-6xx) to a SIP INVITE request, unless the gateway is able to retry the INVITE request to avoid the problem (e.g., by supplying authentication in the case of a 401 or 407 response), the gateway SHALL transmit a QSIG DISCONNECT message. The cause value in the QSIG DISCONNECT message

SHALL be derived from the SIP 4xx-6xx response according to Table 2. Cause value 31 (Normal, unspecified) SHALL be used as the default for SIP responses not shown in Table 2. The gateway SHALL also disconnect media streams, if established, and allow QSIG and SIP signalling to complete in accordance with [2] and [10], respectively.

When generating a QSIG Cause information element, the location field SHOULD contain the value "user", if generated as a result of a SIP response code 6xx, or the value "Private network serving the remote user" in other circumstances.

Table 2: Mapping of SIP 4xx-6xx responses to an INVITE request to QSIG Cause values

SIP response	QSIG Cause value (NOTE 6)	
400 Bad request	41	Temporary failure
401 Unauthorized	21	Call rejected (NOTE 5)
402 Payment required	21	Call rejected
403 Forbidden	21	Call rejected
404 Not found	1	Unallocated number
405 Method not allowed	63	Service or option unavailable, unspecified
406 Not acceptable	79	Service or option not implemented, unspecified
407 Proxy Authentication required	21	Call rejected (NOTE 5)
408 Request timeout	102	Recovery on timer expiry
410 Gone	22	Number changed
413 Request entity too large	127	Interworking, unspecified (NOTE 6)
414 Request-URI too long	127	Interworking, unspecified (NOTE 6)
415 Unsupported media type	79	Service or option not implemented, unspecified (NOTE 6)
416 Unsupported URI scheme	127	Interworking, unspecified (NOTE 6)
420 Bad extension	127	Interworking, unspecified (NOTE 6)
421 Extension required	127	Interworking, unspecified (NOTE 6)
423 Interval too brief	127	Interworking, unspecified (NOTE 6)
480 Temporarily unavailable	18	No user responding
481 Call/transaction does not exist	41	Temporary failure
482 Loop detected	25	Exchange routing error
483 Too many hops	25	Exchange routing error

484 Address incomplete	28 Invalid number format (NOTE 6)
485 Ambiguous	1 Unallocated Number
486 Busy here	17 User busy
487 Request terminated	(NOTE 7)
488 Not Acceptable Here	65 Bearer capability not implemented or 31 Normal, unspecified (NOTE 8)
500 Server internal error	41 Temporary failure
501 Not implemented	79 Service or option not implemented, unspecified
502 Bad gateway	38 Network out of order
503 Service unavailable	41 Temporary failure
504 Gateway time-out	102 Recovery on timer expiry
505 Version not supported	127 Interworking, unspecified (NOTE 6)
513 Message too large	127 Interworking, unspecified (NOTE 6)
600 Busy everywhere	17 User busy
603 Decline	21 Call rejected
604 Does not exist anywhere	1 Unallocated number
606 Not acceptable	65 Bearer capability not implemented or 31 Normal, unspecified (NOTE 8)

NOTE 5: In some cases, it may be possible for the gateway to provide credentials to the SIP UAS that is rejecting an INVITE due to authorization failure. If the gateway can authenticate itself, then obviously it should do so and proceed with the call. Only if the gateway cannot authorize itself should the gateway clear the call in the QSIG network with this cause value.

NOTE 6: For some response codes, the gateway may be able to retry the INVITE request in order to work around the problem. In particular, this may be the case with response codes indicating a protocol error. The gateway SHOULD clear the call in the QSIG network with the indicated cause value only if retry is not possible or fails.

NOTE 7: The circumstances in which SIP response code 487 can be expected to arise do not require it to be mapped to a QSIG cause code, since the QSIG call will normally already be cleared or in the process of clearing. If QSIG call clearing does, however, need to be initiated, the default cause value should be used.

NOTE 8: When the Warning header is present in a SIP 606 or 488 message, the warning code should be examined to determine whether it is reasonable to generate cause value 65. This cause value should be generated only if there is a chance that a new call attempt with different content in the Bearer capability information element will avoid the problem. In other circumstances, the default cause value should be used.

8.4.5 Gateway-Initiated Call Clearing

If the gateway initiates clearing of the QSIG call owing to QSIG timer expiry, QSIG protocol error, or use of the QSIG RESTART message in accordance with [2], the gateway SHALL also initiate clearing of the SIP call in accordance with Section 8.4.1. If this involves the sending of a final response to a SIP INVITE request, the gateway SHALL use response code 480 (Temporarily Unavailable) if optional QSIG timer T301 has expired or, otherwise, response code 408 (Request timeout) or 500 (Server internal error), as appropriate.

If the gateway initiates clearing of the SIP call owing to SIP timer expiry or SIP protocol error in accordance with [10], the gateway SHALL also initiate clearing of the QSIG call in accordance with [2] using cause value 102 (Recovery on timer expiry) or 41 (Temporary failure), as appropriate.

8.5. Request to Change Media Characteristics

If after a call has been successfully established the gateway receives a SIP INVITE request to change the media characteristics of the call in a way that would be incompatible with the bearer capability in use within the PISN, the gateway SHALL send back a SIP 488 (Not Acceptable Here) response and SHALL NOT change the media characteristics of the existing call.

9. Number Mapping

In QSIG, users are identified by numbers, as defined in [1]. Numbers are conveyed within the Called party number, Calling party number, and Connected number information elements. The Calling party number and Connected number information elements also contain a presentation indicator, which can indicate that privacy is required (presentation restricted), and a screening indicator, which indicates the source and authentication status of the number.

In SIP, users are identified by Universal Resource Identifiers (URIs) conveyed within the Request-URI and various headers, including the From and To headers specified in [10] and optionally the P-Asserted-Identity header specified in [14]. In addition, privacy is indicated by the Privacy header specified in [13].

This clause specifies the mapping between QSIG Called party number, Calling party number, and Connected number information elements and corresponding elements in SIP.

A gateway MAY implement the P-Asserted-Identity header in accordance with [14]. If a gateway implements the P-Asserted-Identity header, it SHALL also implement the Privacy header in accordance with [13]. If a gateway does not implement the P-Asserted-Identity header, it MAY implement the Privacy header.

9.1. Mapping from QSIG to SIP

The method used to convert a number to a URI is outside the scope of this specification. However, the gateway SHOULD take account of the Numbering Plan (NPI) and Type Of Number (TON) fields in the QSIG information element concerned when interpreting a number.

Some aspects of mapping depend on whether the gateway is in the same trust domain (as defined in [14]) as the next hop SIP node (i.e., the proxy or UA to which the INVITE request is sent or from which INVITE request is received) to honour requests for identity privacy in the Privacy header. This will be network-dependent, and it is RECOMMENDED that gateways supporting the P-Asserted-Identity header hold a configurable list of next hop nodes that are to be trusted in this respect.

9.1.1. Using Information from the QSIG Called Party Number Information Element

When mapping a QSIG SETUP message to a SIP INVITE request, the gateway SHALL convert the number in the QSIG Called party number information to a URI and include that URI in the SIP Request-URI and in the To header.

9.1.2. Using Information from the QSIG Calling Party Number Information Element

When mapping a QSIG SETUP message to a SIP INVITE request, the gateway SHALL use the Calling party number information element, if present, as follows.

If the information element contains a number, the gateway SHALL attempt to derive a URI from that number. Further behaviour depends on whether a URI has been derived and the value of the presentation indication.

9.1.2.1. No URI derived, and presentation indicator does not have value "presentation restricted"

In this case (including the case where the Calling party number information element is absent), the gateway SHALL include a URI identifying the gateway in the From header. Also, if the gateway supports the mechanism defined in [14], the gateway SHALL NOT generate a P-Asserted-Identity header.

9.1.2.2. No URI derived, and presentation indicator has value "presentation restricted"

In this case, the gateway SHALL generate an anonymous From header. Also, if the gateway supports the mechanism defined in [14], the gateway SHALL generate a Privacy header field with parameter priv-value = "id" and SHALL NOT generate a P-Asserted-Identity header. The inclusion of additional values of the priv-value parameter in the Privacy header is outside the scope of this specification.

9.1.2.3. URI derived, and presentation indicator has value "presentation restricted"

If the gateway supports the P-Asserted-Identity header and trusts the next hop proxy to honour the Privacy header, the gateway SHALL generate a P-Asserted-Identity header containing the derived URI, SHALL generate a Privacy header with parameter priv-value = "id", and SHALL generate an anonymous From header. The inclusion of additional values of the priv-value parameter in the Privacy header is outside the scope of this specification.

If the gateway does not support the P-Asserted-Identity header or does not trust the proxy to honour the Privacy header, the gateway SHALL behave as in Section 9.1.2.2.

9.1.2.4. URI derived, and presentation indicator does not have value "presentation restricted"

In this case, the gateway SHALL generate a P-Asserted-Identity header containing the derived URI if the gateway supports this header, SHALL NOT generate a Privacy header, and SHALL include the derived URI in the From header. In addition, the gateway MAY use S/MIME, as described in Section 23 of [10], to sign a copy of the From header included in a message/sipfrag body of the INVITE request as described in [20].

9.1.3. Using Information from the QSIG Connected Number Information Element

When mapping a QSIG CONNECT message to a SIP 200 (OK) response to an INVITE request, the gateway SHALL use the Connected number information element, if present, as follows.

If the information element contains a number, the gateway SHALL attempt to derive a URI from that number. Further behaviour depends on whether a URI has been derived and the value of the presentation indication.

9.1.3.1. No URI derived, and presentation indicator does not have value "presentation restricted"

In this case (including the case where the Connected number information element is absent), the gateway SHALL NOT generate a P-Asserted-Identity header and SHALL NOT generate a Privacy header.

9.1.3.2. No URI derived, and presentation indicator has value "presentation restricted"

In this case, if the gateway supports the mechanism defined in [14], the gateway SHALL generate a Privacy header field with parameter priv-value = "id" and SHALL NOT generate a P-Asserted-Identity header. The inclusion of additional values of the priv-value parameter in the Privacy header is outside the scope of this specification.

9.1.3.3. URI derived, and presentation indicator has value "presentation restricted"

If the gateway supports the P-Asserted-Identity header and trusts the next hop proxy to honour the Privacy header, the gateway SHALL generate a P-Asserted-Identity header containing the derived URI and SHALL generate a Privacy header with parameter priv-value = "id". The inclusion of additional values of the priv-value parameter in the Privacy header is outside the scope of this specification.

If the gateway does not support the P-Asserted-Identity header or does not trust the proxy to honour the Privacy header, the gateway SHALL behave as in Section 9.1.3.2.

9.1.3.4. URI derived, and presentation indicator does not have value "presentation restricted"

In this case, the gateway SHALL generate a P-Asserted-Identity header containing the derived URI if the gateway supports this header and SHALL NOT generate a Privacy header. In addition, the gateway MAY use S/MIME, as described in Section 23 of [10], to sign a To header containing the derived URI, the To header being included in a message/sipfrag body of the INVITE response as described in [20].

NOTE: The To header in the message/sipfrag body may differ from the to header in the response's headers.

9.2. Mapping from SIP to QSIG

The method used to convert a URI to a number is outside the scope of this specification. However, NPI and TON fields in the QSIG information element concerned SHALL be set to appropriate values in accordance with [1].

Some aspects of mapping depend on whether the gateway trusts the next hop SIP node (i.e., the proxy or UA to which the INVITE request is sent or from which INVITE request is received) to provide accurate information in the P-Asserted-Identity header. This will be network-dependent, and it is RECOMMENDED that gateways hold a configurable list of next hop nodes that are to be trusted in this respect.

Some aspects of mapping depend on whether the gateway is prepared to use a URI in the From header to derive a number for the Calling party number information element. The default behaviour SHOULD be not to use an unsigned or unvalidated From header for this purpose, since in principle the information comes from an untrusted source (the remote UA). However, it is recognised that some network administrations may believe that the benefits to be derived from supplying a calling party number outweigh any risks of supplying false information. Therefore, a gateway MAY be configurable to use an unsigned or unvalidated From header for this purpose.

9.2.1. Generating the QSIG Called Party Number Information Element

When mapping a SIP INVITE request to a QSIG SETUP message, the gateway SHALL convert the URI in the SIP Request-URI to a number and include that number in the QSIG Called party number information element.

NOTE: The To header should not be used for this purpose. This is because re-targeting of the request in the SIP network can change the Request-URI but leave the To header unchanged. It is important that routing in the QSIG network be based on the final target from the SIP network.

9.2.2. Generating the QSIG Calling Party Number Information Element

When mapping a SIP INVITE request to a QSIG SETUP message, the gateway SHALL generate a Calling party number information element as follows.

If the SIP INVITE request contains an S/MIME signed message/sipfrag body [20] containing a From header, and if the gateway supports this capability and can verify the authenticity and trustworthiness of this information, the gateway SHALL attempt to derive a number from the URI in that header. If no number is derived from a message/sipfrag body, if the SIP INVITE request contains a P-Asserted-Identity header, and if the gateway supports that header and trusts the information therein, the gateway SHALL attempt to derive a number from the URI in that header. If a number is derived from one of these headers, the gateway SHALL include it in the Calling party number information element and include value "network provided" in the screening indicator.

If no number is derivable as described above and if the gateway is prepared to use the unsigned or unvalidated From header, the gateway SHALL attempt to derive a number from the URI in the From header. If a number is derived from the From header, the gateway SHALL include it in the Calling party number information element and include value "user provided, not screened" in the screening indicator.

If no number is derivable, the gateway SHALL NOT include a number in the Calling party number information element.

If the SIP INVITE request contains a Privacy header with value "id" in parameter priv-value and the gateway supports this header, or if the value in the From header indicates anonymous, the gateway SHALL include value "presentation restricted" in the presentation indicator. Based on local policy, the gateway MAY use the presence of other priv-values to set the presentation indicator to "presentation restricted". Otherwise the gateway SHALL include value "presentation allowed" if a number is present or "not available due to interworking" if no number is present.

If the resulting Calling party number information element contains no number and contains value "not available due to interworking" in the presentation indicator, the gateway MAY omit the information element from the QSIG SETUP message.

9.2.3. Generating the QSIG Connected Number Information Element

When mapping a SIP 2xx response to an INVITE request to a QSIG CONNECT message, the gateway SHALL generate a Connected number information element as follows.

If the SIP 2xx response contains an S/MIME signed message/sipfrag [20] body containing a To header and the gateway supports this capability and can verify the authenticity and trustworthiness of this information, the gateway SHALL attempt to derive a number from the URI in that header. If no number is derived from a message/sipfrag body, if the SIP 2xx response contains a P-Asserted-Identity header, and if the gateway supports that header and trusts the information therein, the gateway SHALL attempt to derive a number from the URI in that header. If a number is derived from one of these headers, the gateway SHALL include it in the Connected number information element and include value "network provided" in the screening indicator.

If no number is derivable as described above, the gateway SHOULD NOT include a number in the Connected number information element.

If the SIP 2xx response contains a Privacy header with value "id" in parameter priv-value and the gateway supports this header, the gateway SHALL include value "presentation restricted" in the presentation indicator. Based on local policy, the gateway MAY use the presence of other priv-values to set the presentation indicator to "presentation restricted". Otherwise, the gateway SHALL include value "presentation allowed" if a number is present or "not available due to interworking" if no number is present.

If the resulting Connected number information element contains no number and value "not available due to interworking" in the presentation indicator, the gateway MAY omit the information element from the QSIG CONNECT message.

10. Requirements for Support of Basic Services

This document specifies signalling interworking for basic services that provide a bi-directional transfer capability for speech, facsimile, and modem media between the two networks.

10.1. Derivation of QSIG Bearer Capability Information Element

The gateway SHALL generate the Bearer Capability Information Element in the QSIG SETUP message based on SDP offer information received along with the SIP INVITE request. If the SIP INVITE request does not contain SDP offer information or the media type in the SDP offer information is only 'audio', then the Bearer capability information element SHALL BE generated according to Table 3. Coding of the Bearer capability information element for other media types is outside the scope of this specification.

In addition, the gateway MAY include a Low layer compatibility information element and/or High layer compatibility information in the QSIG SETUP message if the gateway is able to derive relevant information from the SDP offer information. Specific mappings are outside the scope of this specification.

Table 3: Bearer capability encoding for 'audio' transfer

Field	Value
Coding Standard	"CCITT standardized coding" (00)
Information transfer capability	"3,1 kHz audio" (10000)
Transfer mode	"circuit mode" (00)
Information transfer rate	"64 Kbits/s" (10000)
Multiplier	Octet omitted
User information layer 1 protocol	Generated by gateway based on Information of the PISN. Supported values are "CCITT recommendation G.711 mu-law" (00010) "CCITT recommendation G.711 A-law" (00011)

10.2. Derivation of Media Type in SDP

The gateway SHALL generate SDP offer information to include in the SIP INVITE request based on information in the QSIG SETUP message. The gateway MAY take account of QSIG Low layer compatibility and/or High layer compatibility information elements, if present in the QSIG SETUP message, when deriving SDP offer information, in which case specific mappings are outside the scope of this specification. Otherwise, the gateway shall generate SDP offer information based only on the Bearer capability information element in the QSIG SETUP message, in which case the media type SHALL be derived according to Table 4.

Table 4: Media type setting in SDP based on Bearer capability information element

Information transfer capability in Bearer capability information element	Media type in SDP
"speech" (00000)	audio
"3,1 kHz audio" (10000)	audio

11. Security Considerations

11.1. General

Normal considerations apply for UA use of SIP security measures, including digest authentication, TLS, and S/MIME as described in [10].

The translation of QSIG information elements into SIP headers can introduce some privacy and security concerns. For example, care needs to be taken to provide adequate privacy for a user requesting presentation restriction if the Calling party number information element is openly mapped to the From header. Procedures for dealing with this particular situation are specified in Section 9.1.2. However, since the mapping specified in this document is mainly concerned with translating information elements into the headers and fields used to route SIP requests, gateways consequently reveal (through this translation process) the minimum possible amount of information.

There are some concerns, however, that arise from the other direction of mapping, the mapping of SIP headers to QSIG information elements, which are enumerated in the following paragraphs.

11.2. Calls from QSIG to Invalid or Restricted Numbers

When end users dial numbers in a PISN, their selections populate the Called party number information element in the QSIG SETUP message. Similarly, the SIP URI or tel URL and its optional parameters in the Request-URI of a SIP INVITE request, which can be created directly by end users of a SIP device, map to that information element at a gateway. However, in a PISN, policy can prevent the user from dialing certain (invalid or restricted) numbers. Thus, gateway implementers may wish to provide a means for gateway administrators to apply policies restricting the use of certain SIP URIs or tel URLs, or SIP URI or tel URL parameters, when authorizing a call from SIP to QSIG.

11.3. Abuse of SIP Response Code

Some additional risks may result from the mapping of SIP response codes to QSIG cause values. SIP user agents could conceivably respond to an INVITE request from a gateway with any arbitrary SIP response code, and thus they can dictate (within the boundaries of the mappings supported by the gateway) the Q.850 cause code that will be sent by the gateway in the resulting QSIG call clearing message. Generally speaking, the manner in which a call is rejected is unlikely to provide any avenue for fraud or denial of service (e.g., by signalling that a call should not be billed, or that the network should take critical resources off-line). However, gateway implementers may wish to make provision for gateway administrators to modify the response code to cause value mappings to avoid any undesirable network-specific behaviour resulting from the mappings recommended in Section 8.4.4.

11.4. Use of the To Header URI

This specification requires the gateway to map the Request-URI rather than the To header in a SIP INVITE request to the Called party number information element in a QSIG SETUP message. Although a SIP UA is expected to put the same URI in the To header and in the Request-URI, this is not policed by other SIP entities. Therefore, a To header URI that differs from the Request-URI received at the gateway cannot be used as a reliable indication that the call has been re-targeted in the SIP network or as a reliable indication of the original target. Gateway implementers making use of the To header for mapping to QSIG elements (e.g., as part of QSIG call diversion signalling) may wish to make provision for disabling this mapping when deployed in situations where the reliability of the QSIG elements concerned is important.

11.5. Use of the From Header URI

The arbitrary population of the From header of requests by SIP user agents has some well-understood security implications for devices that rely on the From header as an accurate representation of the identity of the originator. Any gateway that intends to use an unsigned or unverified From header to populate the Calling party number information element of a QSIG SETUP message should authenticate the originator of the request and make sure that it is authorized to assert that calling number (or make use of some more secure method to ascertain the identity of the caller). Note that gateways, like all other SIP user agents, MUST support Digest authentication as described in [10]. Similar considerations apply to the use of the SIP P-Asserted-Identity header for mapping to the QSIG Calling party number or Connected number information element, i.e., the source of this information should be authenticated. Use of a signed message/sipfrag body to derive a QSIG Calling party number or Connected number information element is another secure alternative.

11.6. Abuse of Early Media

There is another class of potential risk that is related to the cut-through of the backwards media path before the call is answered. Several practices described in this document involve the connection of media streams to user information channels on inter-PINX links and the sending of progress description number 1 or 8 in a backward QSIG message. This can result in media being cut through end-to-end, and it is possible for the called user agent then to play arbitrary audio to the caller for an indefinite period of time before transmitting a final response (in the form of a 2xx or higher response code) to an INVITE request. This is useful since it also permits network entities (particularly legacy networks that are incapable of transmitting Q.850 cause values) to play tones and announcements to indicate call failure or call progress, without triggering charging by transmitting a 2xx response. Also, early cut-through can help prevent clipping of the initial media when the call is answered. There are conceivable respects in which this capability could be used fraudulently by the called user agent for transmitting arbitrary information without answering the call or before answering the call. However, in corporate networks, charging is often not an issue, and for calls arriving at a corporate network from a carrier network, the carrier network normally takes steps to prevent fraud.

The usefulness of this capability appears to outweigh any risks involved, which may in practice be no greater than in existing PISN/ISDN environments. However, gateway implementers may wish to make provision for gateway administrators to turn off cut-through or minimise its impact (e.g., by imposing a time limit) when deployed in situations where problems can arise.

11.7. Protection from Denial-of-Service Attacks

Unlike a traditional PISN phone, a SIP user agent can launch multiple simultaneous requests in order to reach a particular resource. It would be trivial for a SIP user agent to launch 100 SIP INVITE requests at a 100 port gateway, thereby tying up all of its ports. A malicious user could choose to launch requests to telephone numbers that are known never to answer, or, where overlap signalling is used, to incomplete addresses. This could saturate resources at the gateway indefinitely, potentially without incurring any charges. Gateway implementers may therefore wish to provide means of restricting according to policy the number of simultaneous requests originating from the same authenticated source, or similar mechanisms to address this possible denial-of-service attack.

12. Acknowledgements

This document is a product of the authors' activities in Ecma (www.ecma-international.org) on interoperability of QSIG with IP networks. An earlier version is published as Standard ECMA-339. Ecma has made this work available to the IETF as the basis for publishing an RFC.

The authors wish to acknowledge the assistance of Francois Audet, Adam Roach, Jean-Francois Rey, Thomas Stach, and members of Ecma TC32-TG17 in preparing and commenting on this document.

13. Normative References

[1] International Standard ISO/IEC 11571 "Private Integrated Services Networks (PISN) - Addressing" (also published by Ecma as Standard ECMA-155).

[2] International Standard ISO/IEC 11572 "Private Integrated Services Network - Circuit-mode Bearer Services - Inter-Exchange Signalling Procedures and Protocol" (also published by Ecma as Standard ECMA-143).

[3] International Standard ISO/IEC 11582 "Private Integrated Services Network - Generic Functional Protocol for the Support of Supplementary Services - Inter-Exchange Signalling Procedures and Protocol" (also published by Ecma as Standard ECMA-165).

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[5] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[6] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[7] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[8] Handley, M. and V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998.

[9] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L., and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, October 2000.

[10] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[11] Rosenberg, J. and H. Schulzrinne, "Reliability of Provisional Responses in Session Initiation Protocol (SIP)", RFC 3262, June 2002.

[12] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

[13] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, November 2002.

[14] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.

[15] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[16] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[17] ITU-T Recommendation E.164, "The International Public Telecommunication Numbering Plan", (1997-05).

[18] Camarillo, G., Roach, A., Peterson, J., and L. Ong, "Mapping of Integrated Services Digital Network (ISDN) User Part (ISUP) Overlap Signalling to the Session Initiation Protocol (SIP)", RFC 3578, August 2003.

[19] Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, October 2002.

[20] Sparks, R., "Internet Media Type message/sipfrag", RFC 3420, November 2002.

Appendix A. Example Message Sequences

A.1. Introduction

This appendix shows some typical message sequences that can occur for an interworking between QSIG and SIP. It is informative.

NOTE: For all message sequence diagrams, there is no message mapping between QSIG and SIP unless explicitly indicated by dotted lines. Also, if there are no dotted lines connecting two messages, this means that these are independent of each other in terms of the time when they occur.

NOTE: Numbers prefixing SIP method names and response codes in the diagrams represent sequence numbers. Messages bearing the same number will have the same value in the CSeq header.

NOTE: In these examples, SIP provisional responses (other than 100) are shown as being sent reliably, using the PRACK method for acknowledgement.

A.2. Message Sequences for Call Establishment from QSIG to SIP

Below are typical message sequences for successful call establishment from QSIG to SIP

A.2.1. QSIG to SIP, using en bloc procedures on both QSIG and SIP

```
                           +-------------------+
                           |                   |
                           |     GATEWAY       |
        PISN               |                   |        IP NETWORK
        |                  +-----+------+------+                 |
        |                        |      |                        |
        |                        |      |                        |
        |   QSIG SETUP           |      |        1-INVITE        |
       1|----------------------->|......|----------------------->| 2
        |                        |      |                        |
        |                        |      |                        |
        | QSIG CALL PROCEEDING   |      |        1-100 TRYING    |
       3|<-----------------------|      |<-----------------------+ 4
        |                        |      |                        |
        |                        |      |                        |
        |   QSIG ALERTING        |      |        1-180 RINGING   |
       8|<-----------------------|......|<-----------------------+ 5
        |                        |      |                        |
        |                        |      |        2-PRACK         |
        |                        |      |----------------------->| 6
        |                        |      |        2-200 OK        |
        |                        |      |<-----------------------+ 7
        |                        |      |                        |
        |   QSIG CONNECT         |      |        1-200 OK        |
      11|<-----------------------|......|<-----------------------+ 9
        |                        |      |                        |
        |   QSIG CONNECT ACK     |      |        1-ACK           |
      12|----------------------->|      |----------------------->| 10
        |                        |      |                        |
        |<======================>|      |<======================>|
        |        AUDIO           |      |         AUDIO          |
```

Figure 3: Typical message sequence for successful call establishment from QSIG to SIP, using en bloc procedures on both QSIG and SIP

1 The PISN sends a QSIG SETUP message to the gateway to begin a session with a SIP UA.
2 On receipt of the QSIG SETUP message, the gateway generates a SIP INVITE request and sends it to an appropriate SIP entity in the IP network based on the called number.
3 The gateway sends a QSIG CALL PROCEEDING message to the PISN; no more QSIG INFORMATION messages will be accepted.
4 The IP network sends a SIP 100 (Trying) response to the gateway.
5 The IP network sends a SIP 180 (Ringing) response.

6 The gateway may send back a SIP PRACK request to the IP network based on the inclusion of a Require header or a Supported header with option tag 100rel in the initial SIP INVITE request.

7 The IP network sends a SIP 200 (OK) response to the gateway to acknowledge the SIP PRACK request

8 The gateway maps this SIP 180 (Ringing) response to a QSIG ALERTING message and sends it to the PISN.

9 The IP network sends a SIP 200 (OK) response when the call is answered.

10 The gateway sends a SIP ACK request to acknowledge the SIP 200 (OK) response.

11 The gateway maps this SIP 200 (OK) response to a QSIG CONNECT message and sends it to the PISN.

12 The PISN sends a QSIG CONNECT ACKNOWLEDGE message in response to the QSIG CONNECT message.

A.2.2. QSIG to SIP, using overlap receiving on QSIG and en bloc sending on SIP

```
                        +------------------------+
     PISN               |         GATEWAY        |      IP NETWORK
                        |                        |
     |  QSIG SETUP      +--------+-------+-------+                |
    1|-------------------------->|       |                        |
     |                           |       |                        |
     |  QSIG SETUP ACK           |       |                        |
    2|<--------------------------|       |                        |
     |                           |       |                        |
     | QSIG INFORMATION          |       |                        |
    3|-------------------------->|       |                        |
     |                           |       |                        |
     | QSIG INFORMATION          |       |  1-INVITE              |
   3a|-------------------------->|.......|----------------------->|4
     | QSIG CALL PROCEEDING      |       |  1-100 TRYING          |
    5|<--------------------------|       |<-----------------------|6
     |                           |       |                        |
     | QSIG ALERTING             |       |  1-180 RINGING         |
   10|<--------------------------|.......|<-----------------------|7
     |                           |       |  2-PRACK               |
     |                           |       |----------------------->|8
     |                           |       |  2-200 OK              |
     |                           |       |<-----------------------|9
     | QSIG CONNECT              |       |  1-200 OK              |
   13|<--------------------------|.......|<-----------------------|11
     |                           |       |                        |
     | QSIG CONNECT ACK          |       |  1-ACK                 |
   14|-------------------------->|       |----------------------->|12
     |          AUDIO            |       |           AUDIO        |
     |<=========================>|       |<======================>|
```

Figure 4: Typical message sequence for successful call establishment from QSIG to SIP, using overlap receiving on QSIG and en bloc sending on SIP

1 The PISN sends a QSIG SETUP message to the gateway to begin a session with a SIP UA. The QSIG SETUP message does not contain a Sending Complete information element.

2 The gateway sends a QSIG SETUP ACKNOWLEDGE message to the PISN. More digits are expected.

3 More digits are sent from the PISN within a QSIG INFORMATION message.

3a More digits are sent from the PISN within a QSIG INFORMATION message. The QSIG INFORMATION message contains a Sending Complete information element.

4 The Gateway generates a SIP INVITE request and sends it to an appropriate SIP entity in the IP network, based on the called number.
5 The gateway sends a QSIG CALL PROCEEDING message to the PISN; no more QSIG INFORMATION messages will be accepted.
6 The IP network sends a SIP 100 (Trying) response to the gateway.
7 The IP network sends a SIP 180 (Ringing) response.
8 The gateway may send back a SIP PRACK request to the IP network based on the inclusion of a Require header or a Supported header with option tag 100rel in the initial SIP INVITE request.
9 The IP network sends a SIP 200 (OK) response to the gateway to acknowledge the SIP PRACK request.
10 The gateway maps this SIP 180 (Ringing) response to a QSIG ALERTING message and sends it to the PINX.
11 The IP network sends a SIP 200 (OK) response when the call is answered.
12 The gateway sends an SIP ACK request to acknowledge the SIP 200 (OK) response.
13 The gateway maps this SIP 200 (OK) response to a QSIG CONNECT message and sends it to the PINX.
14 The PISN sends a QSIG CONNECT ACKNOWLEDGE message in response to the QSIG CONNECT message.

A.2.3. QSIG to SIP, using overlap procedures on both QSIG and SIP

```
                        +----------------------+
     PISN               |        GATEWAY       |         IP NETWORK
                        |                      |
     |  QSIG SETUP      +-------+-------+------+                   |
   1 |------------------------->|       |                         |
     |                          |       |                         |
     |  QSIG SETUP ACK          |       |                         |
   2 |<-------------------------|       |                         |
     |                          |       |                         |
     | QSIG INFORMATION         |       |                         |
   3 |------------------------->|       |                         |
     | QSIG INFORMATION         |       | 1-INVITE                |
   3 |------------------------->|.......|------------------------>|4
     |                          |       | 1-484                   |
     |                          |       |<------------------------|5
     |                          |       | 1-ACK                   |
     |                          |       |------------------------>|6
     | QSIG INFORMATION         |       | 2-INVITE                |
   7 |------------------------->|.......|------------------------>|4
     |                          |       | 2-484                   |
     |                          |       |<------------------------|5
     |                          |       | 2-ACK                   |
     |                          |       |------------------------>|6
     |                          |       |                         |
     | QSIG INFORMATION         |       |                         |
     | Sending Complete IE      |       | 3-INVITE                |
   8 |------------------------->|.......|------------------------>|10
     | QSIG CALL PROCEEDING     |       | 3-100 TRYING            |
   9 |<-------------------------|       |<------------------------|11
     |                          |       |                         |
     | QSIG ALERTING            |       | 3-180 RINGING           |
  15 |<-------------------------|.......|<------------------------|12
     |                          |       | 4-PRACK                 |
     |                          |       |------------------------>|13
     |                          |       | 4-200 OK                |
     |                          |       |<------------------------|14
     | QSIG CONNECT             |       | 3-200 OK                |
  18 |<-------------------------|.......|<------------------------|16
     |                          |       |                         |
     | QSIG CONNECT ACK         |       | 3-ACK                   |
  19 |------------------------->|       |------------------------>|17
     |         AUDIO            |       |         AUDIO           |
     |<========================>|       |<=======================>|
     |                          |       |                         |
```

Figure 5: Typical message sequence for successful call establishment from QSIG to SIP, using overlap procedures on both QSIG and SIP

1 The PISN sends a QSIG SETUP message to the gateway to begin a session with a SIP UA. The QSIG SETUP message does not contain a Sending complete information element.
2 The gateway sends a QSIG SETUP ACKNOWLEDGE message to the PISN. More digits are expected.
3 More digits are sent from the PISN within a QSIG INFORMATION message.
4 When the gateway receives the minimum number of digits required to route the call, it generates a SIP INVITE request and sends it to an appropriate SIP entity in the IP network based on the called number
5 Due to an insufficient number of digits, the IP network will return a SIP 484 (Address Incomplete) response.
6 The SIP 484 (Address Incomplete) response is acknowledged.
7 More digits are received from the PISN in a QSIG INFORMATION message. A new INVITE is sent with the same Call-ID and From values but an updated Request-URI.
8 More digits are received from the PISN in a QSIG INFORMATION message. The QSIG INFORMATION message contains a Sending Complete information element.
9 The gateway sends a QSIG CALL PROCEEDING message to the PISN; no more information will be accepted.
10 The gateway sends a new SIP INVITE request with an updated Request-URI field.
11 The IP network sends a SIP 100 (Trying) response to the gateway.
12 The IP network sends a SIP 180 (Ringing) response.
13 The gateway may send back a SIP PRACK request to the IP network based on the inclusion of a Require header or a Supported header with option tag 100rel in the initial SIP INVITE request.
14 The IP network sends a SIP 200 (OK) response to the gateway to acknowledge the SIP PRACK request.
15 The gateway maps this SIP 180 (Ringing) response to a QSIG ALERTING message and sends it to the PISN.
16 The IP network sends a SIP 200 (OK) response when the call is answered.
17 The gateway sends a SIP ACK request to acknowledge the SIP 200 (OK) response.
18 The gateway maps this SIP 200 (OK) response to a QSIG CONNECT message.
19 The PISN sends a QSIG CONNECT ACKNOWLEDGE message in response to the QSIG CONNECT message.

A.3. Message sequences for call establishment from SIP to QSIG

Below are typical message sequences for successful call establishment from SIP to QSIG

A.3.1. SIP to QSIG, using en bloc procedures

```
                        +----------------------+
    IP NETWORK          |       GATEWAY        |          PISN
                        |                      |
     |                  +-------+-------+------+             |
     |                          |       |                    |
     |                          |       |                    |
     |                          |       |                    |
     |    1-INVITE              |       | QSIG SETUP         |
   1 |------------------------->|.......|------------------->| 3
     |    1-100 TRYING          |       | QSIG CALL PROCEEDING
   2 |<-------------------------|       |<-------------------| 4
     |    1-180 RINGING         |       | QSIG ALERTING      |
   6 |<-------------------------|.......|<-------------------| 5
     |                          |       |                    |
     |                          |       |                    |
     |    2-PRACK               |       |                    |
   7 |------------------------->|       |                    |
     |    2-200 OK              |       |                    |
   8 |<-------------------------|       |                    |
     |    1-200 OK              |       | QSIG CONNECT       |
  11 |<-------------------------|.......|<-------------------| 9
     |                          |       |                    |
     |    1-ACK                 |       | QSIG CONNECT ACK   |
  12 |------------------------->|       |------------------->| 10
     |        AUDIO             |       |      AUDIO         |
     |<========================>|       |<==================>|
     |                          |       |                    |
```

Figure 6: Typical message sequence for successful call establishment from SIP to QSIG, using en bloc procedures

1 The IP network sends a SIP INVITE request to the gateway.
2 The gateway sends a SIP 100 (Trying) response to the IP network.
3 On receipt of the SIP INVITE request, the gateway sends a QSIG SETUP message.
4 The PISN sends a QSIG CALL PROCEEDING message to the gateway.
5 A QSIG ALERTING message is returned to indicate that the end user in the PISN is being alerted.
6 The gateway maps the QSIG ALERTING message to a SIP 180 (Ringing) response.

7 The IP network can send back a SIP PRACK request to the IP network based on the inclusion of a Require header or a Supported header with option tag 100rel in the initial SIP INVITE request.
8 The gateway sends a SIP 200 (OK) response to acknowledge the SIP PRACK request.
9 The PISN sends a QSIG CONNECT message to the gateway when the call is answered.
10 The gateway sends a QSIG CONNECT ACKNOWLEDGE message to acknowledge the QSIG CONNECT message.
11 The QSIG CONNECT message is mapped to a SIP 200 (OK) response.
12 The IP network, upon receiving a SIP INVITE final response (200), will send a SIP ACK request to acknowledge receipt.

A.3.2. SIP to QSIG, using overlap receiving on SIP and en bloc sending on QSIG

```
                        +----------------------+
     IP NETWORK         |        GATEWAY       |               PISN
                        |                      |
     | 1-INVITE         +-------+-------+------+                  |
   1 |------------------------->|       |                         |
     |     1-484                |       |                         |
   2 |<-------------------------|       |                         |
     |     1-ACK                |       |                         |
   3 |------------------------->|       |                         |
     |     2-INVITE             |       |                         |
   1 |------------------------->|       |                         |
     |     2-484                |       |                         |
   2 |<-------------------------|       |                         |
     |     2- ACK               |       |                         |
   3 |------------------------->|       |                         |
     |     3-INVITE             |       | QSIG SETUP              |
   4 |------------------------->|.......|------------------------>|6
     |     3-100 TRYING         |       | QSIG CALL PROCEEDING    |
   5 |<-------------------------|       |<------------------------|7
     |     3-180 RINGING        |       | QSIG ALERTING           |
   9 |<-------------------------|.......|<------------------------|8
     |                          |       |                         |
     |                          |       |                         |
     |     4-PRACK              |       |                         |
  10 |------------------------->|       |                         |
     |     4-200 OK             |       |                         |
  11 |<-------------------------|       |                         |
     |     3-200 OK             |       | QSIG CONNECT            |
  14 |<-------------------------|.......|<------------------------|12
     |                          |       |                         |
     |     3-ACK                |       | QSIG CONNECT ACK        |
  15 |------------------------->|       |------------------------>|13
     |         AUDIO            |       |         AUDIO           |
     |<========================>|       |<=======================>|
     |                          |       |                         |
```

Figure 7: Typical message sequence for successful call establishment from SIP to QSIG, using overlap receiving on SIP and en bloc sending on QSIG

1 The IP network sends a SIP INVITE request to the gateway.
2 Due to an insufficient number of digits, the gateway returns a SIP 484 (Address Incomplete) response.
3 The IP network acknowledges the SIP 484 (Address Incomplete) response.

4 The IP network sends a new SIP INVITE request with the same Call-ID and updated Request-URI.
5 The gateway now has all the digits required to route the call to the PISN. The gateway sends back a SIP 100 (Trying) response.
6 The gateway sends a QSIG SETUP message.
7 The PISN sends a QSIG CALL PROCEEDING message to the gateway.
8 A QSIG ALERTING message is returned to indicate that the end user in the PISN is being alerted.
9 The gateway maps the QSIG ALERTING message to a SIP 180 (Ringing) response.
10 The IP network can send back a SIP PRACK request to the IP network based on the inclusion of a Require header or a Supported header with option tag 100rel in the initial SIP INVITE request.
11 The gateway sends a SIP 200 (OK) response to acknowledge the SIP PRACK request.
12 The PISN sends a QSIG CONNECT message to the gateway when the call is answered.
13 The gateway sends a QSIG CONNECT ACKNOWLEDGE message to acknowledge the CONNECT message.
14 The QSIG CONNECT message is mapped to a SIP 200 (OK) response.
15 The IP network, upon receiving a SIP INVITE final response (200), will send a SIP ACK request to acknowledge receipt.

A.3.3. SIP to QSIG, using overlap procedures on both SIP and QSIG

```
                        +----------------------+
     IP NETWORK         |        GATEWAY       |               PISN
                        |                      |
     | 1-INVITE         +-------+-------+------+                  |
   1 |------------------------->|       |                         |
     |     1-484                |       |                         |
   2 |<-------------------------|       |                         |
     |     1-ACK                |       |                         |
   3 |------------------------->|       |                         |
     |     2-INVITE             |       | QSIG SETUP              |
   4 |------------------------->|.......|------------------------>| 6
     |     2-100 TRYING         |       | QSIG SETUP ACK          |
   5 |<-------------------------|       |<------------------------| 7
     |     3- INVITE            |       | QSIG INFORMATION        |
   8 |------------------------->|.......|------------------------>| 10
     |     3-100 TRYING         |       |                         |
   9 |<-------------------------|       | QSIG CALL PROCEEDING    |
     |                          |       |<------------------------| 11
   13|     3-180 RINGING        |       | QSIG ALERTING           |
     |<-------------------------|.......|<------------------------| 12
     |     2-484                |       |                         |
   14|<-------------------------|       |                         |
     |     2-ACK                |       |                         |
   15|------------------------->|       |                         |
     |     4-PRACK              |       |                         |
   16|------------------------->|       |                         |
     |     4-200 OK             |       |                         |
   17|<-------------------------|       |                         |
     |     3-200 OK             |       | QSIG CONNECT            |
   20|<-------------------------|.......|<------------------------| 18
     |                          |       |                         |
     |     3-ACK                |       | QSIG CONNECT ACK        |
   21|------------------------->|       |------------------------>| 19
     |         AUDIO            |       |         AUDIO           |
     |<========================>|       |<=======================>|
     |                          |       |                         |
```

Figure 8: Typical message sequence for successful call establishment from SIP to QSIG, using overlap procedures on both SIP and QSIG

1 The IP network sends a SIP INVITE request to the gateway.
2 Due to an insufficient number of digits, the gateway returns a SIP 484 (Address Incomplete) response.
3 The IP network acknowledges the SIP 484 (Address Incomplete) response.

4 The IP network sends a new SIP INVITE request with the same Call-ID and updated Request-URI.
5 The gateway now has all the digits required to route the call to the PISN. The gateway sends back a SIP 100 (Trying) response to the IP network.
6 The gateway sends a QSIG SETUP message.
7 The PISN needs more digits to route the call and sends a QSIG SETUP ACKNOWLEDGE message to the gateway.
8 The IP network sends a new SIP INVITE request with the same Call-ID and From values and updated Request-URI.
9 The gateway sends back a SIP 100 (Trying) response to the IP network.
10 The gateway maps the new SIP INVITE request to a QSIG INFORMATION message.
11 The PISN has all the digits required and sends back a QSIG CALL PROCEEDING message to the gateway.
12 A QSIG ALERTING message is returned to indicate that the end user in the PISN is being alerted.
13 The gateway maps the QSIG ALERTING message to a SIP 180 (Ringing) response.
14 The gateway sends a SIP 484 (Address Incomplete) response for the previous SIP INVITE request.
15 The IP network acknowledges the SIP 484 (Address Incomplete) response.
16 The IP network can send back a SIP PRACK request to the IP network based on the inclusion of a Require header or a Supported header with option tag 100rel in the initial SIP INVITE request.
17 The gateway sends a SIP 200 (OK) response to acknowledge the SIP PRACK request.
18 The PISN sends a QSIG CONNECT message to the gateway when the call is answered.
19 The gateway sends a QSIG CONNECT ACKNOWLEDGE message to acknowledge the QSIG CONNECT message.
20 The QSIG CONNECT message is mapped to a SIP 200 (OK) response.
21 The IP network, upon receiving a SIP INVITE final response (200), will send a SIP ACK request to acknowledge receipt.

A.4. Message Sequence for Call Clearing from QSIG to SIP

Below are typical message sequences for Call Clearing from QSIG to SIP

A.4.1. QSIG to SIP, subsequent to call establishment

```
                         +-------------------+
                         |                   |
                         |      GATEWAY      |
     PISN                |                   |         IP NETWORK
      |                  +-----+------+------+                 |
      |                        |      |                        |
      |                        |      |                        |
      |     QSIG DISCONNECT    |      |   2- BYE               |
    1 |----------------------->|......|----------------------->| 4
      |     QSIG RELEASE       |      |        2-200 OK        |
    2 |<-----------------------|      |<-----------------------| 5
      |     QSIG RELEASE COMP  |      |                        |
    3 |----------------------->|      |                        |
      |                        |      |                        |
      |                        |      |                        |
      |                        |      |                        |
```

Figure 9: Typical message sequence for call clearing from QSIG to SIP, subsequent to call establishment

1 The PISN sends a QSIG DISCONNECT message to the gateway.
2 The gateway sends back a QSIG RELEASE message to the PISN in response to the QSIG DISCONNECT message.
3 The PISN sends a QSIG RELEASE COMPLETE message in response. All PISN resources are now released.
4 The gateway maps the QSIG DISCONNECT message to a SIP BYE request.
5 The IP network sends back a SIP 200 (OK) response to the SIP BYE request. All IP resources are now released.

A.4.2. QSIG to SIP, during establishment of a call from SIP to QSIG

```
                              +-------------------+
                              |                   |
                              |     GATEWAY       |
           PISN               |                   |        IP NETWORK
           |                  +-----+------+------+                 |
           |                        |      |                        |
           |                        |      |                        |
           |     QSIG DISCONNECT    |      |   1- 4XX / 6XX         |
          1|----------------------->|......|----------------------->|4
           |     QSIG RELEASE       |      |        1- ACK          |
          2|<-----------------------|      |<-----------------------|5
           |     QSIG RELEASE COMP  |      |                        |
          3|----------------------->|      |                        |
           |                        |      |                        |
           |                        |      |                        |
```

Figure 10: Typical message sequence for call clearing from QSIG to SIP, during establishment of a call from SIP to QSIG (gateway has not sent a final response to the SIP INVITE request)

1 The PISN sends a QSIG DISCONNECT message to the gateway
2 The gateway sends back a QSIG RELEASE message to the PISN in response to the QSIG DISCONNECT message
3 The PISN sends a QSIG RELEASE COMPLETE message in response. All PISN resources are now released.
4 The gateway maps the QSIG DISCONNECT message to a SIP 4xx-6xx response
5 The IP network sends back a SIP ACK request in response to the SIP 4xx-6xx response. All IP resources are now released

A.4.3. QSIG to SIP, during establishment of a call from QSIG to SIP

```
                            +--------------------+
                            |                    |
                            |      GATEWAY       |
         PISN               |                    |        IP NETWORK
          |                 +-----+------+-------+             |
          |                       |      |                     |
          |                       |      |                     |
          |                       |      |                     |
          |    QSIG DISCONNECT    |      |   1- CANCEL         |
        1 |---------------------->|......|-------------------->| 4
          |    QSIG RELEASE       |      |1-487 Request Terminated
        2 |<----------------------|      |<--------------------| 5
          |    QSIG RELEASE COMP  |      |                     |
        3 |---------------------->|      |   1- ACK            |
          |                       |      |-------------------->| 6
          |                       |      |                     |
          |                       |      |   1- 200 OK         |
          |                       |      |<--------------------| 7
          |                       |      |                     |
```

Figure 11: Typical message sequence for call clearing from QSIG to SIP, during establishment of a call from QSIG to SIP (gateway has received a provisional response to the SIP INVITE request but not a final response)

1 The PISN sends a QSIG DISCONNECT message to the gateway.
2 The gateway sends back a QSIG RELEASE message to the PISN in response to the QSIG DISCONNECT message.
3 The PISN sends a QSIG RELEASE COMPLETE message in response. All PISN resources are now released.
4 The gateway maps the QSIG DISCONNECT message to a SIP CANCEL request (subject to receipt of a provisional response, but not of a final response).
5 The IP network sends back a SIP 487 (Request Terminated) response to the SIP INVITE request.
6 The gateway, on receiving a SIP final response (487) to the SIP INVITE request, sends back a SIP ACK request to acknowledge receipt.
7 The IP network sends back a SIP 200 (OK) response to the SIP CANCEL request. All IP resources are now released.

A.5. Message Sequence for Call Clearing from SIP to QSIG

Below are typical message sequences for Call Clearing from SIP to QSIG

A.5.1. SIP to QSIG, subsequent to call establishment

```
                             +-------------------+
                             |                   |
                             |      GATEWAY      |
           IP NETWORK        |                   |                PISN
           |                 +-----+------+------+                  |
           |                       |      |                         |
           |                       |      |                         |
           |  2- BYE               |      |     QSIG DISCONNECT     |
         1 |---------------------->|......|------------------------>| 3
           |                       |      |     QSIG RELEASE        |
           |                       |      |<------------------------| 4
           |       2-200 OK        |      |     QSIG RELEASE COMP   |
         2 |<----------------------|      |------------------------>| 5
           |                       |      |                         |
           |                       |      |                         |
```

Figure 12: Typical message sequence for call clearing from SIP to QSIG, subsequent to call establishment

1 The IP network sends a SIP BYE request to the gateway.
2 The gateway sends back a SIP 200 (OK) response to the SIP BYE request. All IP resources are now released.
3 The gateway maps the SIP BYE request to a QSIG DISCONNECT message.
4 The PISN sends back a QSIG RELEASE message to the gateway in response to the QSIG DISCONNECT message.
5 The gateway sends a QSIG RELEASE COMPLETE message in response. All PISN resources are now released.

A.5.2. SIP to QSIG, during establishment of a call from QSIG to SIP

```
                             +-------------------+
                             |                   |
                             |     GATEWAY       |
          IP NETWORK         |                   |              PISN
          |                  +-----+------+------+                 |
          |                        |      |                        |
          |                        |      |                        |
          |   1- 4XX / 6XX         |      |     QSIG DISCONNECT    |
         1|----------------------->|......|----------------------->| 3
          |                        |      |     QSIG RELEASE       |
          |                        |      |<-----------------------| 4
          |        1- ACK          |      |     QSIG RELEASE COMP  |
         2|<-----------------------|      |----------------------->| 5
          |                        |      |                        |
          |                        |      |                        |
          |                        |      |                        |
```

Figure 13: Typical message sequence for call clearing from SIP to QSIG, during establishment of a call from QSIG to SIP (gateway has not previously received a final response to the SIP INVITE request)

1 The IP network sends a SIP 4xx-6xx response to the gateway.
2 The gateway sends back a SIP ACK request in response to the SIP 4xx-6xx response. All IP resources are now released.
3 The gateway maps the SIP 4xx-6xx response to a QSIG DISCONNECT message.
4 The PISN sends back a QSIG RELEASE message to the gateway in response to the QSIG DISCONNECT message.
5 The gateway sends a QSIG RELEASE COMPLETE message in response. All PISN resources are now released.

A.5.3. SIP to QSIG, during establishment of a call from SIP to QSIG

```
                             +-------------------+
                             |                   |
                             |      GATEWAY      |
         IP NETWORK          |                   |              PISN
          |                  +-----+------+------+                 |
          |                        |      |                        |
          |                        |      |                        |
          |   1- CANCEL            |      |     QSIG DISCONNECT    |
         1|----------------------->|......|----------------------->| 4
          |                        |      |     QSIG RELEASE       |
          |                        |      |<-----------------------| 5
          |1-487 Request Terminated|      |     QSIG RELEASE COMP  |
         2|<-----------------------|      |----------------------->| 6
          |                        |      |                        |
          |   1- ACK               |      |                        |
         3|----------------------->|      |                        |
          |                        |      |                        |
          |   1- 200 OK            |      |                        |
         4|<-----------------------|      |                        |
```

Figure 14: Typical message sequence for call clearing from SIP to QSIG, during establishment of a call from SIP to QSIG (gateway has sent a provisional response to the SIP INVITE request but not a final response)

1 The IP network sends a SIP CANCEL request to the gateway.
2 The gateway sends back a SIP 487 (Request Terminated) response to the SIP INVITE request.
3 The IP network, on receiving a SIP final response (487) to the SIP INVITE request, sends back a SIP ACK request to acknowledge receipt.
4 The gateway sends back a SIP 200 (OK) response to the SIP CANCEL request. All IP resources are now released.
5 The gateway maps the SIP 4xx-6xx response to a QSIG DISCONNECT message.
6 The PISN sends back a QSIG RELEASE message to the gateway in response to the QSIG DISCONNECT message.
7 The gateway sends a QSIG RELEASE COMPLETE message in response. All PISN resources are now released.

Authors' Addresses

John Elwell
Siemens plc
Technology Drive
Beeston
Nottingham, UK, NG9 1LA

EMail: john.elwell@siemens.com

Frank Derks
NEC Philips Unified Solutions
Anton Philipsweg 1
1223 KZ Hilversum
The Netherlands

EMail: frank.derks@nec-philips.com

Olivier Rousseau
Alcatel Business Systems
32,Avenue Kleber
92700 Colombes
France

EMail: Olivier.Rousseau@alcatel.fr

Patrick Mourot
Alcatel Business Systems
1,Rue Dr A. Schweitzer
67400 Illkirch
France

EMail: Patrick.Mourot@alcatel.fr

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).