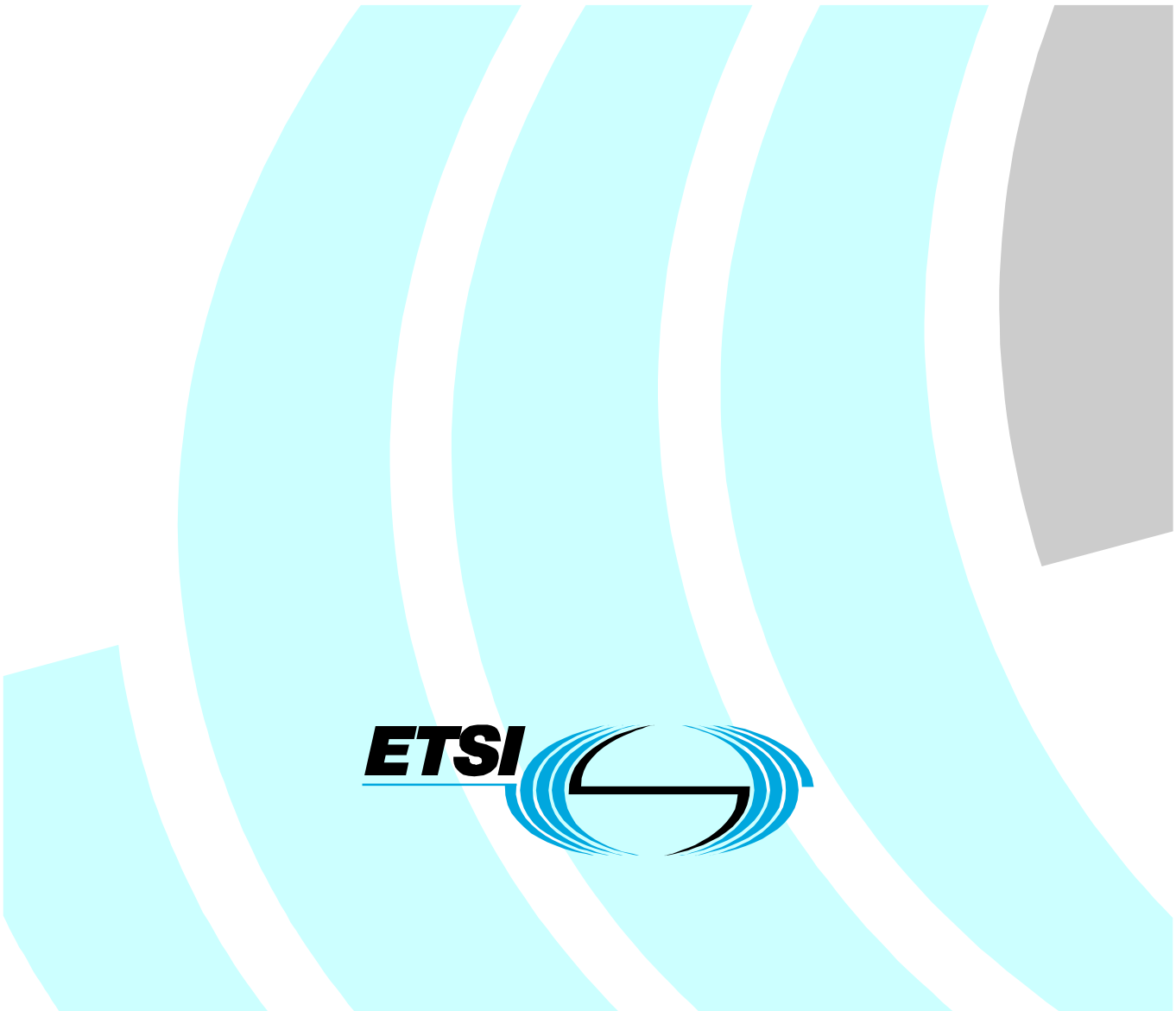
ETSI TS 102 166 V1.1.1 (2003-01)

Technical Specification

Corporate telecommunication Networks (CN); Signalling interworking between QSIG and SIP; Basic services



Reference
DTS/ECMA-00282

Keywords
PISN, QSIG, signalling, SIP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Table of contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

All published ETSI deliverables shall include information which directs the reader to the above source of information.

Foreword

This Technical Specification (TS) has been produced by ECMA on behalf of its members and those of the European Telecommunications Standards Institute (ETSI).

Brief History

The present document is one of a series of ECMA Standards defining the interworking of services and signalling protocols deployed in corporate telecommunication networks (CNs) (also known as enterprise networks). The series uses telecommunication concepts as developed by ITU-T and conforms to the framework of International Standards on Open Systems Interconnection as defined by ISO/IEC. It has been produced under ETSI work item DTS/ECMA-00282.

The present document defines the signalling protocol interworking for basic services between a Private Integrated Services Network (PISN) and a packet-based private telecommunications network based on the Internet Protocol (IP). It is further assumed that the protocol for the PISN part is QSIG and that the protocol for the IP-based network is SIP.

The present document is based upon the practical experience of ECMA member companies and the results of their active and continuous participation in the work of ISO/IEC JTC1, ITU-T, ETSI and other international and national standardization bodies. It represents a pragmatic and widely based consensus.

The present document has been adopted by the General Assembly of December 2002.

1 Scope

The present document specifies signalling interworking between "QSIG" and the Session Initiation Protocol (SIP) in support of basic services within a corporate telecommunication network (CN).

"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 other ECMA Standards, in particular ECMA-143 [2] (call control in support of basic services), ECMA-165 [4] (generic functional protocol for the support of supplementary services) and a number of Standards specifying individual supplementary services.

SIP is an application layer protocol for establishing, terminating and modifying multimedia sessions. It is typically carried over the Internet Protocol (IP) (IETF RFC 791 [7] and IETF RFC 2460 [12]). Telephone calls are considered as a type of multimedia session where just audio is exchanged. SIP is defined in IETF RFC 3261 [14].

The present document specifies 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. Call-related and call-independent signalling in support of supplementary services is outside the scope of the present document, 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 the present document. However, the functionality specified in the present document is in principle applicable to such a scenario when deployed in conjunction with other relevant functionality (e.g. number translation, security functions, etc.).

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

A brief assessment of security considerations in the IP network resulting from the interworking specified in the present document is given in annex C.

2 Conformance

In order to conform to the present document, a gateway shall satisfy the requirements identified in the Implementation Conformance Statement (ICS) proforma in annex A.

3 References

The following standards contain provisions which, through reference in this text, constitute provisions of the present document. All standards are subject to revision, and parties to agreements based on the present document are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

In the case of references to ECMA Standards that are aligned with ISO/IEC International Standards, the number of the appropriate ISO/IEC International Standard is given in brackets after the ECMA reference.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ECMA-133: "Private Integrated Services Network (PISN) - Reference configuration for PISN exchanges (PINX) (International Standard ISO/IEC 11579-1)".

[2] ECMA-143: "Private Integrated Services Network (PISN) - Circuit Mode Bearer Services - Inter-Exchange Signalling Procedures and Protocol (International Standard ISO/IEC 11572)".

[3] ECMA-155: "Private Integrated Services Networks - Addressing (International Standard ISO/IEC 11571)".

[4] ECMA-165: "Private Integrated Services Network (PISN) - Generic Functional Protocol for the Support of Supplementary Services - Inter-Exchange Signalling Procedures and Protocol (QSIG-GF) (International Standard ISO/IEC 11582)".

[5] ECMA-307: "Corporate Telecommunication Networks - Signalling Interworking between QSIG and H.323 - Generic Functional Protocol for the Support of Supplementary Services (International Standard ISO/IEC 21409)".

[6] IETF RFC 768: "User Datagram Protocol"; J. Postel.

[7] IETF RFC 791: "Internet Protocol"; J. Postel.

[8] IETF RFC 793: "Transmission Control Protocol"; J. Postel.

[9] IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types"; N. Freed/N. Borenstein.

[10] IETF RFC 2246: "The TLS protocol Version 1.0", T. Dierks, C. Allen.

[11] IETF RFC 2327: "SDP: Session Description Protocol"; M. Handley/V. Jacobson.

[12] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification"; S. Deering, R. Hinden.

[13] IETF RFC 2960: "Stream Control Transmission Protocol"; R. Stewart et alia.

[14] IETF RFC 3261: "SIP: Session Initiation Protocol"; M. Handley/H. Schulzrinne/E. Schooler/J. Rosenberg.

[15] IETF RFC 3262: "Reliability of Provisional Responses in Session Initiation Protocol (SIP)"; J. Rosenberg /H. Schulzrinne.

[16] IETF RFC 3264: "An Offer/Answer Model with Session Description Protocol (SDP)"; J. Rosenberg /H. Schulzrinne.

[17] IETF RFC 3323: "A Privacy Mechanism for the Session Initiation Protocol (SIP)"; J. Peterson.

[18] IETF RFC 3325: "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks"; C. Jennings, J. Peterson, M. Watson.

[19] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[20] IETF RFC 3311: "The Session Initiation Protocol (SIP) UPDATE Method".

[21] ITU-T Recommendation G.711: "Pulse code modulation (PCM) of voice frequencies".

4 Definitions

For the purposes of the present document, the following terms and definitions apply:

4.1 External definitions

The present document uses the following terms defined in other documents:

Call	(ECMA-307 [5])
Corporate telecommunication network (CN)	(ECMA-307 [5])
Private Integrated Services Network (PISN)	(ECMA-307 [5])
Private Integrated services Network eXchange (PINX)	(ECMA-133 [1])

Additionally the definitions in ECMA-143 [2] and IETF RFC 3261 [14] apply as appropriate.

4.2 Other definitions

4.2.1 Gateway

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

4.2.2 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.

4.2.3 Media stream

Audio or other user information transmitted in UDP packets 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.

5 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

6 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 24 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 ITU-T Recommendation E.164 [19] or a private numbering plan. This basic call capability is specified in ECMA-143 [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.

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

The present 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.

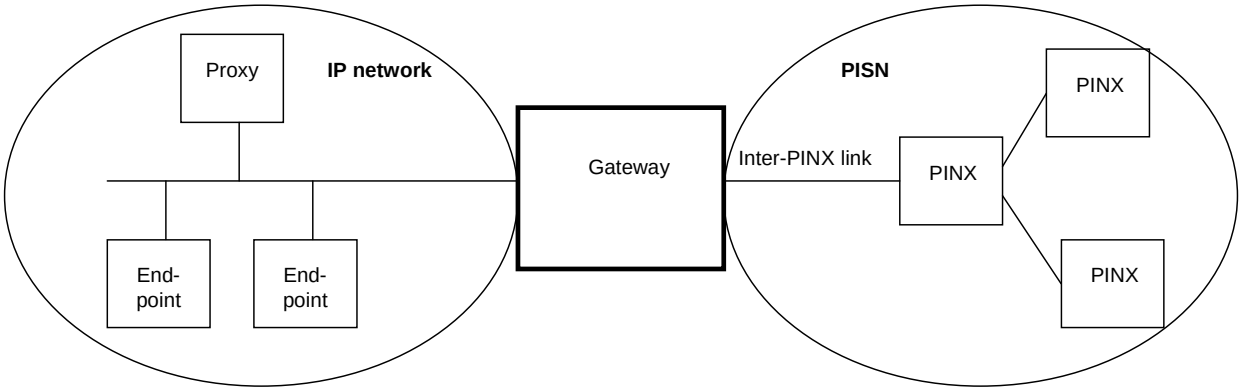


Figure 1: Environment

In addition to the signalling interworking functionality specified in the present document, 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 information 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 (IETF RFC 768 [6]) and TCP (IETF RFC 793 [8]) as transport layer protocols, these being used for the transport of SIP signalling messages and, in the case of UDP, also for media information;
- optionally the support of TLS (IETF RFC 2246 [10]) and/or SCTP (IETF RFC 2960 [13]) 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 information in each direction between the PISN and the IP network, including as a minimum packetization of media information sent to the IP network and de-packetization of media information received from the IP network.

NOTE: IETF RFC 3261 [14] 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.

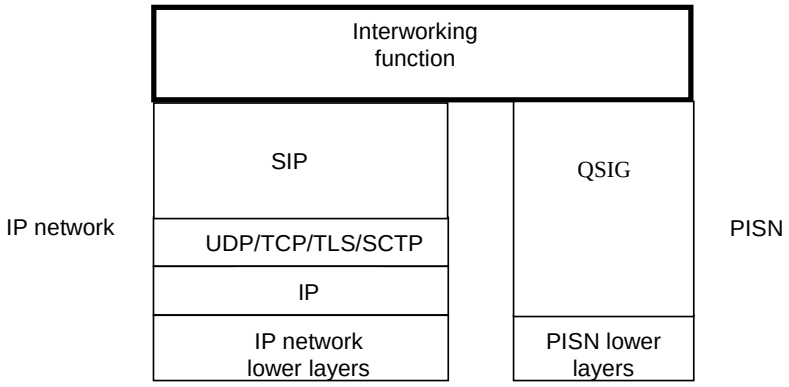


Figure 2: Protocol model

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.

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 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 200 OK response 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.

Annex B gives examples of typical message sequences that can arise.

7 General requirements

In order to conform to the present document, a gateway shall support QSIG in accordance with ECMA-143 [2] as a gateway and shall support SIP in accordance with IETF RFC 3261 [14] 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 IETF RFC 3261 [14]. In addition, the gateway shall support SIP TU behaviour for a UA in accordance with IETF RFC 3261 [14] except where stated otherwise in the present document.

NOTE 1: IETF RFC 3261 [14] 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 IETF RFC 3262 [15] as a UA.

NOTE 2: IETF RFC 3262 [15] 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 IETF RFC 2327 [11] and its use in accordance with the offer/answer model in IETF RFC 3264 [16].

Clause 9 also specifies optional use of the Privacy header in accordance with IETF RFC 3323 [17] and the P-Asserted-Identity header in accordance with IETF RFC 3325 [18].

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

SIP methods not defined in IETF RFC 3261 [14], IETF RFC 3262 [15], IETF RFC 3323 [17] or IETF RFC 3325 [18] are outside the scope of the present document 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 look-up 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 the present document. However, any behaviour specified in the present document on receipt of a SIP final response should apply only when there are no more candidate destinations to try.

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 ECMA-143 [2] and shall act in accordance with ECMA-143 [2] on detection of a QSIG protocol error. The requirements of this clause 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 the present document.

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 IETF RFC 3261 [14] and shall act in accordance with IETF RFC 3261 [14] on detection of a SIP protocol error. Requirements of this clause 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 clause 8.2.2.2 of IETF RFC 3261 [14]) 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 clause.

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

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 ECMA-143 [2] and shall act in accordance with ECMA-143 [2] if a QSIG protocol timer expires. Any other action on expiry of a QSIG protocol timer is outside the scope of the present document, except that if it results in the clearing of the QSIG call, the gateway shall also clear the SIP call in accordance with clause 8.4.5.

The gateway shall run SIP protocol timers as specified in IETF RFC 3261 [14] and shall act in accordance with IETF RFC 3261 [14] if a SIP protocol timer expires. Any other action on expiry of a SIP protocol timer is outside the scope of the present document, except that if it results in the clearing of the SIP call, the gateway shall also clear the QSIG call in accordance with clause 8.4.5.

8.2 Call establishment from QSIG to SIP

8.2.1 Call establishment from QSIG to SIP using enbloc 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: 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 the gateway cannot determine to 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 clause 9. The gateway shall include in the INVITE request a Supported header containing option tag 100rel, to indicate support for IETF RFC 3262 [15].

The gateway shall include SDP information in the SIP INVITE request as described in clause 10.

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 ECMA-143 [2].

8.2.1.2 Receipt of SIP 100 (Trying) response

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

The gateway shall map a received SIP 18x response 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 a media stream has been established towards the gateway and 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, no QSIG PROGRESS message containing progress description number 8 has been sent and a media stream has been established towards the gateway, the gateway shall generate a QSIG PROGRESS message. The QSIG PROGRESS message shall contain progress description number 8 in a Progress indicator information element. The gateway shall also connect the media streams to the corresponding user information channel of the inter-PINX link.

- If a SIP 181/182/183 response is received, no QSIG ALERTING message has been sent, no QSIG PROGRESS message containing progress description number 1 or 8 has been sent and no media stream has been established towards the gateway, the gateway shall generate a QSIG PROGRESS message. The QSIG PROGRESS message shall contain progress description number 1 in a Progress indicator information element.

NOTE 1: This will ensure that QSIG timer T310 is stopped if running at the Originating PINX.

NOTE 2: Media streams are established as a result of receiving SDP answer information in a reliable provisional response and can be modified by means of the SIP UPDATE method (IETF RFC 3311 [20]). If a media stream is established towards the gateway, connecting the media stream to the corresponding user information channel on the inter-PINX link will allow the caller to hear in-band tones or announcements.

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 IETF RFC 3262 [15].

8.2.1.4 Receipt of SIP 2xx response

If the gateway receives a SIP 200 (OK) response as the first SIP 200 response to a SIP INVITE request, the gateway shall map the SIP 200 (OK) response to a QSIG CONNECT message. The gateway shall also send a SIP ACK request to acknowledge the 200 (OK) response. The gateway shall not include any SDP information in the SIP ACK request. If the gateway receives further 200 (OK) responses, it shall respond to each in accordance with IETF RFC 3261 [14] 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 200 (OK) response is received in response to the SIP PRACK request, the gateway shall not map this message to any QSIG message.

If the gateway receives a SIP 2xx response other than 200 (OK), the gateway shall send a SIP ACK request.

NOTE: A SIP 200 (OK) response can be received later as a result of a forking proxy.

8.2.1.5 Receipt of SIP 3xx response

On receipt of a SIP 3xx response, the gateway shall act in accordance with IETF RFC 3261 [14].

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 the present document.

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 clause 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 clause 8.2.2.2 shall apply.

8.2.2.1 Enbloc 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 clause 8.2.1.1. The Request-URI and To fields (see clause 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

SIP responses shall be mapped as described in clause 8.2.1.

8.2.2.2 Overlap signalling in SIP network

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 clause 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 ECMA-143 [2].

NOTE 1: ECMA-143 [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 clause 8.2.2.1.2. If the gateway still does not have the minimum number of digits required than it shall wait for more QSIG INFORMATION messages to arrive.

If the gateway has already sent one or more SIP INVITE requests, and whether or not final responses to those requests have been received, it shall send a new SIP INVITE request with the new digits. The new SIP INVITE request shall have the same Call-ID as the first SIP INVITE request sent but shall have updated Request-URI and To fields. The updated Request-URI and To fields (see clause 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 CSeq header should contain a value higher than that in the previous SIP INVITE request.

NOTE 2: The first SIP INVITE request and all subsequent SIP INVITE requests sent in this way belong to the same call but to different dialogs.

8.2.2.2.3 Receipt of SIP 100 (Trying) response

The requirements of clause 8.2.1.2 shall apply.

8.2.2.2.4 Receipt of SIP 18x provisional response

The requirements of clause 8.2.1.3 shall apply.

8.2.2.2.5 Receipt of SIP 2xx response

The requirements of clause 8.2.1.4 shall apply. In addition the gateway shall send a SIP CANCEL request, either immediately or after a short delay, to cancel any SIP INVITE transactions for which no final response has been received.

NOTE: Delaying the sending of a SIP CANCEL request allows time for final responses to be received on any outstanding transactions, thereby avoiding unnecessary signalling.

8.2.2.2.6 Receipt of SIP 3xx response

The requirements of clause 8.2.1.5 shall apply.

8.2.2.2.7 Receipt of a SIP 484 (Address Incomplete) response

The SIP 484 response indicates that more digits are required to complete the call. On receipt of a SIP 484 response the gateway shall send back a SIP ACK request. The gateway shall also send a QSIG DISCONNECT message (see clause 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 484 response shall not trigger the sending of any QSIG message.

8.2.2.2.8 Receipt of a SIP 4xx (except 484), 5xx or 6xx response

If a SIP 4xx (except 484), 5xx or 6xx final response arrives for a pending SIP INVITE transaction, the gateway shall send a SIP ACK request. If this occurs when no further QSIG INFORMATION messages are expected and final responses have been received to all transmitted SIP INVITE requests, the gateway shall send a QSIG DISCONNECT message (see clause 8.4.4). Otherwise the gateway may send a QSIG DISCONNECT message.

NOTE: The gateway can take account of the SIP response code and other information to assess whether to wait for further responses before initiating clearing.

8.2.2.2.9 Receipt of multiple SIP responses

The responses to all the SIP INVITE requests sent except for the last one are typically SIP 4xx responses (e.g. 484 (Address Incomplete)) that terminate the SIP INVITE transaction.

However, the gateway can receive a SIP 183 (Session Progress) response with a media description. The media stream will typically contain a message such as "…We are trying to connect you… ". The issue of receiving different SIP 183 (Session Progress) responses with media descriptions for different SIP INVITE transactions is a gateway concern. The gateway should decide which media stream (if any) is to be played to the user.

NOTE: The gateway can receive multiple SIP 183 responses with media description not only as a result of sending multiple INVITE requests due to overlap sending but also as a result of a forking proxy.

8.2.2.2.10 Cancelling pending SIP INVITE transactions

When a gateway sends a new SIP INVITE request containing new digits, it should not send a SIP CANCEL request to cancel the previous SIP INVITE transaction. 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 clause 8.2.2.2.5 there is provision for cancelling any transactions still in progress after a SIP 2xx response has been received.

8.2.2.2.11 SIP INVITE requests reaching multiple gateways

Each SIP INVITE request sent by a gateway represents a new transaction and hence can be routed differently. For instance, the first SIP INVITE request might be routed to a particular egress gateway and a subsequent SIP INVITE request to another gateway. The result is that both gateways initiate call establishment in the remote network. Since one of the call establishments has an incomplete destination number, it can be expected to fail, having already consumed resources in the remote network.

To avoid this problem it is recommended that all the SIP INVITE requests should follow the same path as the first one. This would however restrict the number of services the SIP network can provide. It would not be possible to route a subsequent SIP INVITE request to an application server just because the previous one was routed in a different way.

This issue should be taken into consideration before using overlap signalling in SIP. If initiating multiple call establishments in the remote network is not acceptable in a particular application, overlap signalling should not be used.

8.2.2.2.12 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 message 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, and 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 clause 9 and shall generate the Bearer capability information element in accordance with clause 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 1: 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 shall not issue a QSIG SETUP message and shall send a SIP 488 (Not Acceptable Here) response.

NOTE 2: 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 IETF RFC 3262 [15]) 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.

NOTE 3: 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, since a reliable provisional response is not necessary.

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. 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 IETF RFC 3262 [15], inclusion of option tag 100rel in a provisional response instructs the UAC to acknowledge the provisional response by sending a PRACK request. IETF RFC 3262 [15] 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 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 183 provisional response shall be in accordance with clause 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. 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 IETF RFC 3262 [15], inclusion of option tag 100rel in a provisional response instructs the UAC to acknowledge the provisional response by sending a PRACK request. IETF RFC 3262 [15] 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 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 clause 8.3.5.

8.3.5 Inclusion of SDP information in a SIP 18x provisional response

When sending a SIP 18x provisional response, the gateway shall include SDP information 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 1: 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 2: 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 3: 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 clause 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 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 1: 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 18x provisional response.

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

NOTE 3: 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 clause 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 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

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.

If a gateway receives a SIP INVITE request with the same Call-ID as an existing call for which the QSIG state is overlap sending and with updated Request-URI and To fields from which a called party number with a superset of digits can be derived, it shall generate a QSIG INFORMATION message using the call reference of the existing QSIG call instead of a new QSIG SETUP message. 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 with the same Call-ID as an existing SIP INVITE request for which the gateway has not yet sent a final response and failing to meet the other conditions above concerning overlap sending, the gateway shall clear the call by sending back a SIP 485 (Ambiguous) response and a QSIG DISCONNECT message with Cause Value 16 (Normal call clearing).

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 and received a SIP ACK request or has received a SIP 200 (OK) response 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 (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 IETF RFC 3261 [14], 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 behaviour 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 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 ECMA-143 [2] and IETF RFC 3261 [14] respectively.

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

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	(see note 1)	
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	603 403	Decline, if location field in Cause information element indicates user. Otherwise: Forbidden
22	Number changed	301 410	Moved permanently, if information in diagnostic field of Cause information element is suitable for generating a SIP Contact header. Otherwise: 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 (see note 2)
69	Requested facility not implemented	501	Not implemented
70	Only restricted digital information available	488	Not acceptable here (see note 2)
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 1: 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, the default response code should be used. NOTE 2: 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 ECMA-143 [2] and IETF RFC 3261 [14] respectively.

NOTE: When responding to a SIP BYE request, in accordance with IETF RFC 3261 [14] 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 ECMA-143 [2] and IETF RFC 3261 [14] respectively.

8.4.4 Receipt of a SIP 4xx - 6xx response

Except where otherwise specified in the context of overlap sending (see clause 8.2.2.2), on receipt of a SIP final response (4xx-6xx) to a SIP INVITE request, 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 ECMA-143 [2] and IETF RFC 3261 [14] 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 QSIG Cause values

SIP response		QSIG Cause value	
400	Bad request	41	Temporary failure
401	Unauthorized	21	Call rejected (see note 1)
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 (see note 1)
408	Request timeout	102	Recovery on timer expiry
410	Gone	22	Number changed
413	Request entity too large	127	Interworking, unspecified (see note 2)
414	Request-URI too long	127	Interworking, unspecified (see note 2)
415	Unsupported media type	79	Service or option not implemented, unspecified (see note 2)
416	Unsupported URI scheme	127	Interworking, unspecified (see note 2)
420	Bad extension	127	Interworking, unspecified (see note 2)
421	Extension required	127	Interworking, unspecified (see note 2)
423	Interval too brief	127	Interworking, unspecified (see note 2)
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 (see note 2)
485	Ambiguous	1	Unallocated Number
486	Busy here	17	User busy
487	Requested Terminated	(see note 3)	
488	Not Acceptable Here	65 31	Bearer capability not implemented or Normal, unspecified (see note 4)
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 (see note 2)
513	Message too large	127	Interworking, unspecified (see note 2)
600	Busy everywhere	17	User busy
603	Decline	21	Call rejected
604	Does not exist anywhere	1	Unallocated number
606	Not acceptable	65 31	Bearer capability not implemented, or Normal, unspecified (see note 4)

NOTE 1: 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 2: If at all possible, the gateway should respond to these protocol errors by remedying unacceptable behaviour and attempting to re-originate the session. Only if this proves impossible should the gateway clear the call in the QSIG network with this cause value.

NOTE 3: 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 4: 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 ECMA-143 [2], the gateway shall also initiate clearing of the SIP call in accordance with clause 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 IETF RFC 3261 [14], the gateway shall also initiate clearing of the QSIG call in accordance with ECMA-143 [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 503 (Service unavailable) 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 ECMA-155 [3]. 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 that 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 IETF RFC 3261 [14] and the P-Asserted-Identity header specified in IETF RFC 3325 [18]. In addition, privacy is indicated by the Privacy header specified in IETF RFC 3323 [17].

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 IETF RFC 3325 [18]. If a gateway implements the P-Asserted-Identity header it shall also implement the Privacy header in accordance with IETF RFC 3323 [17]. 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 the present document. 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 trusts the adjacent proxy (i.e. the proxy 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 be configurable to either trust or not trust the proxy 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 not generate a P-Asserted-Identity header, shall not generate a Privacy header and shall include a URI identifying the gateway in the From header.

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

In this case the gateway shall not generate a P-Asserted-Identity header, shall generate a Privacy header with parameter priv-value = "id" if the gateway supports this header, 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 the present document.

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 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 the present document.

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 clause 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.

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 the gateway shall not generate a P-Asserted-Identity header and shall generate a Privacy header with parameter priv-value = "id" if the gateway supports this header. The inclusion of additional values of the priv-value parameter in the Privacy header is outside the scope of the present document.

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 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 the present document.

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 clause 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.

9.2 Mapping from SIP to QSIG

The method used to convert a URI to a number is outside the scope of the present document. However, NPI and TON fields in the QSIG information element concerned shall be set to appropriate values in accordance with ECMA-155 [3].

Some aspects of mapping depend on whether the gateway trusts the adjacent proxy (i.e. the proxy 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 be configurable to either trust or not trust the proxy 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 the 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 consider 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 the 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 a P-Asserted-Identity header and 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 the P-Asserted-Identity header, 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 from a P-Asserted-Identity header (including the case where there is no P-Asserted-Identity header) and if the gateway is prepared to use the 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, the gateway shall include value "presentation restricted" in the presentation indicator. 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 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 200 (OK) response to an INVITE request to a QSIG CONNECT message, the gateway shall generate a Connected number information element as follows.

If the SIP 200 (OK) response contains a P-Asserted-Identity header and 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 the P-Asserted-Identity header, 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 (including the case where there is no P-Asserted-Identity header), the gateway shall not include a number in the Connected number information element.

If the SIP 200 (OK) 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. 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

The present 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 information received along with the SIP INVITE request. If the SIP INVITE request does not contain SDP information or the media type in the SDP 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 the present document.

Table 3: Bearer capability encoding for "audio" transfer

Field	Value
Coding Standard	"ITU-T 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 "ITU-T Recommendation G.711 [21] μ-law" (00010) "ITU-T Recommendation G.711 [21] A-law" (00011)

10.2 Derivation of media type in SDP

The gateway shall generate SDP information to include in the SIP INVITE request based on the Bearer capability information element received in the QSIG SETUP message. The media type included in the SDP information shall be 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
"unrestricted digital information" (01000)	data

Annex A (normative): Implementation Conformance Statement (ICS) proforma

A.1 Introduction

A.1.1 Purpose of an ICS proforma

The supplier of an implementation which is claimed to conform to the present document shall complete the following Implementation Conformance Statement (ICS) proforma.

A completed ICS proforma is the ICS for the implementation in question. The ICS is a statement of which capabilities and options have been implemented for a given specification.

The ICS can have a number of uses, including use:

- by the implementor, as a check list for implementations to reduce the risk of unintended non-conformance, e.g. through oversight;
- by the supplier and acquirer, or potential acquirer, of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the Standard's ICS proforma;
- by the user or potential user of the implementation, as a basis for initially checking the possibility of interworking with another implementation - while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible ICS;
- by a tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

A.2 Instructions for completing the ICS proforma

A.2.1 General structure of the ICS proforma

The ICS proforma is a fixed format questionnaire divided into sub-clauses each containing a group of individual items. Each item is identified by an item reference, the description of the item (question to be answered), and the reference(s) to the clause(s) that specifies (specify) the item in the main body of the present document.

The "Conditions for Status" column contains a specification, if appropriate, of the predicate upon which a conditional status is based. The indication of an item reference in this column indicates a simple-predicate condition (support of this item is dependent on the support marked for the referenced item).

The "Status" column indicates whether an item is applicable and if so whether support is mandatory or optional. The following terms are used:

I	irrelevant or out-of-scope - this capability is outside the scope of the standard to which this ICS proforma applies and is not subject to conformance testing in this context;
M	mandatory (the capability is required for conformance to the standard);
N/A	not applicable - in the given context, it is impossible to use the capability; no answer in the support column is required,
O	optional (the capability is not required for conformance to the standard, but if the capability is implemented it is required to conform to the specification in the present document);
O.<n>	qualified optional - in this case, <n> is an integer that identifies a unique group of related optional items; if no additional qualification is indicated, the support of at least one of the optional items is required for conformance to the present document; otherwise, the qualification and logic of the selection among the optional items is defined below the table explicitly;
X	excluded or prohibited - there is a requirement not to use this capability in a given context;

Answers to the questionnaire items are to be provided in the "Support" column, by simply marking an answer to indicate a restricted choice (Yes, No or N/A). In specific cases, the indication of explicit values may be requested. Where a support column box is left blank, no answer is required.

If a "prerequisite line" (see clause A.2.4) is used after a clause heading or table title, and its predicate is false, no answer is required for the whole clause or table, respectively.

A.2.2 Additional information

Items of Additional Information allow a supplier to provide further information intended to assist the interpretation of the ICS. It is not intended or expected that a large quantity will be supplied, and an ICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations.

References to items of Additional Information may be entered next to any answer in the questionnaire, and may be included in items of Exception Information.

A.2.3 Exception information

It may occasionally happen that a supplier will wish to answer an item with mandatory or prohibited status (after any conditions have been applied) in a way that conflicts with the indicated requirement. No pre-printed answer will be found in the Support column for this. Instead, the supplier is required to write into the support column an x.<i> reference to an item of Exception Information, and to provide the appropriate rationale in the Exception item itself.

An implementation for which an Exception item is required in this way does not conform to the present document. A possible reason for the situation described above is that a defect in the Standard has been reported, a correction for which is expected to change the requirement not met by the implementation.

A.2.4 Further indications of the ICS proforma tables

In addition to the columns of a table, the following information may be indicated:

"Prerequisite line"

A prerequisite line after a clause heading or table title indicates that the whole clause or the whole table is not required to be completed if the predicate is false.

"Qualification"

At the end of a table, a detailed qualification for a group of optional items may be indicated, as specified in the description of the status "qualified optional" in clause A.2.1.

"Comments"

This box at the end of a table allows a supplier to enter any comments to that table. Comments may also be provided separately (without using this box).

A.3 Identification of the implementation

A.3.1 Implementation identification

Supplier (see note 1)	
Contact point for queries about the ICS (see note 1)	
Implementation Name(s) and Version(s) (see notes 1 and 2)	
Other information necessary for full identification - e.g. name(s) and version(s) for machines and/or operating systems; System name(s)	

NOTE 1: Only the first three items are required for all implementations; other information may be completed as appropriate in meeting the requirement for full identification.

NOTE 2: The terms Name and Version should be interpreted appropriately to correspond with a supplier's terminology (e.g. Type, Series, Model).

A.3.2 Specification for which this ICS applies

Title	Corporate Telecommunication Networks - Signalling Interworking between QSIG and SIP - Basic Services
Version	1.0
Corrigenda Implemented (if applicable)	
Addenda Implemented (if applicable)	
Amendments Implemented (if applicable)	
Have any exception items been required?	No[ ]Yes[ ] (The answer Yes means that the implementation does not conform to the present document) (see note)
Date of Statement	
NOTE: In this case, an explanation shall be given of the nature of non-conformance either below or on a separate sheet of paper. Nature of non-conformance (if applicable):	

A.4 General requirements

Table A.1: General requirements

Item	Question: Does the implementation...	Conditions for status	Status	Reference	Support
GR1	support QSIG in accordance with ECMA-143 as a gateway?		M	7	[ ]Yes
GR2	support SIP in accordance with IETF RFC 3261 as a UA?		M	7	[ ]Yes
GR3	support SIP reliable provisional responses in accordance with IETF RFC 3262 as UA?		M	7	[ ]Yes
GR4	support calls from QSIG to SIP		M	7	[ ]Yes
GR5	support calls from SIP to QSIG		M	7	[ ]Yes
GR6	support QSIG message validation and handling of protocol errors		M	8.1	[ ]Yes
GR7	support SIP message validation and handling of protocol errors		M	8.1	[ ]Yes
Comments:					

A.5 Call establishment from QSIG to SIP using en bloc procedures

Table A.2: Call establishment from QSIG to SIP using en bloc procedures

Item	Question: Does the implementation...	Conditions for status	Status	Reference	Support
QS1	support receipt of QSIG SETUP message		M	8.2.1.1	[ ]Yes
QS2	support receipt of SIP 100 response		M	8.2.1.2	[ ]Yes
QS3	support receipt of SIP 18x provisional response		M	8.2.1.3	[ ]Yes
QS4	support receipt of SIP 2xx response		M	8.2.1.4	[ ]Yes
QS4	support receipt of SIP 3xx response		M	8.2.1.5	[ ]Yes
Comments:					

A.6 Call establishment from QSIG to SIP using overlap procedures in QSIG network and en bloc procedures in SIP network

Table A.3: Call establishment from QSIG to SIP using overlap procedures in QSIG network and en bloc procedures in SIP network

Item	Question: Does the implementation...	Conditions for status	Status	Reference	Support
QSO1	support receipt of QSIG SETUP message		M	8.2.2.1.1	[ ]Yes
QSO2	support receipt of QSIG INFORMATION message		M	8.2.2.1.2	[ ]Yes
QSO3	support of SIP responses		M	8.2.2.1.3	[ ]Yes
Comments:					

A.7 Call establishment from QSIG to SIP using overlap procedures in QSIG network and in SIP network

Table A.4: Call establishment from QSIG to SIP using overlap procedures in QSIG network and in SIP network

Item	Question: Does the implementation...	Conditions for status	Status	Reference	Support
QSOO1	support receipt of QSIG SETUP message		M	8.2.2.2.1	[ ]Yes
QSOO2	support receipt of QSIG INFORMATION message		M	8.2.2.2.2	[ ]Yes
QSOO3	support receipt of SIP 100 response		M	8.2.2.2.3	[ ]Yes
QSOO4	support receipt of SIP 1xx provisional response		M	8.2.2.2.4	[ ]Yes
QSOO5	support receipt of SIP 2xx response		M	8.2.2.2.5	[ ]Yes
QSOO6	support receipt of SIP 3xx response		M	8.2.2.2.6	[ ]Yes
QSOO7	support receipt of SIP 484 response		M	8.2.2.2.7	[ ]Yes
QSOO8	support receipt of SIP 4xx response (other than 484), SIP 5xx response or SIP 6xx response in the context of overlap sending		M	8.2.2.2.8	[ ]Yes
Comments:					

A.8 Call establishment from SIP to QSIG

Table A.5: Call establishment from SIP to QSIG

Item	Question: Does the implementation...	Conditions for status	Status	Reference	Support
SQ1	support receipt of SIP INVITE request for a new call		M	8.3.1	[ ]Yes
SQ2	support receipt of QSIG CALL PROCEEDING message		M	8.3.2	[ ]Yes
SQ3	support receipt of QSIG PROGRESS message		M	8.3.3	[ ]Yes
SQ4	support receipt of QSIG ALERTING message		M	8.3.4	[ ]Yes
SQ5	support inclusion of SDP information in a SIP 18x provisional response		M	8.3.5	[ ]Yes
SQ6	support receipt of QSIG CONNECT message		M	8.3.6	[ ]Yes
SQ7	support receipt of SIP PRACK request		M	8.3.7	[ ]Yes
SQ8	support receipt of SIP ACK request		M	8.3.8	[ ]Yes
SQ9	support receipt of SIP INVITE request for a call already being established		M	8.3.9	[ ]Yes
Comments:					

A.9 Call clearing and call failure

Table A.6: Call clearing

Item	Question: Does the implementation...	Conditions for status	Status	Reference	Support
CC1	support receipt of QSIG DISCONNECT, RELEASE or RELEASE COMPLETE message		M	8.4.1	[ ]Yes
CC2	support receipt of SIP BYE request		M	8.4.2	[ ]Yes
CC3	support receipt of SIP CANCEL request		M	8.4.3	[ ]Yes
CC4	support receipt of SIP 4xx-6xx response, except where specified otherwise in the context of overlap sending		M	8.4.4	[ ]Yes
CC5	support gateway-initiated call clearing		M	8.4.5	[ ]Yes
Comments:					

A.10 Other requirements

Table A.7: Other requirements

aItem	Question: Does the implementation...	Conditions for status	Status	Reference	Support
OR1	support rejection of request to change media characteristics		M	8.5	[ ]Yes
OR2	support number mapping from SIP to QSIG		M	9.1	
OR3	support number mapping from QSIG to SIP		M	9.2	
OR4	support the P-Asserted-Identity header		O	9.1, 9.2	[ ] Yes, [ ] No
OR5	support the Privacy header	OR4 NOT OR4	M O	9.1, 9.2	[ ] Yes, [ ] Yes, [ ] No
OR6	support derivation of QSIG Bearer capability information element		M	10.1	
OR7	support derivation of media type in SDP information		M	10.2	
Comments:					

Annex B (informative): Example message sequences

B.1 Introduction

This annex shows some typical message sequences that can occur for an interworking between QSIG and SIP.

NOTE 1: 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 2: 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 3: In these examples SIP provisional responses (other than 100) are shown as being sent reliably, using the PRACK method for acknowledgement.

B.2 Message sequences for call establishment from QSIG to SIP

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

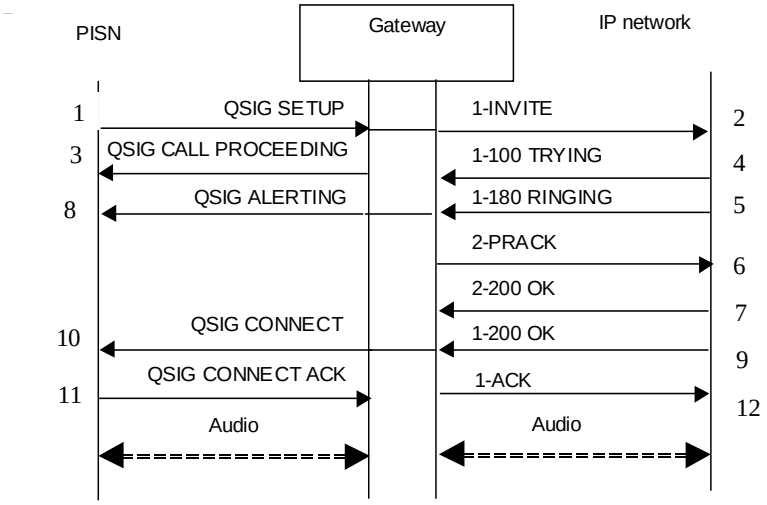


Figure B.1: Typical message sequence for successful call establishment from QSIG to SIP using enbloc procedures on both QSIG and SIP

Steps	Comments
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

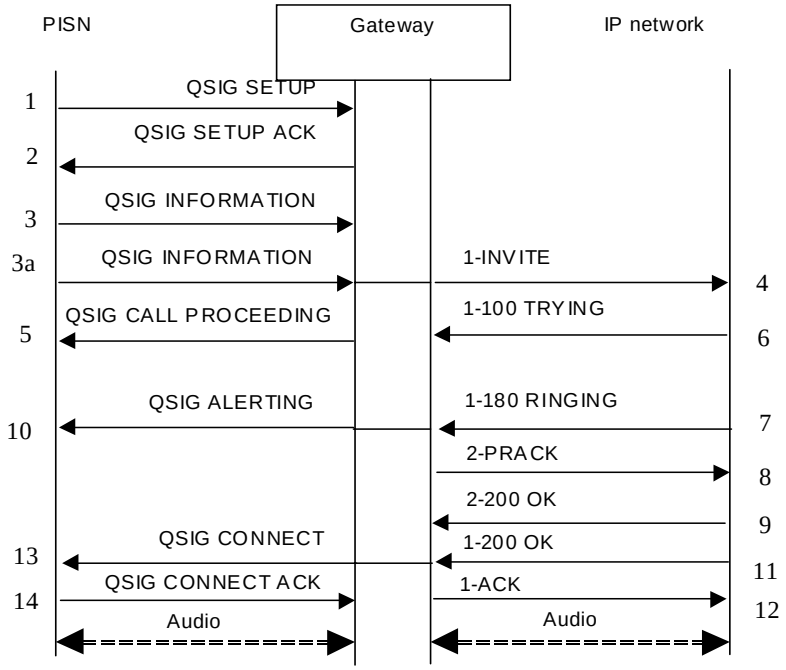


Figure B.2: Typical message sequence for successful call establishment from QSIG to SIP using overlap receiving on QSIG and enbloc sending on SIP

Steps	Comments
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

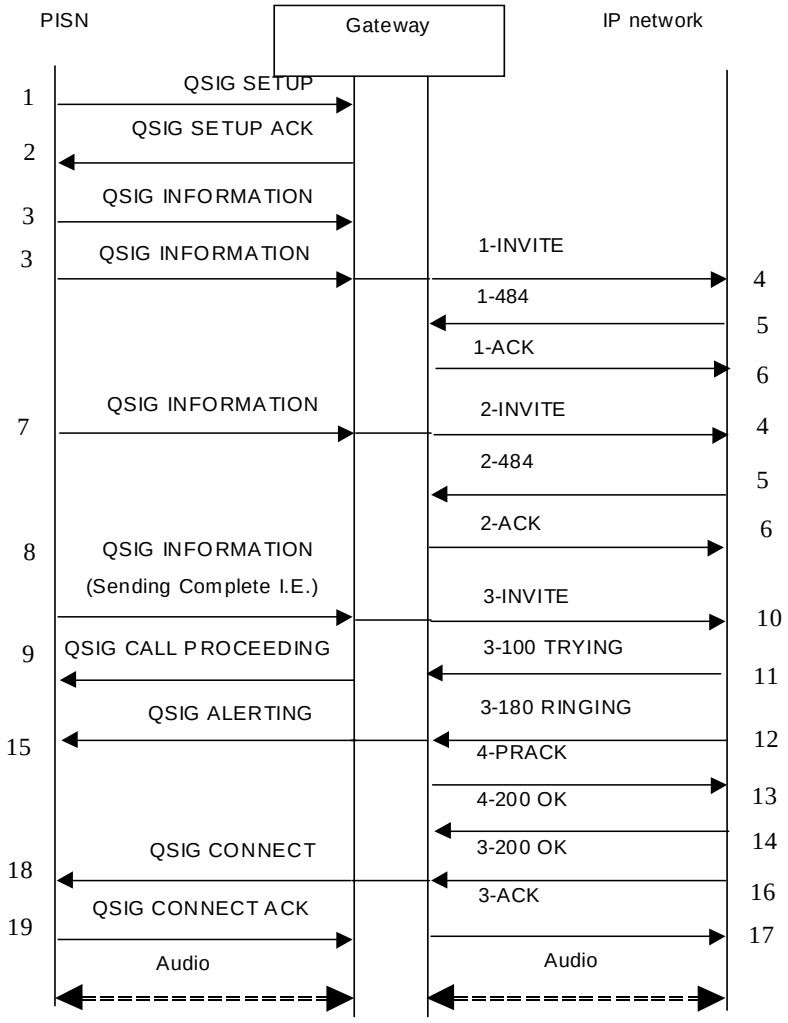


Figure B.3: Typical message sequence for successful call establishment from QSIG to SIP using overlap procedures on both QSIG and SIP

Steps	Comments
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 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

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

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

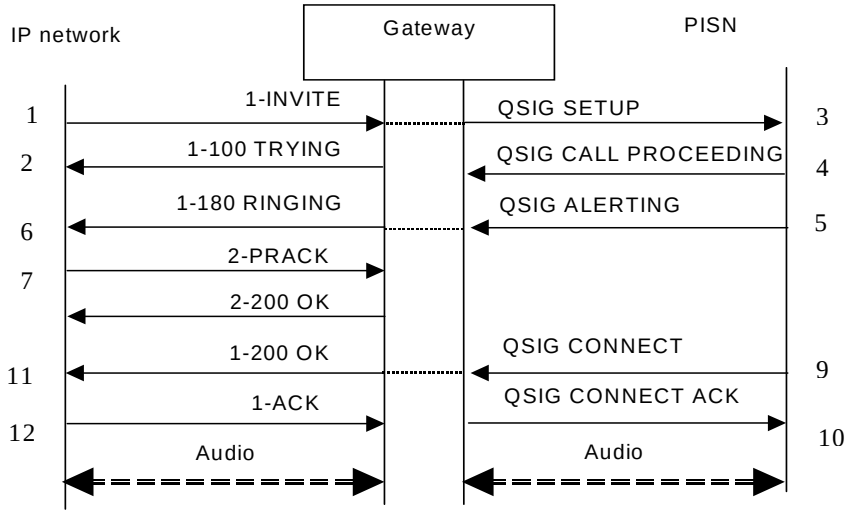


Figure B.4: Typical message sequence for successful call establishment from SIP to QSIG using enbloc procedures

Steps	Comments
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

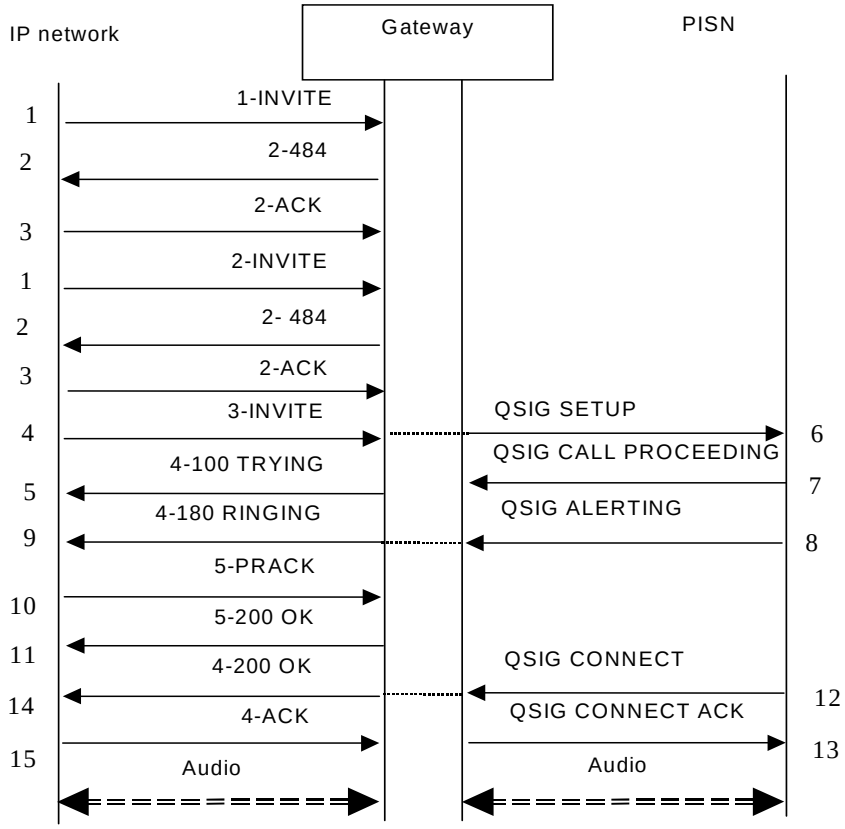


Figure B.5: Typical message sequence for successful call establishment from SIP to QSIG using overlap receiving on SIP and enbloc sending on QSIG

Steps	Comments
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. The gateway sends a SIP 100 (Trying) response to the IP network
3	The IP network acknowledge 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

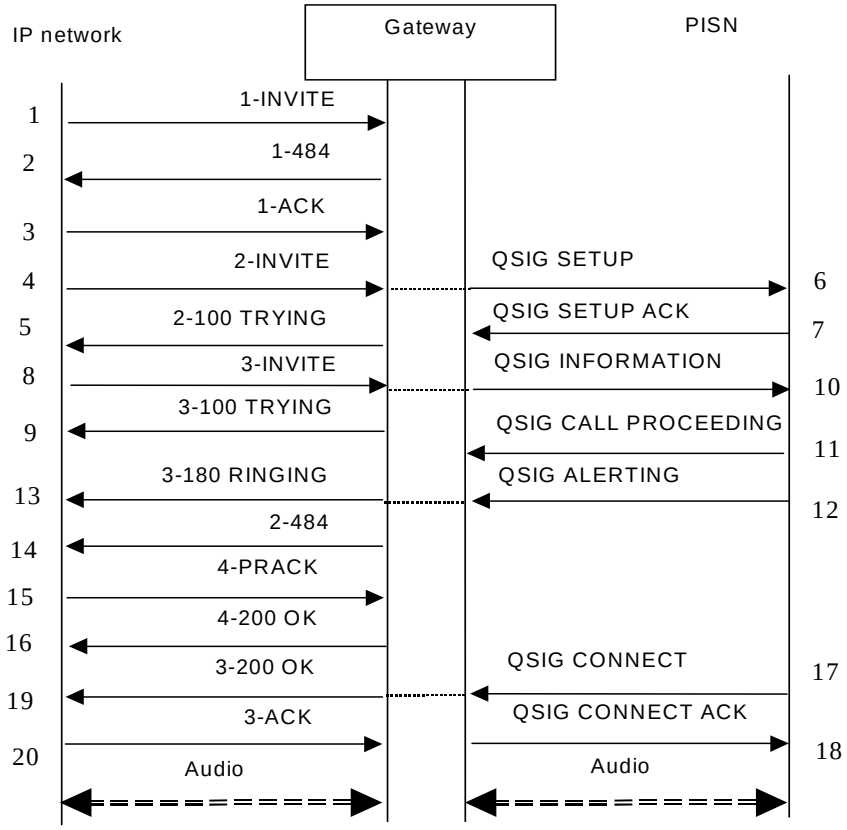


Figure B.6: Typical message sequence for successful call establishment from SIP to QSIG using overlap procedures on both SIP and QSIG

Steps	Comments
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. The gateway sends a SIP 100 (Trying) response to the IP network
3	The IP network acknowledge 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 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 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
16	The gateway sends a SIP 200 (OK) response to acknowledge the SIP PRACK request
17	The PISN sends a QSIG CONNECT message to the gateway when the call is answered
18	The gateway sends a QSIG CONNECT ACKNOWLEDGE message to acknowledge the QSIG CONNECT message
19	The QSIG CONNECT message is mapped to a SIP 200 (OK) response
20	The IP network, upon receiving a SIP INVITE final response (200), will send a SIP ACK request to acknowledge receipt

B.4 Message sequence for call clearing from QSIG to SIP

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

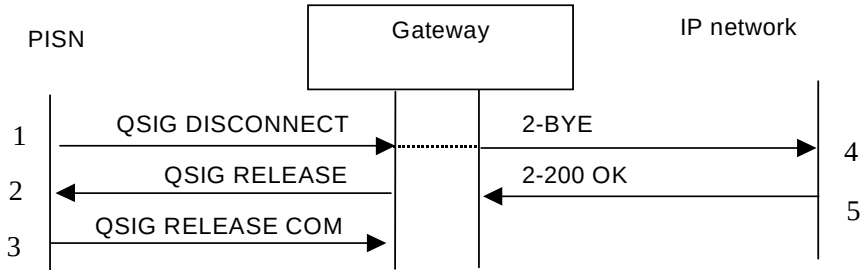


Figure B.7: Typical message sequence for call clearing from QSIG to SIP subsequent to call establishment

Steps	Comments
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

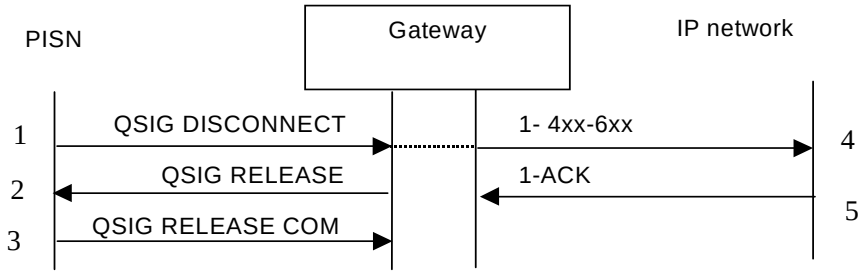


Figure B.8: Typical message sequence for call clearing from QSIG to SIP during establishment of a call from SIP to QSIG (gateway has not sent a final response to the SIP INVITE request)

Steps	Comments
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

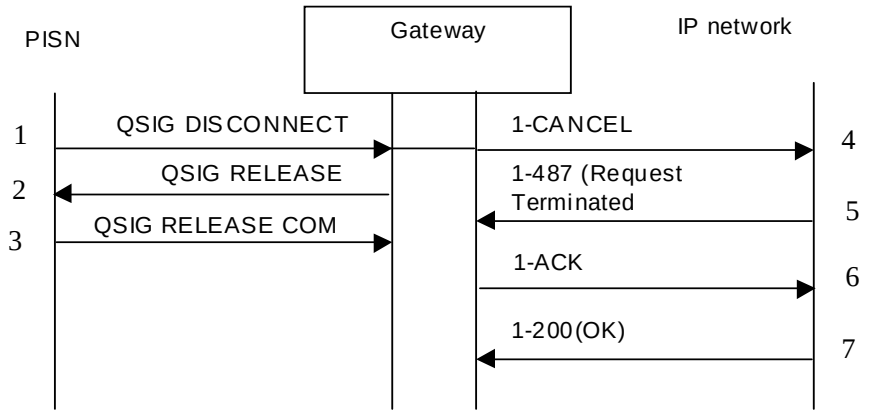


Figure B.9: Typical message sequence for call clearing from QSIG to SIP during establishment of a call from QSIG to SIP (gateway has received a provisional response to the SIP INVITE request but not a final response)

Steps	Comments
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 a provisional response but no final response having been received)
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

B.5 Message sequence for call clearing from SIP to QSIG

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

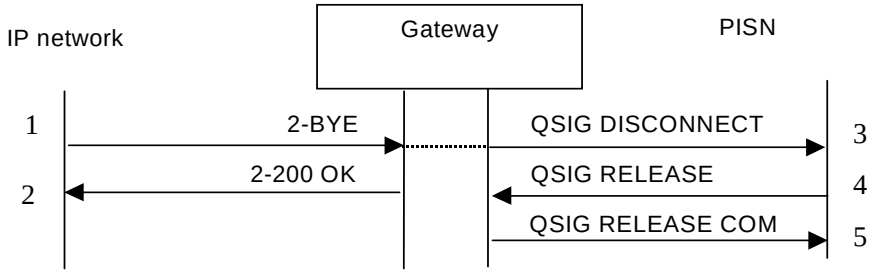


Figure B.10: Typical message sequence for call clearing from SIP to QSIG subsequent to call establishment

Steps	Comments
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

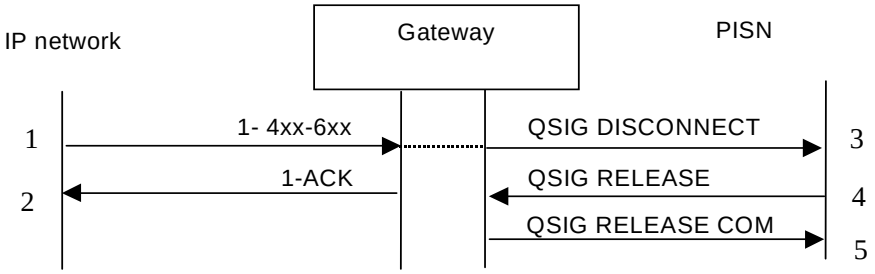


Figure B.11: Typical message sequence for call clearing from SIP to QSIG during establishment of a call from QSIG to SIP (gateway has not previously received a final response to the SIP INVITE request)

Steps	Comments
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

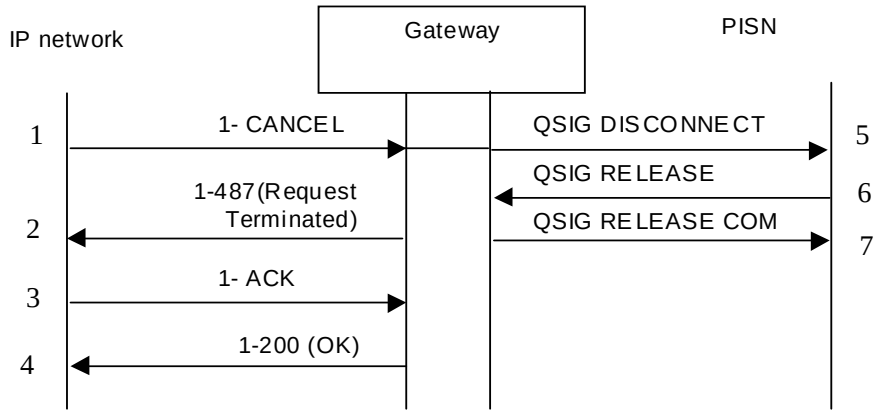


Figure B.12: Typical message sequence for call clearing from SIP to QSIG during establishment of a call from SIP to QSIG (gateway has sent a provisional response to the SIP INVITE request but not a final response)

Steps	Comments
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

Annex C (informative): Security considerations

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 clause 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.

In most respects, the information that is translated from QSIG to SIP has no special security requirements. In order for translated information elements to be used to route requests, they should be legible to intermediaries; end-to-end confidentiality of this data would be unnecessary and most likely detrimental. There are also numerous circumstances under which intermediaries can legitimately overwrite the values that have been provided by translation, and hence integrity over these headers is similarly not desirable.

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. 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 dialling 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.

Some additional risks may result from the SIP response code to QSIG cause value mapping. 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 clause 8.4.4.

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 retargeted 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.

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 the 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 IETF RFC 3261 [14]. 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.

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). 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 to 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.

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. Gateways 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.

History

Document history		
V1.1.1	January 2003	Publication