INTERNATIONAL STANDARD

ISO/IEC 23915

First edition
2005-11-01

Information technology — Telecommunications and information exchange between systems — Corporate Telecommunication Networks — Signalling Interworking between QSIG and SIP — Call Diversion

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Réseaux de télécommunications d'entreprise — Interaction de signalisation entre QSIG et SIP — Déviation d'appel

Reference number
ISO/IEC 23915:2005(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 23915 was prepared by Ecma International (as ECMA-360) and was adopted, under a special “fast-track procedure”, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

Introduction

This International Standard is one of a series of 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.

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

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

Information technology — Telecommunications and information exchange between systems — Corporate Telecommunication Networks — Signalling Interworking between QSIG and SIP — Call Diversion

1 Scope

This document specifies signalling interworking between "QSIG" and the Session Initiation Protocol (SIP) in support of call diversion within corporate telecommunication networks (CN), also known as enterprise networks.

"QSIG" is a signalling protocol that operates between Private Integrated services Network 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 Standards, in particular [1] (call control in support of basic services), [2] (generic functional protocol for the support of supplementary services) and a number of Standards specifying individual supplementary services. Diversion services are specified in [4] and the QSIG signalling protocol in support of these services is specified in [5]. In particular, this signalling protocol signals information about call diversion to the users involved.

SIP is an application layer protocol for establishing, terminating and modifying multimedia sessions. It is typically carried over IP [8], [10]. Telephone calls are considered as a type of multimedia session where just audio is exchanged. SIP is defined in [11]. An extension to SIP provides history information [14] that can be used to signal information about the retargeting of a request, in particular a call establishment request, as it is routed through a network.

This document specifies signalling interworking for call diversion during the establishment of calls between a PISN employing QSIG and a corporate IP network employing SIP. It covers both the impact on SIP of call diversion in the QSIG network and the impact on QSIG of request retargeting in the SIP network. Signalling interworking for call diversion operates on top of signalling interworking for basic calls, which is specified in [6].

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

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

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[1] International Standard ISO/IEC 11572 "Information technology — Telecommunications and information exchange between systems — Private Integrated Services Network — Circuit mode bearer services — Inter-exchange signalling procedures and protocol" (also published by Ecma as Standard ECMA-143).

[2] International Standard ISO/IEC 11582 "Information technology -- Telecommunications and information exchange between systems -- Private Integrated Services Network -- Generic functional protocol for the support of supplementary services -- Inter-exchange signalling procedures and protocol" (also published by Ecma as Standard ECMA-165).

[3] International Standard ISO/IEC 13868 "Information technology -- Telecommunications and information exchange between systems -- Private Integrated Services Network -- Inter-exchange signalling protocol -- Name identification supplementary services" (also published by Ecma as Standard ECMA-164).

[4] International Standard ISO/IEC 13872 "Information technology -- Telecommunications and information exchange between systems -- Private Integrated Services Network -- Specification, functional model and information flows -- Call Diversion supplementary services" (also published by Ecma as Standard ECMA-173).

[5] International Standard ISO/IEC 13873 "Information technology -- Telecommunications and information exchange between systems -- Private Integrated Services Network -- Inter-exchange signalling protocol -- Call Diversion supplementary services" (also published by Ecma as Standard ECMA-174).

[6] International Standard ISO/IEC 17343 "Information technology -- Telecommunications and information exchange between systems -- Corporate telecommunication networks -- Signalling interworking between QSIG and SIP -- Basic services" (also published by Ecma as Standard ECMA-339).

[7] Ecma Technical Report TR/86, "Corporate Telecommunication Networks – User Identification in a SIP/QSIG Environment".

[8] J. Postel, "Internet Protocol", RFC 791.

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

[10] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6)", RFC 2460.

[11] J. Rosenberg, H. Schulzrinne, et al., "SIP: Session initiation protocol", RFC 3261.

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

[13] H. Schulzrinne, D. Oran, G. Camarillo, "The Reason Header field for the Session Initiation Protocol (SIP)", RFC 3326.

[14] M. Barnes "An Extension to the Session Initiation Protocol for Request History Information", draft-ietf-sipping-history-info-03 (work in progress).

3 Terms and definitions

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [9] and indicate requirement levels for compliant implementations.

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

3.1 External definitions

The definitions in [1] and [11] apply as appropriate.

3.2 Other definitions

3.2.1
Call diversion
the act of retargeting a call during call establishment by changing the user identity that is used as the basis for routing to the destination.

3.2.2
Call forwarding busy (CFB)
call diversion invoked because the targeted user is busy.

3.2.3
Call forwarding no reply (CFNR)
call diversion invoked because the targeted user fails to reply within a certain time.

3.2.4
Call forwarding unconditional (CFU)
call diversion invoked for reasons other than those leading to CFB or CFNR.

3.2.5
Corporate telecommunication Network (CN)
sets of privately-owned or carrier-provided equipment that are located at geographically dispersed locations and are interconnected to provide telecommunication services to a defined group of users.

NOTE 1 A CN can comprise a PISN, a private IP network (intranet) or a combination of the two.

NOTE 2 Also known as enterprise network.

3.2.6
Entity A
the entity that provides information about diversion to user A.

3.2.7
Entity B
the entity that invokes diversion for a call targeted at user B.

3.2.8
Entity C
the entity that provides information about diversion to user C.

3.2.9
Gateway
an entity that performs interworking between a PISN using QSIG and an IP network using SIP.

3.2.10
IP network
a network, unless otherwise stated a corporate network, offering connectionless packet-mode services based on the Internet Protocol (IP) as the network layer protocol.

3.2.11
Leg A
the call segment between entity A and the rerouting entity for a call that undergoes diversion.

3.2.12
Leg B
the call segment between the rerouting entity and entity B for a call that undergoes diversion.

3.2.13
Leg C
the call segment between the rerouting entity and entity C for a call that undergoes diversion.

3.2.14
Private Integrated Services Network (PISN)
a CN or part of a CN that employs circuit-switched technology.

3.2.15
Private Integrated services Network eXchange (PINX)
a PISN nodal entity comprising switching and call handling functions and supporting QSIG signalling in accordance with [1].

3.2.16
Rerouting entity
the entity that performs call rerouting on request from entity B and that provides information about diversion to entity A and entity C.

3.2.17
User A
the calling user of a call that undergoes diversion.

3.2.18
User B
the user on behalf of which call diversion is invoked for an incoming call to that user.

3.2.19
User C
the user to which a call is diverted.

4 Abbreviations and acronyms

APDU	Application Protocol Data Unit
CFB	Call forwarding busy
CFNR	Call forwarding no reply
CFU	Call forwarding unconditional
IP	Internet Protocol
PINX	Private Integrated services Network eXchange
PISN	Private Integrated Services Network
SIP	Session Initiation Protocol
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
URI	Universal Resource Identifier

5 Background and architecture for SIP-QSIG interworking

The background and architecture of [6] applies. In addition, the interworking function in the protocol model handles interworking for call diversion services. This involves interworking between the QSIG call diversion protocol specified in [5] and SIP, including the use of SIP request history information as specified in [14].

6 Call diversion

Call diversion, as specified in QSIG and for the purposes of this document, is the act of retargeting a call during call establishment by changing the user identity that is used as the basis for routing to the destination. This can be viewed as being a change of destination user, although in some cases two identities can belong to the same user, e.g., a home number and office number. The three users involved are known as user A (the calling user A), user B (the called user or diverting user) and user C (the diverted-to user).

Reasons for invoking diversion are various and can depend on factors such as the state of the line serving user B, the time of day and the type or identity of user A. It could also be as a result of action by user B in response to the arrival of a call (sometimes known as call deflection). A diversion can occur immediately, i.e. without alerting user B, or after a period of alerting without reply. With the exception of call deflection, diversion requirements must be pre-configured into some equipment acting on behalf of user B, e.g., a telephone, a PINX or a SIP proxy. This could be achieved, for example, by rules-based scripting.

It is often useful or even important that the users involved in a diverted call (user A and user C) are informed of the diversion. This can be particularly important for automata, e.g., for a call diverted to a voice mail system it might be important to indicate to the system that the call has been diverted from user B. However, privacy considerations can sometimes lead to the suppression of this information.

The general model for a call that undergoes diversion is shown in Figure 1. Entity B is the entity that invokes diversion, based on configuration or, in the case of call deflection, on request from user B. The rerouting entity performs call rerouting on instruction from entity B and provides information about the diversion to entity A and entity C. Entity A and entity C handle diversion on behalf of users A and C respectively by providing information about diversion.

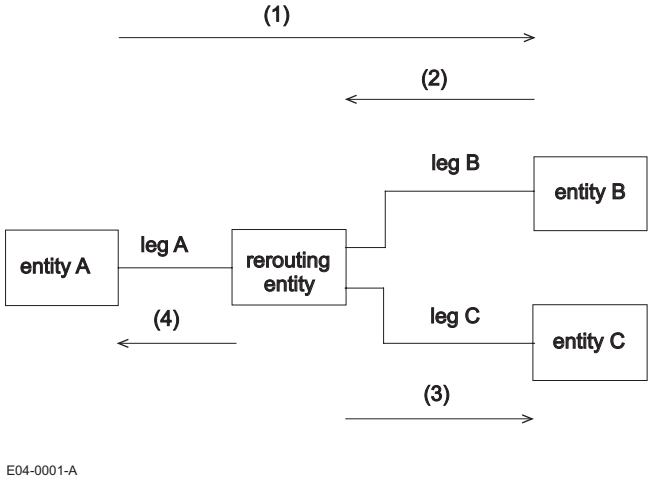

Figure 1 – Logical model for diversion in a QSIG network

From this model it can be seen that there are three call legs:

— leg A between entity A and the rerouting entity (null if these two entities are collocated);

— leg B between entity B and the rerouting entity (null if these two entities are collocated);

— leg C between entity C and the rerouting PINX (null if these two entities are collocated).

Diversion signalling on leg A provides information about diversion to entity A, which can use it to provide information to user A. Diversion signalling on leg B instructs the rerouting entity to carry out rerouting. Diversion signalling on leg C provides information about diversion to entity C, which can use it to provide information to user C.

Figure 1 also illustrates the basic dynamic behaviour:

1. Call establishment from user A as far as entity B.

2. Rerouting request from entity B to the rerouting entity.

3. Rerouted call establishment from the rerouting entity to entity C accompanied by information about the diversion.

4. Information about the diversion from the rerouting entity to entity A.

Diversions can be chained. In this case the rerouted call from the rerouting entity reaches another entity B. The same or a different rerouting entity then reroutes the call towards the new user C.

7 Call diversion in QSIG

Call diversion in QSIG is the act of retargeting a call during call establishment by changing the called party number, which is the user identity used as the basis for routing to the destination. Call diversion in QSIG follows the model described above. Entity A is located in user A's PINX (PINX A), entity B is located in user B's PINX (PINX B) and entity C is located in user C's PINX (PINX C). The rerouting entity is located either at user B's PINX (diversion by forward switching) or at user A's PINX (diversion by rerouting).

Because of potential interactions with other supplementary services, the signalling for which passes transparently through intermediate (Transit) PINXs, the rerouting PINX is constrained to be either PINX B or PINX A. The former case is known as diversion by forward switching, and is analogous to SIP retargeting by a proxy. The latter case is known as diversion by rerouting and is analogous to SIP retargeting by redirection.

For the purposes of QSIG, diversions are classified into one of the following types:

— call forwarding no reply (CFNR) (forwarding as a result of no user reply after alerting user B for a certain time);

— call forwarding busy (CFB) (forwarding as a result of user B's device being busy); and

— call forwarding unconditional (CFU) (forwarding for reasons other than no reply or busy).

NOTE CFU is not necessarily entirely unconditional, since it can depend on other factors, e.g., time of day.

In common with other supplementary services, QSIG signalling for diversion is based on [2] and comprises the following remote operations:

— callRerouting – this confirmed operation is applicable to leg B and provides a means for PINX B to request the rerouting PINX to reroute a call to user C.

— cfnrDivertedLegFailed – this unconfirmed operation is applicable to leg B and indicates failure to establish call leg C subsequent to accepting a callRerouting operation. cfnrDivertedLegFailed applies only to CFNR (i.e. to diversions after user B has been alerted) and indicates to PINX B that user B should continue to be alerted. For other types of diversion leg B is cleared down as soon as the callRerouting operation is accepted, without waiting to see if the call towards user C can be established.

— divertingLegInformation1 – this unconfirmed operation is applicable to leg A and signals information about the diversion to PINX A, including any privacy requirement of user B to prevent disclosure of diversion

information to user A. Note that PINX A can use the information for internal purposes (e.g., call logging) but is trusted not to disclose private information to user A.

— divertingLegInformation2 – this unconfirmed operation is applicable to leg C and signals information about the diversion to PINX C.

— divertingLegInformation3 – this unconfirmed operation is applicable to legs A and C and signals privacy information from PINX C to PINX A. This privacy information provides the possibility for user C to suppress the disclosure of its identity to user A. PINX A must take into account both the privacy information in divertingLegInformation1 and the privacy information in divertingLegInformation3 before disclosing information to user A.

Chained diversions are supported. PINX A receives a divertingLegInformation1 operation for each diversion, but often a divertingLegInformation3 operation only for the final diversion (since this information is not necessarily available until answer). The final PINX C receives a single divertingLegInformation2 operation containing information about the first and last diversions but not intermediate diversions.

8 Call diversion in SIP

Call diversion is not specified for SIP. However, SIP does have the concept of retargeting an INVITE request. This occurs at a proxy, instigated either by the proxy itself or on request from a redirect using a 3xx response. It can also occur at the UAC as a result of a 3xx response from a redirect. Relating this to the model, the rerouting entity for a SIP diversion is the proxy or UAC that retargets the INVITE request. Entity B is either that same proxy or UAC or a redirect that issues a 3xx response. A 3xx response therefore has some synergy with a QSIG callRerouting operation. Entity A is the UAC for the INVITE request and entity C is the UAS of the retargeted-to user.

Retargeting involves changing the Request-URI within the INVITE request, this field being the basis for routing the request.

[11] does not provide signalling support for notifying user A's UA or user C's UA that retargeting has occurred. Additional signalling for this purpose is specified in [14]. This allows a retargeting proxy or UAC to insert a History-Info header into a request when it is forwarded downstream, i.e. on leg C towards entity C. Moreover entity C reflects the received History-Info header back over leg C and leg A towards entity A. In this way, both entity A and entity C receive information about the retarget and can provide this information to their respective users. The History-Info header contains a number of entries, each containing a URI that was a Request-URI at some stage during the routing of the call.

Chained retargets are supported. Entity A and entity C receive information about multiple retargets carried out during the routing of the INVITE request.

History information can be of a sensitive nature, and therefore [14] makes provision for keeping it private. History information subject to privacy must not be passed outside the domain where it originates. Within that domain, the Privacy header [12] with privacy value "history" [14] is used to indicate that either the entire history information or a particular entry is subject to privacy and must not be passed outside the domain.

9 Diversion interworking

9.1 Scenarios for diversion interworking

From the descriptions in clauses 7 and 8 it can be seen that both diversion in QSIG and retargeting, along with the History-Info header, in SIP can be mapped to the call diversion model described in clause 6. Therefore interworking can be described in terms of this model.

Interworking can occur on leg A, on leg B or on leg C. In either case, the rerouting entity can be in either the SIP network or the QSIG network. This leads to 6 interworking scenarios.

— Scenario A1: interworking on leg A, call from QSIG to SIP undergoing retargeting in the SIP network. Entity A in QSIG network, rerouting entity, entity B and entity C in SIP network.

— Scenario A2: interworking on leg A, call from SIP to QSIG undergoing diversion in the QSIG network. Entity A in SIP network, rerouting entity, entity B and entity C in QSIG network.

— Scenario B1: interworking on leg B, call from QSIG to SIP where QSIG network performs rerouting in response to a redirection request from the SIP network. Entity A, entity C and rerouting entity in QSIG network, entity B in SIP network.

— Scenario B2: interworking on leg B, call from SIP to QSIG where SIP network performs retargeting in response to a rerouting request from the QSIG network. Entity A, entity C and rerouting entity in SIP network, entity B in QSIG network.

— Scenario C1: interworking on leg C, call diverted by QSIG network to destination in SIP network. Entity A, entity B and rerouting entity in QSIG network, entity C in SIP network.

— Scenario C2: interworking on leg C, call retargeted by SIP network to destination in QSIG network. Entity A, entity B and rerouting entity in SIP network, entity C in QSIG network.

Call diversion interworking can occur more than once for a given call (chained diversions). The different instances of interworking can be on the same leg (where a leg passes through two or more gateways) or on different legs. For example, entity A could be in a QSIG network, the rerouting entity and entity B could be in a SIP network, and entity C could be in a QSIG network. In this case interworking occurs on leg A (scenario A1) and on leg C (scenario C2). Each instance of interworking conforms to one of the 6 scenarios listed above. No new interworking scenario is introduced as a result.

Chained diversions can introduce mixed scenarios whereby a particular gateway plays the role of one scenario for the one diversion and either the same scenario or a different scenario for the next diversion. For example, consider a gateway performing a scenario C1 role as the result of diversion in the QSIG network (rerouting entity in the QSIG network) to a diverted-to user in the SIP network. The gateway can also perform the role of scenario A1 if a further diversion occurs in the SIP network (rerouting entity in the SIP network).

9.2 Mapping of numbers, names and URIs

Most of the examples shown in clause 10 involve mapping of identifiers, e.g., the identifier representing the diverted to user or the identifier representing the diverting user. In QSIG users are identified by numbers. In SIP users are identified by URIs. Mapping of identifiers is described in detail in [7].

In some cases it may not be possible for a gateway to map a SIP URI to a QSIG number or vice versa. If it is not possible to derive an identifier that is essential for generating a signalling element relating to diversion, unless otherwise stated the call should be allowed to continue without that signalling element.

In some cases it may be possible to map between a QSIG name, as defined in [3], and a SIP URI (e.g., direct mapping between the display-name field of a URI and a QSIG name).

9.3 Derivation of QSIG diversion reasons

The History-Info header contains one or more entries, each containing a retargeted-from URI and, as an optional parameter, a Reason header [13]. The Reason header contains the reason for retargeting. Some of the scenarios require the derivation of a QSIG element of type DiversionReason (indicating CFU, CFB or CFNR), and the Reason header, where available, is the most suitable source of information for this. At present the Reason header can contain either a SIP response code or a Q.850 cause value. Normally, if the Reason header has originated at a native SIP entity as opposed to a gateway, it will contain a SIP response code. Neither a SIP response code nor a Q.850 cause value can directly indicate a reason for diversion (CFU, CFB or CFNR). The Reason header can be extended with reasons from other protocols, so therefore has the potential to include diversion reasons in the future. In the absence of such an extension to the Reason header, or if such diversion reasons are not received, SIP response codes in the Reason header will have to suffice

for deriving a QSIG element of type DiversionReason. There needs to be a default diversion reason value to cater for cases where the Reason header is omitted or where it contains a reason that does not readily suggest a particular diversion reason. The particular mapping will depend on the scenario concerned.

9.3.1 Scenario A1

In QSIG, diversion reason CFNR (from the diversionReason element of the divertingLegInformation 1 invoke APDU) is theoretically meaningful only after ALERTING. Also for the first diversion after ALERTING theoretically the only meaningful diversion reason is CFNR. However, in practice violating these rules will probably not cause problems at downstream PINXs.

SIP response codes do not readily distinguish between the three diversion reason values, and therefore taking account of whether ALERTING has been sent is perhaps beneficial in selecting a more meaningful value.

The following rules SHOULD be applied in the absence of an explicit reason for diversion:

1. If the reason code in the Reason header is 486 (Busy Here) or 600 (Busy Everywhere), map to CFB.

2. Otherwise if ALERTING has previously been sent, map to CFNR.

3. Otherwise map to CFU.

9.3.2 Scenario B1

A diversion reason is required for the rerouteingReason element of the callRerouteing invoke APDU. A History-Info header is not normally contained in the 3xx response (except to denote previous retargets), and therefore there is no Reason header and the only source of information is the 3xx response code. The various 3xx response codes do not readily map to diversion reasons.

A possible future extension would be to include a Reason header in a 3xx response to indicate the diversion reason. In the absence of a Reason header, the following rules SHOULD be applied:

1. If ALERTING has previously been sent, map to CFNR.

2. Otherwise map to CFU.

For populating the originalRerouteingReason element from History-Info header entries received in provisional responses or in the 3xx response, the rules for scenario A1 (9.3.1) apply.

9.3.3 Scenario C2

Diversion reasons are required for the diversionReason element and optionally the originalDiversionReason element of the divertingLegInformation2 invoke APDU. In this scenario it is not possible to determine whether alerting was achieved prior to diversion. The following rules SHOULD be applied in the absence of an explicit reason for diversion:

1. If the reason code in the Reason header is 486 (Busy Here) or 600 (Busy Everywhere), map to CFB.

2. If the reason code in the Reason header is 480 (Temporarily Unavailable), map to CFNR.

3. Otherwise map to CFU.

9.4 Derivation of SIP response codes (scenarios A2 and C1)

QSIG elements of type DiversionReason should ideally be mapped to a corresponding reason in the History-Info header entry, i.e. to the Reason header parameter of the retargeted-from URI. In the absence of an extension to the Reason header for diversion reasons, the diversion reason will need to be mapped to appropriate SIP response codes. The following rules SHOULD be applied.

1. Map CFU to 302 (Moved Temporarily).

2. Map CFB to 486 (Busy Here).

3. Map CFNR to 480 (Temporarily Unavailable).

In the absence of an element from which to derive a SIP response code, 302 (Moved Temporarily) SHOULD be used.

9.5 Mapping the QSIG diversion counter

QSIG has a mandatory diversionCounter element in a callRerouteing invoke APDU and in a divertingLegInformation2 invoke APDU. In each case the diversionCounter element contains the number of diversions that have occurred up to and including the present diversion. This allows a PINX to place a limit on the number of diversions that a call can undergo, and in particular this is a way of preventing infinite loops. A PINX can reject a further diversion if a configurable limit has been reached.

SIP does not have the direct equivalent. The number of retargets can be deduced from the number of History-Info header entries, subject to this information being provided. Infinite looping is prevented by means of the Max-Forwards header, which limits the number of proxies a request can pass through. An initial value is placed in this header by the UAC, and the value is decremented at each proxy.

The fact that each signalling protocol has its own mechanism for preventing loops, means that loops will be prevented within the respective networks. However, without appropriate interworking between the two, looping backwards and forwards between a QSIG network and a SIP network is possible with scenarios C1 and C2. The different approaches in the two signalling protocols prevent a perfect solution, but the requirements and recommendations in 9.11 and 9.12 for mapping from and to the diversionCounter element in a divertingLegInformation2 invoke APDU are aimed at reducing the chances of looping.

Because scenarios B1 and B2 involve redirection, looping is prevented by the mechanisms that exist in the network that provides the entity (i.e. QSIG mechanisms for scenario B1 and SIP mechanisms for scenario B2). Therefore mapping to and from the diversionCounter element in a callRerouteing invoke APDU is less critical. Requirements are specified in 9.9 and 9.10.

9.6 Privacy considerations

Both QSIG and SIP adopt a similar principle for handling information subject to privacy. Such information can be passed within a single domain marked as subject to privacy, but MUST NOT be passed outside that domain.

A gateway can receive information marked as subject to privacy from a QSIG entity in the same domain. It MUST NOT pass this on to a SIP entity that is not in the same domain or not capable of providing a privacy service as defined in [12]. When passing on to a SIP entity in the same domain and capable of providing a privacy service, the information MUST be marked as subject to privacy.

A gateway can receive information marked as subject to privacy from a SIP entity in the same domain. It MUST NOT pass this on to a QSIG entity that is not in the same domain. When passing on to a QSIG entity in the same domain, the information MUST be marked as subject to privacy.

9.7 Interworking for scenario A1

The gateway SHALL behave as specified in [6] for a call from QSIG to SIP, modified in accordance with the following.

9.7.1 Transmitting a SIP INVITE request

When transmitting a SIP INVITE request as a result of receiving a QSIG SETUP message, the gateway SHALL include HistInfo in a Supported header.

NOTE If the QSIG SETUP message contains a divertingLegInformation2 invoke APDU, scenario C1 (see 9.11) also applies.

9.7.2 Receipt of a SIP 1xx or 2xx response

On receipt of a SIP 1xx or 2xx response containing a History-Info header, the gateway SHALL select any URIs in the History-Info header except for:

- the first URI;
- any duplicated URIs; and
- any URIs that have been received in any earlier 1xx responses.

For each selected URI, if any, the gateway SHALL attempt to generate a divertingLegInformation1 invoke APDU. If as a result of the SIP 1xx or 2xx response the gateway transmits a QSIG ALERTING, PROGRESS or CONNECT message, the gateway SHALL include any generated divertingLegInformation1 invoke APDUs in that message. Otherwise the gateway SHALL include these APDUs in a QSIG FACILITY message. If there is more than one APDU transmitted, the order in the QSIG message SHALL be the same as the order of the corresponding URIs in the History-Info header.

The gateway SHALL attempt to derive a nominatedNr (number) for inclusion in a divertingLegInformation1 invoke APDU from the corresponding URI in the History-Info header (see 9.2). If unable to derive a number, the gateway SHALL NOT generate an APDU based on that URI.

The gateway SHALL derive a diversionReason for inclusion in a divertingLegInformation1 invoke APDU from information associated with the URI preceding the corresponding URI in the History-Info header.

If the corresponding URI in the History-Info header contains a parameter "Privacy=history" or if the response contains a Privacy header with priv-value "history", behaviour depends on whether the gateway trusts the QSIG network to honour privacy, i.e. whether the QSIG network is in the same domain. If not, the gateway SHALL NOT generate an APDU based on that URI.

If a transmitted QSIG message contains one or more divertingLegInformation1 invoke APDUs, the gateway SHALL also include in the same message a divertingLegInformation3 invoke APDU. The presentationAllowedIndicator element SHOULD have the value TRUE. Element redirectionName MAY be included, in which case it SHALL contain a name derived from the last URI in the received History-Info header.

9.7.3 Receipt of a SIP 4xx, 5xx or 6xx response

On receipt of a SIP 4xx, 5xx or 6xx response containing a History-Info header and resulting in the transmission of a QSIG DISCONNECT message, the gateway SHALL attempt to generate divertingLegInformation1 invoke APDUs and a divertingLegInformation3 invoke APDU as it would when receiving a 1xx or 2xx response (see 9.7.2). If any APDUs have been generated the gateway SHALL transmit them in a FACILITY message prior to transmitting the DISCONNECT message.

If instead of transmitting a QSIG DISCONNECT message the gateway transmits a further SIP INVITE request, the gateway MAY transmit a QSIG FACILITY as above or MAY await further information in response to the new INVITE request.

9.8 Interworking for scenario A2

The gateway SHALL behave as specified in [6] for a call from SIP to QSIG, modified in accordance with the following.

9.8.1 Receipt of a SIP INVITE request

On receipt of a SIP INVITE request, the gateway SHALL record the presence or absence of HistInfo in a Supported header. If absent, the gateway SHALL NOT include a History-Info header in any responding message. If present, the gateway shall also store any History-Info header received in the SIP INVITE request for inclusion in SIP responses.

NOTE If a History-Info header is present and contains more than one APDU, scenario C2 (see 9.12) also applies.

9.8.2 Receipt of a QSIG divertingLegInformation1 invoke APDU

On receipt of a QSIG divertingLegInformation1 invoke APDU in a QSIG ALERTING, PROGRESS, FACILITY or CONNECT message, if element subscriptionOption has value notificationWithDivertedToNr and the gateway is able to derive a URI from the nominatedNr element the gateway SHALL store the URI together with the diversionReason as a candidate URI for inclusion in a History-Info header. The gateway MAY also store this information and mark it as subject to privacy if element subscriptionOption has a different value (indicating privacy) and the SIP response is to be sent to an entity in the same domain capable of providing a privacy service as defined in [12]. Each candidate URI SHALL be stored along with any existing candidate URIs derived from previous QSIG messages. If there is a divertingLegInformation3 invoke APDU in the same message, the rules of 9.8.3 apply after storing any candidate URIs.

9.8.3 Receipt of a QSIG divertingLegInformation3 invoke APDU

On receipt of QSIG divertingLegInformation3 invoke APDU with value TRUE in element presentationAllowedIndicator in a QSIG ALERTING, PROGRESS, FACILITY or CONNECT message, the gateway SHALL mark any candidate URIs as confirmed URIs. The gateway MAY also augment the most recent URI with information derived from element redirectionName in the divertingLegInformation3 invoke APDU. On receipt of QSIG divertingLegInformation3 invoke APDU with value FALSE in element presentationAllowedIndicator in a QSIG ALERTING, PROGRESS, FACILITY or CONNECT message, the gateway SHALL mark any candidate URIs as subject to privacy if the SIP response will be sent to an entity in the same domain capable of providing a privacy service as defined in [12], but otherwise the gateway SHALL delete any candidate URIs.

9.8.4 Transmitting a SIP response in which History-Info is allowed

When transmitting a SIP non-2xx response in which a History-Info header is allowed, the gateway MAY include a History-Info header if HistInfo was indicated in the Supported header in the SIP INVITE request. When transmitting a SIP 2xx response, the gateway SHALL include a History-Info header in any of the following circumstances, provided HistInfo was indicated in the Supported header in the SIP INVITE request:

— a History-Info header was received in the SIP INVITE request; or

— a History-Info header has been sent in a previous SIP provisional response; or

— there is at least one confirmed URI available.

The gateway SHALL build a transmitted History-Info header based on the following:

— the most recently transmitted History-Info header in a SIP provisional response to the SIP INVITE request, if applicable;

— else, the History-Info header received in the SIP INVITE request, if applicable;

— else a new History-Info header comprising an entry that includes the URI received in the Request-URI of the SIP INVITE request.

In each case the gateway SHALL append to the History-Info header an entry for each of the confirmed URIs stored, if any, in the order in which the corresponding QSIG divertingLegInformation1 invoke APDUs were

received. The gateway SHALL derive from the diversionReason associated with each URI a SIP Reason header for inclusion in the preceding History-Info entry. If any of the confirmed URIs are marked as subject to privacy, the gateway SHALL also include in the response a Privacy header with priv-value "history" to prevent the information being disclosed outside the domain. Finally, the gateway SHALL delete candidate URIs from storage. In the case of a SIP provisional response the gateway SHALL store the transmitted History-Info entries for use in the SIP final response.

NOTE 1 For example, if the SIP INVITE request contained URI1 and URI2, no History-Info header has been transmitted in a previous SIP response message, and there is one confirmed URI, URI3, stored, the transmitted History-Info header should comprise entries containing URI1, URI2 and URI3, with the diversionReason stored against URI 3 forming the SIP Reason header embedded in URI2.

NOTE 2 The QSIG Connected number information element can contain a different number from that in nominatedNr in the most recent divertingLegInformation1 invoke APDU. This does not necessarily imply a further diversion but could instead be the result of some other behaviour in the QSIG network (e.g., call pick-up, line hunting). No attempt should be made to build an additional History-Info entry based on the QSIG Connected number information element.

9.9 Interworking for scenario B1

The gateway SHALL behave as specified in [6] for a call from QSIG to SIP, modified in accordance with the following.

9.9.1 Receipt of a SIP 3xx response

On receipt of a SIP 3xx response to a SIP INVITE request, the gateway MAY initiate diversion by rerouting in the QSIG network. The decision to do this can depend on several factors, e.g.,

— the ability to derive a QSIG number to divert to;

— the particular 3xx response code;

— routing knowledge;

— policy;

— the presence of more than one URI in the Contact header;

— knowledge of previous retargeting history;

— privacy considerations, which might prevent the submission of certain information that is mandatory in a QSIG callRerouteing invoke APDU.

The gateway MAY defer initiation of diversion by rerouting in the QSIG network until retargeting in the SIP network has been attempted and has failed, in which case the gateway MAY take account of the reason for failure when making its decision.

If the gateway does not initiate diversion by rerouting in the QSIG network, it SHALL either initiate clearing of the call in the QSIG network by transmitting a QSIG DISCONNECT message or retarget the SIP INVITE request. In the latter case, scenario A1 will apply.

To initiate diversion by rerouting in the QSIG network, the gateway SHALL transmit a QSIG FACILITY message containing a CallRerouteing invoke APDU constructed as follows:

— the reroutingReason element SHOULD be derived from the SIP 3xx response code (see 9.3.2);

— the originalReroutingReason element MAY be included if the gateway is aware of a previous diversion and its reason (e.g., if a divertingLegInformation2 invoke APDU was present in the QSIG SETUP message or one or more History-Info entries have been received in a provisional response or the 3xx final response);

— the calledAddress element SHALL contain the QSIG number derived from a URI in the Contact header;

— the diversionCounter element SHALL contain the value 1 if the gateway is unaware of any previous diversion and SHOULD be a greater value if the gateway is aware of any previous diversions (e.g., if a divertingLegInformation2 invoke APDU was present in the QSIG SETUP message or a History-Info header has been received in a provisional response prior to the 3xx final response);

— the pSS1InfoElement element SHALL contain QSIG information elements in accordance with [6];

— the lastReroutingNr element SHALL be included and SHOULD be the number from the Called party number information element in the received QSIG SETUP message unless the gateway is aware of any more recent target (e.g., from a received History-Info header in a SIP provisional response prior to the SIP 3xx response);

— element subscriptionOption SHALL be included and SHOULD have value notificationWithDivertedToNr, unless the gateway is aware of privacy requirements that dictate a different value;

— element callingNumber SHALL be included in accordance with [5];

— element callingName MAY be included in accordance with [5];

— element originalCalledNr MAY be included, based either on the number in the Called party number information in the QSIG SETUP message or element originalCalledNr in a divertingLegInformation2 invoke APDU in the QSIG SETUP message, in either case subject to the number being different from that in lastReroutingNr;

— element redirectingName MAY be included if the gateway is aware of a name associated with the number in lastReroutingNr;

— element originalCalledName MAY be included if the gateway is aware of a name associated with the number in originalCalledNr.

9.9.2 Receipt of a QSIG DISCONNECT or FACILITY message containing a callRerouteing return result APDU

On receipt of a QSIG DISCONNECT message containing a callRerouteing return result APDU, the gateway SHALL continue to release the QSIG call.

On receipt of a QSIG FACILITY message containing a callRerouteing return result APDU, the gateway SHALL continue to maintain the QSIG call.

NOTE In the case of CFU or CFB, a QSIG DISCONNECT message should be received shortly after the QSIG FACILITY message. However, in the case of CFNR the QSIG DISCONNECT message will be delayed until the diverted call has been established (but not necessarily answered). The gateway should not attempt to accelerate the clearing of the leg because that will cause the QSIG rerouting PINX to clear the whole call. If the diverted call fails to be established the gateway will receive a cfnrDivertedLegFailed invoke APDU.

9.9.3 Receipt of a QSIG FACILITY message containing a callRerouteing return error APDU

On receipt of a QSIG FACILITY message containing a callRerouteing return error APDU, the gateway SHALL either initiate clearing of the call in the QSIG network by transmitting a QSIG DISCONNECT message or retarget the SIP INVITE request. In the latter case, scenario A1 will apply.

9.9.4 Receipt of a QSIG FACILITY message containing a cfnrDivertedLegFailed invoke APDU

On receipt of a QSIG FACILITY message containing a cfnrDivertedLegFailed invoke APDU, the gateway SHALL either initiate clearing of the call in the QSIG network by transmitting a QSIG DISCONNECT message or retarget the SIP INVITE request. In the latter case, scenario A1 will apply.

NOTE The QSIG expectation is that alerting will continue at user B if diversion fails, but SIP does not support this.

9.10 Interworking for scenario B2

The gateway SHALL behave as specified in [6] for a call from SIP to QSIG, modified in accordance with the following.

9.10.1 Receipt of a QSIG FACILITY message containing a CallRerouteing invoke APDU

On receipt of a QSIG FACILITY message containing a CallRerouteing invoke APDU, the gateway MAY transmit a SIP 3xx response. The decision to do this can depend on several factors, e.g.,

— the ability to derive a SIP URI for inclusion in the Contact header;

— the particular type of diversion (CFU, CFB or CFNR);

— routing knowledge;

— policy;

— knowledge of previous retargeting history;

— privacy considerations, which might prevent the transmission of a SIP 3xx response.

The gateway MAY defer transmission of a SIP 3xx response until diversion by rerouting in the QSIG network has been attempted and has failed, in which case the gateway MAY take account of the reason for failure when making its decision.

If the gateway does not transmit a SIP 3xx response, it SHALL either act as the rerouting PINX and attempt diversion by rerouting in the QSIG network or reject the rerouting request by transmitting a QSIG FACILITY message containing a callRerouteing return error APDU. In the former case, scenario A2 will apply instead of B2.

If the gateway transmits a 3xx response, it SHALL select the particular response code in accordance with 9.4. The gateway SHALL include in the SIP 3xx response a Contact header containing a URI derived from the calledAddress element in the QSIG callRerouteing invoke APDU. In addition, the gateway SHALL transmit either a QSIG FACILITY message containing a callRerouteing return result APDU followed by a QSIG DISCONNECT message or a QSIG DISCONNECT message containing a callRerouteing return result APDU.

NOTE Other information in the QSIG callRerouteing invoke APDU is not of any use in this situation. In particular, use cannot be made of the diversionCounter element value for indicating previous diversions in the QSIG network to the SIP network, since there is insufficient information to derive History-Info entries to reflect these previous diversions.

9.11 Interworking for scenario C1

The gateway SHALL behave as specified in [6] for a call from QSIG to SIP, modified in accordance with the following.

This scenario applies if the gateway sends a SIP INVITE request as a result of receiving a QSIG SETUP message containing a divertingLegInformation2 invoke APDU.

9.11.1 Receipt of a QSIG SETUP message containing a divertingLegInformation2 invoke APDU

The gateway SHALL include HistInfo in a Supported header in the INVITE request.

If the divertingLegInformation2 invoke APDU contains an originalCalledNr element, the gateway SHOULD attempt to derive a URI from that number. When deriving the URI, the gateway MAY also take into account the originalCalledName element, if present in the divertingLegInformation2 invoke APDU. If a URI is derived,

the gateway SHALL include a Reason parameter derived from the originalDiversionReason element, if present in the divertingLegInformation2 invoke APDU.

If the divertingLegInformation2 invoke APDU contains divertingNr element, the gateway SHOULD attempt to derive a URI from that number. When deriving the URI, the gateway MAY also take into account the redirectingName element, if present in the divertingLegInformation2 invoke APDU. If a URI is derived, the gateway SHALL include a Reason parameter derived from the diversionReason element in the divertingLegInformation2 invoke APDU.

The gateway SHALL include a History-Info header containing the following:

— if available, an entry containing a URI derived from the originalCalledNr element of the divertingLegInfo2 invoke APDU;

— if available, an entry containing a URI derived from the divertingNr element of the divertingLegInfo2 invoke APDU;

— an entry containing the URI used in the Request-URI field of the INVITE request.

9.11.2 Transmitting a QSIG CONNECT message

If scenario C1 applies, when transmitting a QSIG CONNECT message the gateway SHALL include a divertingLegInformation3 invoke APDU unless one has already been sent in accordance with scenario A1 (9.7). The presentationAllowedIndicator element SHOULD have the value TRUE.

9.12 Interworking for scenario C2

The gateway SHALL behave as specified in [6] for a call from SIP to QSIG, modified in accordance with the following.

This scenario applies if the gateway sends a QSIG SETUP message as a result of receiving a SIP INVITE request containing two or more URIs in a History-Info header.

9.12.1 Transmitting a QSIG SETUP message

On receipt of a SIP INVITE request containing two or more URIs in a History-Info header, the gateway SHALL attempt to derive a number and optionally a name (last diverting number and name) from the penultimate URI in the History-Info header. If successful, the gateway SHALL also derive a diversion reason (last diversion reason), based on the Reason parameter of that same URI, if present.

If a last diverting number has been derived and if the History-Info header contains more than two URIs, the first URI being different from the penultimate URI, the gateway SHALL attempt to derive a number and optionally a name (original diverting number and name) from the first URI in the History-Info header. If successful, the gateway SHALL also derive a diversion reason (original diversion reason), based on the Reason parameter of that same URI, if present.

If a last diverting number has been derived, the gateway SHALL include in the QSIG SETUP message a divertingLegInformation2 invoke APDU containing the following elements:

— diversionCounter containing the number of History-Info header entries minus 1;

— diversionReason containing the last diversion reason;

— divertingNr containing the last diverting number;

— redirectingName containing the original diverting name, if available (otherwise omitted).

In addition, if an original diverting number has been derived, the gateway SHALL include the following elements in the divertingLegInformation2 invoke APDU:

— originalDiversionReason containing the original diversion reason;

— originalCalledNr containing the original diverting number;

— orginalCalledName containing the original diverting name, if available (otherwise omitted).

9.12.2 Receipt of a QSIG message containing a divertingLegInformation3 invoke APDU

If the gateway receives a QSIG message containing a divertingLegInformation3 invoke APDU, the gateway SHALL record this fact until it sends a SIP final response. Otherwise, within the context of this scenario, the gateway SHOULD ignore a divertingLegInformation3 invoke APDU. However, processing in accordance with scenario A2 (9.8) may be required.

9.12.3 Sending History-Info in a response

When sending a SIP response, the gateway SHALL NOT include a History-Info header under any of the following circumstances:

— the INVITE request did not contain HistInfo in the Supported header;

— no QSIG divertingLegInformation3 invoke APDU has been received (and therefore the privacy situation is uncertain); or

— a QSIG divertingLegInformation3 invoke APDU has been received with value FALSE in element presentationAllowedIndicator, unless the SIP response is being sent to an entity within the same domain.

If a QSIG divertingLegInformation3 invoke APDU has been received with value FALSE in element presentationAllowedIndicator and the SIP response is being sent to an entity in the same domain capable of providing a privacy service as defined in [12], the gateway MAY include a History-Info header, in which case it SHALL also include a Privacy header with priv-value "history" to prevent the information being disclosed outside the domain.

In other circumstances the gateway SHALL send a History-Info header in a 2xx response and MAY send a History-Info header in any other response (except 100).

The History-Info header SHALL reflect information received in the History-Info header in the INVITE request. However, processing in accordance with scenario A2 (9.8) may be required, perhaps leading to additional information in the History-Info header.

10 Example message sequences

In the interests of keeping the diagrams simple, ACK and PRACK are not shown.

The following notation is used for diversion information within QSIG messages:

— xxx.inv – invoke application protocol data unit (APDU) of operation xxx.

— xxx.res – return result APDU of operation xxx.

— xxx.err – return error APDU of operation xxx.

10.1 Scenario A1

Call from QSIG to SIP undergoes diversion in SIP network.

10.1.1 Successful call – history information in 200 response

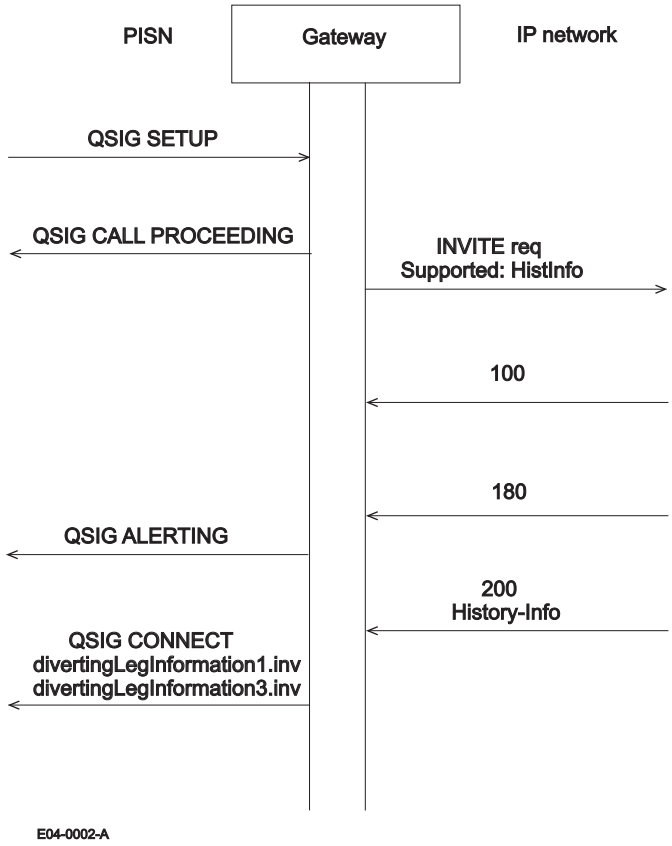

Figure 2 – Example of scenario A1 – successful call – history information in 200 response

NOTE 1 Normally the first targeted-to URI in the History-Info header will be the original targeted-to URI (the Request-URI in the INVITE request sent by the gateway). The Reason header in this URI should be used to derive the diversionReason in divertingLegInformation1.inv (see 9.3). The second targeted-to URI should be used to derive the number in divertingLegInformation1.inv.

NOTE 2 If there is more than one targeted-to URI (in addition to the original targeted-to URI) it would be possible to include more than one divertingLegInformation1 invoke in the CONNECT message.

10.1.2 Successful call – history information in provisional response

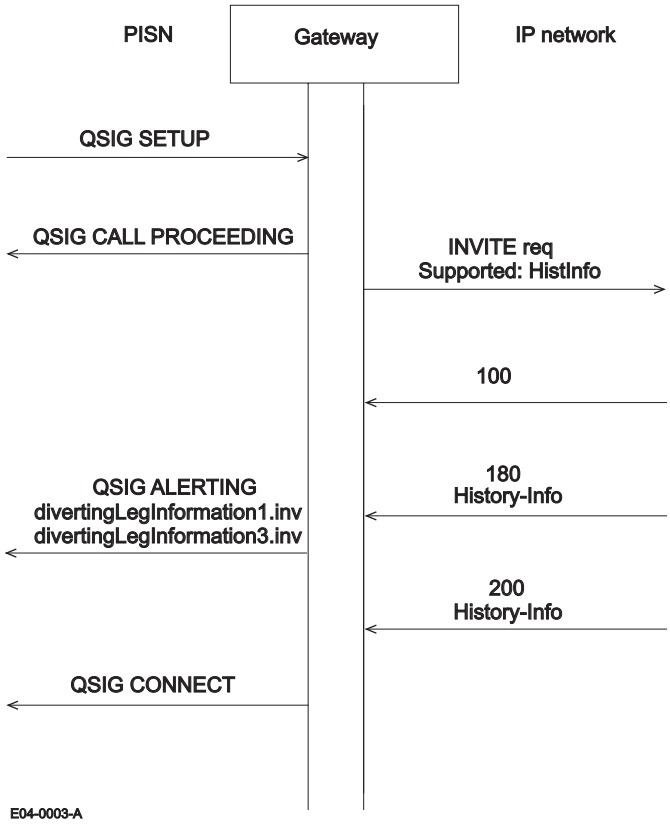

Figure 3 – Example of scenario A1 – successful call – history information in provisional response

NOTE 1 This shows History-Info arriving in a 180 response. An alternative would be receipt of History-Info in a 183 response, in which case the divertingLegInformation1.inv would be sent in the PROGRESS message (if a PROGRESS message is to be sent) or in a FACILITY message.

NOTE 2 Normally the first targeted-to URI in the History-Info header will be the original targeted-to URI (the Request-URI in the INVITE request sent by the gateway). The Reason header in this URI should be used to derive the diversionReason in divertingLegInformation1.inv (see 9.3). The second targeted-to URI should be used to derive the number in divertingLegInformation1.inv.

NOTE 3 If there is more than one targeted-to URI (in addition to the original targeted-to URI) it would be possible to include more than one divertingLegInformation1 invoke in the ALERTING (or PROGRESS or FACILITY) message.

NOTE 4 The divertingLegInformation3.inv is shown as being sent in the same message as the divertingLegInfo1.inv. This is because SIP has no means of indicating later that the retargeted-to URI in the History-Info header is not to be disclosed to the calling user. In a QSIG environment the divertingLegInformation3.inv cannot be sent until it is clear that the diverted-to user does not require privacy, and therefore it is often deferred until the CONNECT message. A gateway could choose to defer until the CONNECT message, but there is no need.

NOTE 5 If further provisional responses are received with extended information in the History-Info header, the additional targeted-to URIs can be used to generate further divertingLegInformation1 and divertingLegInformation3 invokes.

NOTE 6 Another History-Info header will be present in the 200 OK response. Unless this contains additional targeted-to URIs, no divertingLegInformation1.inv should be included in the CONNECT message.

10.1.3 Failed call

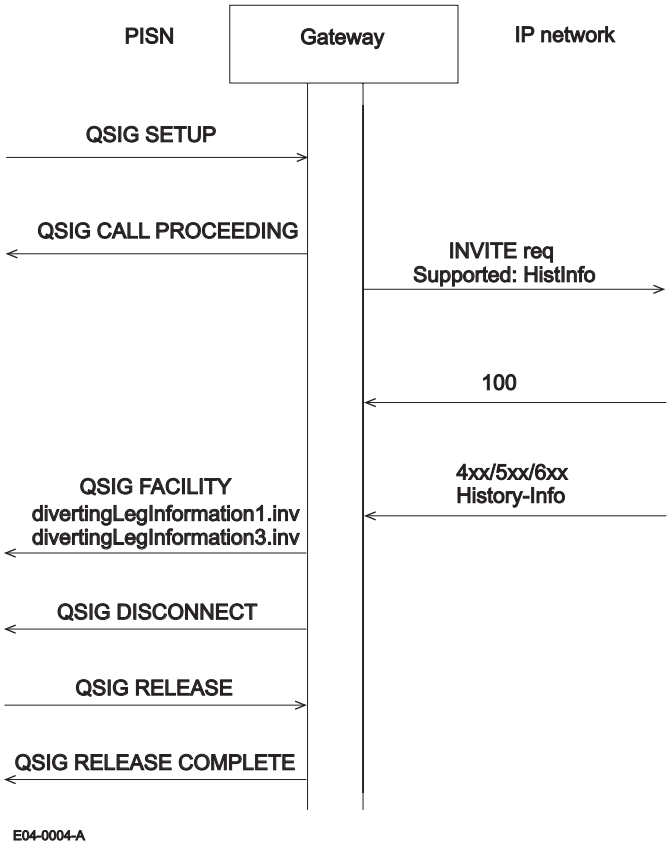

Figure 4 – Example of scenario A1 – failed call

10.2 Scenario A2

Call from SIP to QSIG undergoes diversion in QSIG network.

10.2.1 Successful call – CFU or CFB

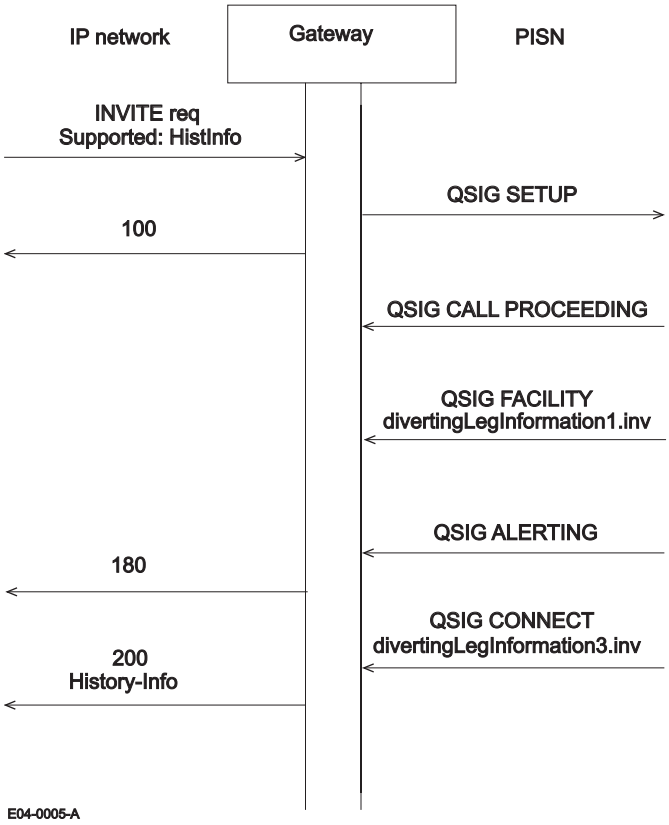

Figure 5 – Example of scenario A2 (CFU or CFB)

NOTE 1 In the History-Info header, the first targeted-to URI should be the Request-URI in the received INVITE request and the second targeted-to URI should be derived from the number in the divertingLegInformation1.inv. The diversionReason needs to be reflected in the Reason header in the first targeted-to URI in the History-Info header (see 9.4). If more than one divertingLegInformation1.inv have been received in the same QSIG message or previous QSIG messages, additional targeted-to URIs can be derived, resulting in additional entries in the History-Info header.

NOTE 2 History-Info should be omitted if Supported: HistInfo is not present in the INVITE request.

NOTE 3 If information in the divertingLegInformation1 or divertingLegInformation3 invoke indicates that privacy is required for user C's number, then this will limit information that can be provided in the History-Info header unless sent within the same domain.

NOTE 4 Until the divertingLegInformation3.inv arrives, the gateway does not know whether privacy restrictions apply, and therefore History-Info cannot be sent earlier. If divertingLegInformation3.inv arrives before the CONNECT, History-Info may be sent in a provisional response (e.g., in 180 or 181).

NOTE 5 If after sending a History-Info header in a provisional response, a further divertingLegInformation1.inv arrives, a further History-Info header can be sent subject to the rules above. This header should contain all entries in the previous History-Info header and the entry derived from the latest divertingLegInformation1.inv.

NOTE 6 Even if History-Info has been sent in a provisional response and no further divertingLegInformation1.inv has been received, the 200 response should contain a History-Info header containing all URIs in the previous History-Info header.

10.2.2 Successful call – CFNR

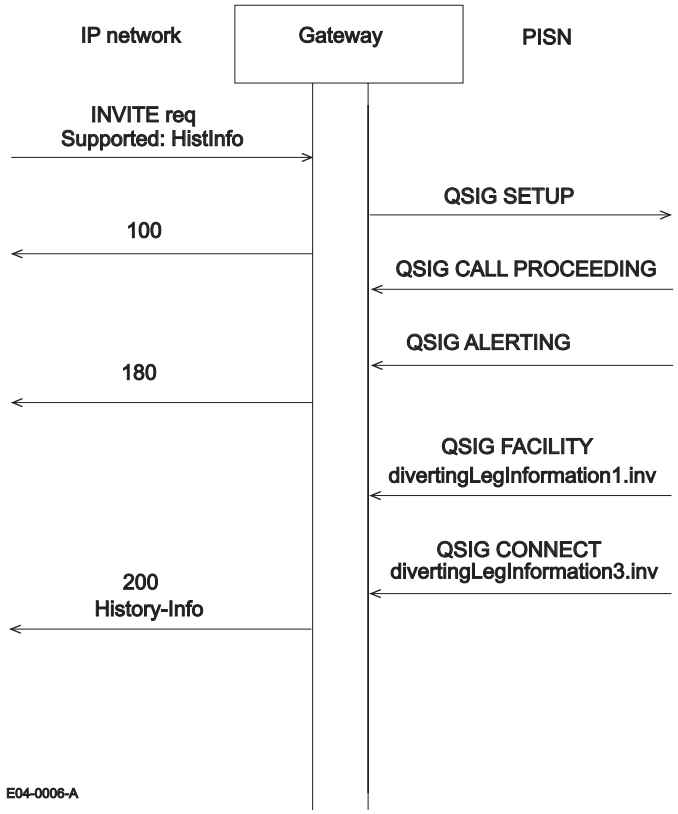

Figure 6 – Example of scenario A2 (CFNR)

10.3 Scenario B1

Call from QSIG to SIP redirected back to QSIG network.

10.3.1 Successful diversion – CFU or CFB

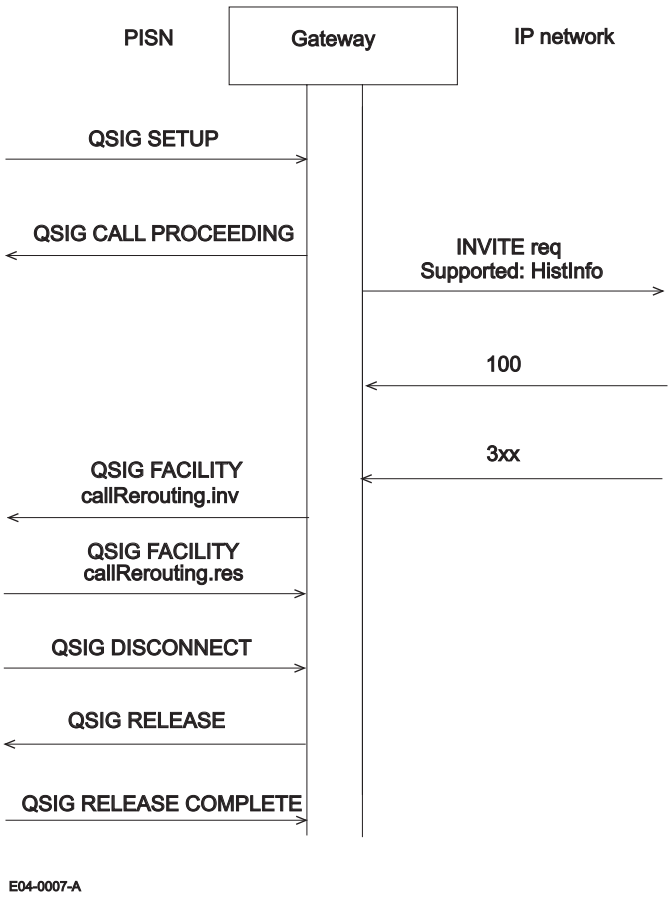

Figure 7 – Example of scenario B1 (call forwarding unconditional or call forwarding busy)

NOTE 1 This scenario applies only if the gateway does not act as a rerouting proxy and issue a further INVITE request to the contact URI(s) supplied. The decision to do this might be based on the value of the contact URI(s). If the gateway acts as a rerouting proxy, scenario A1 applies to the sending of diversion information towards the calling user.

NOTE 2 For derivation of the reroutingReason in callRerouting.inv, see 9.3.

NOTE 3 The number in callRerouting.inv should be derived from the Contact address header in the 3xx response. If there is more than one contact address, one must be selected, e.g., the first one that can be mapped to a number.

NOTE 4 If the reroutingReason in callRerouting invoke indicates CFNR, the QSIG DISCONNECT will not arrive until the diverted call has been successfully established (alerting). The gateway should not attempt to accelerate the clearing of the leg because that will cause the QSIG rerouting PINX to clear the whole call.

NOTE 5 The subscriptionOption in the callRerouting.inv should indicate no restriction, which means that user B has not requested any restriction on providing diversion information to user A. If privacy of this nature is required, SIP redirection is an inappropriate mechanism.

10.3.2 Successful diversion – CFNR

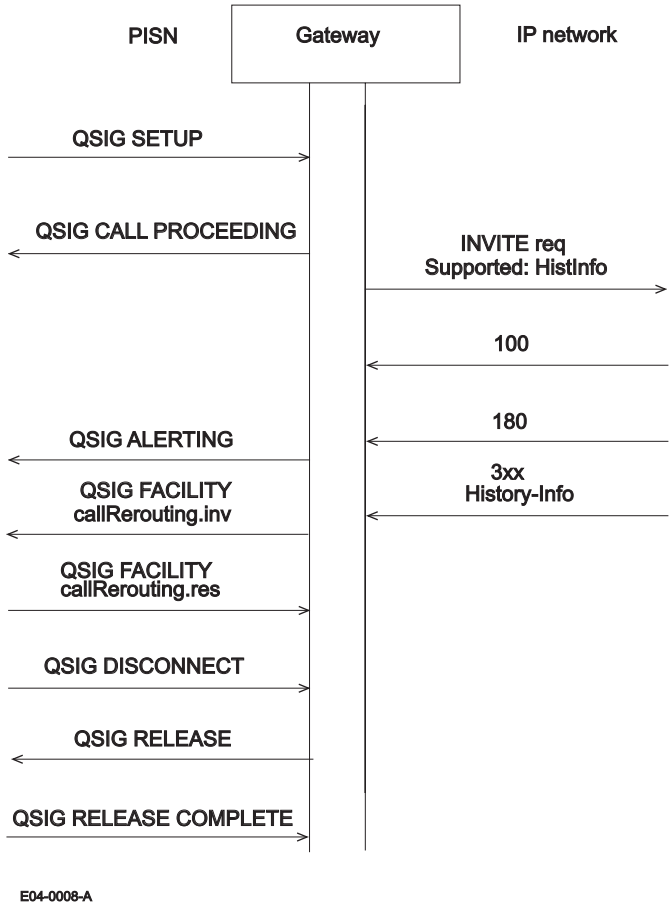

Figure 8 – Example of scenario B1 (call forwarding no reply)

NOTE 1 For derivation of the diversionReason in callRerouting.inv, see 9.3.

NOTE 2 Because this is CFNR, the QSIG DISCONNECT will not arrive until the diverted call has been successfully established (alerting). The gateway should not attempt to accelerate the clearing of the leg because that will cause the QSIG rerouting PINX to clear the whole call.

NOTE 3 The subscriptionOption in the callRerouting.inv should indicate no restriction.

10.3.3 Failure – callRerouting.err received

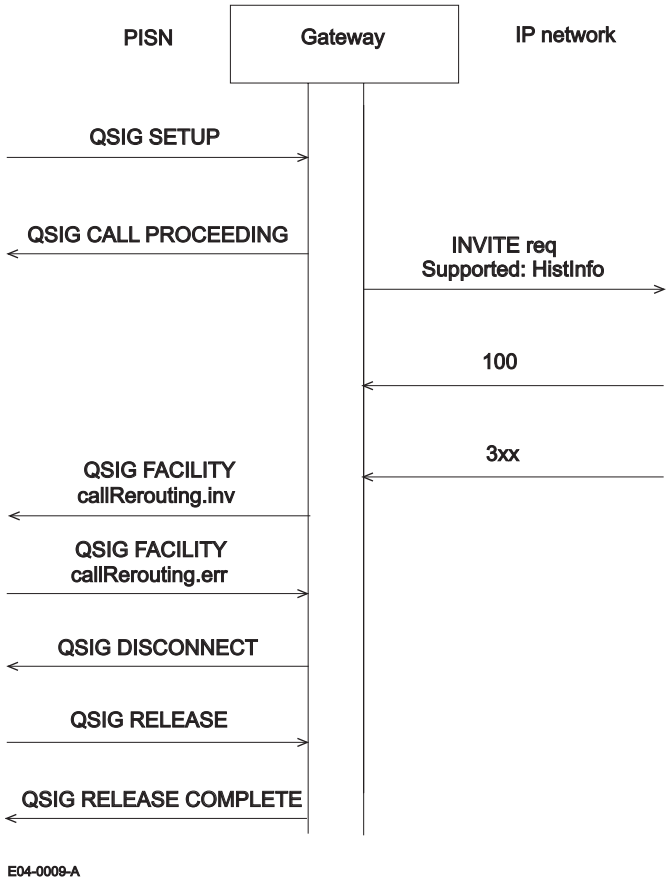

Figure 9 – Example of scenario B1 (call forwarding unconditional or call forwarding busy)

NOTE If callRerouting.err is received, the gateway may attempt to take over the functions of the QSIG rerouting PINX. Otherwise it should initiate clearing as shown.

10.3.4 Failure – No answer following CFNR

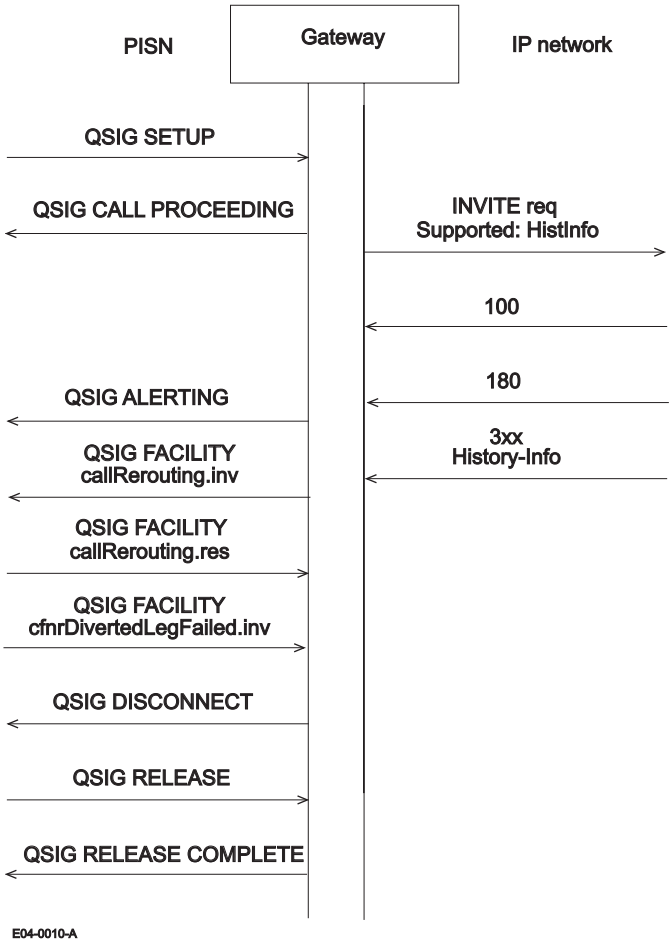

Figure 10 – Example of scenario B1 (call forwarding no reply followed by no answer)

NOTE Because the reroutingReason in callRerouting invoke indicates CFNR, a cfnrDivertedLegFailed invoke will arrive if diversion fails. The QSIG expectation is that alerting will continue at B, but SIP does not support this. Therefore the gateway will need to respond with a QSIG DISCONNECT.

10.4 Scenario B2

Call from SIP to QSIG redirected back to SIP network.

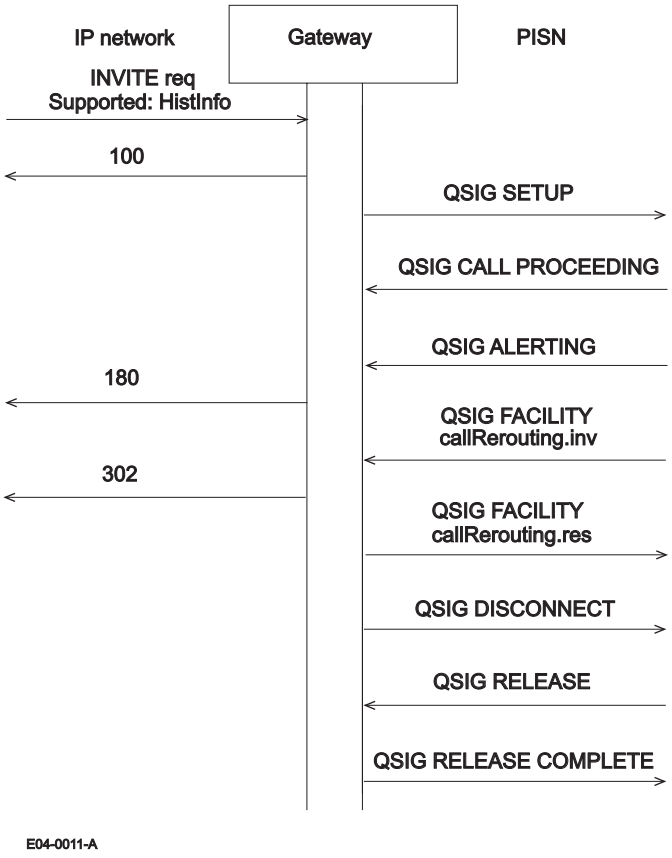

Figure 11 – Example of scenario B2 (call forwarding no reply)

NOTE 1 This scenario applies only if the gateway does not act as the rerouting PINX. This could be determined by configuration or on a dynamic basis (e.g., depending on the value of calledAddress). If the subscriptionOption in the callRerouting.inv indicates that presentation of the diverted-to number to the calling user is restricted, the gateway should act as the rerouting PINX. If the gateway acts as the rerouting PINX, scenario A2 applies to the sending of SIP history information towards the calling user.

NOTE 2 302 (Moved Temporarily) seems to be the nearest 3xx match, regardless of diversionReason. It may also be possible to add a Reason header if this is enhanced for inclusion of a diversion reason.

NOTE 3 The Contact header in the 302 response should be derived from the number in the callRerouting.inv.

NOTE 4 This diagram illustrates CFNR, since callRerouting invoke arrives after ALERTING. For CFNR, the rerouting PINX should wait to see if diversion is successful, so that the call can continue to alert B if not. There is no capability in SIP to indicate success or failure of a 3xx response, and therefore the call to B has to be cleared immediately (as for CFU and CFB).

10.5 Scenario C1

Call diverted in QSIG network to SIP network.

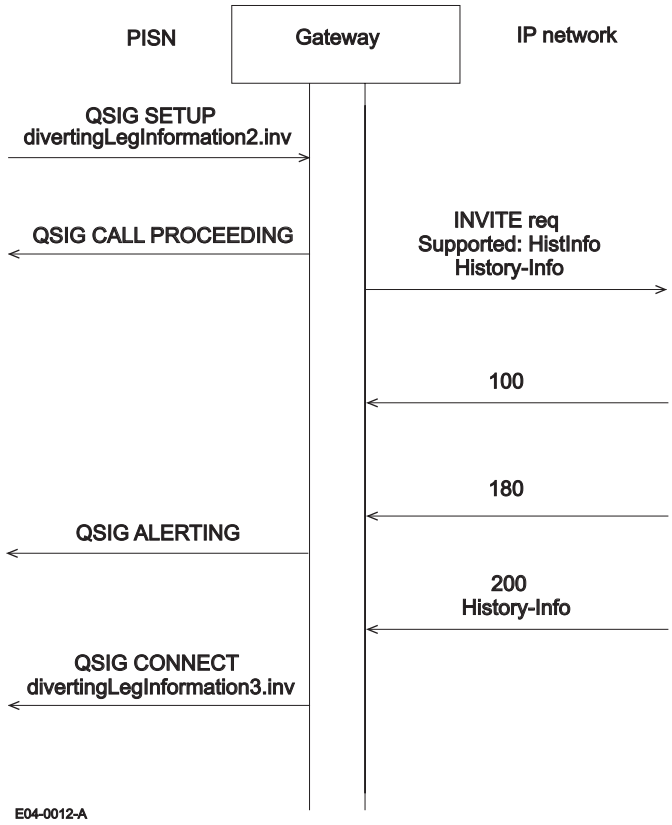

Figure 12 – Example of scenario C1

NOTE 1 If originalCalledNr and originalDiversionReason are absent, two targeted-to URIs should be included in the History-Info header in the INVITE request. The first is derived from the divertingNr element and contains a Reason header derived from the diversionReason element (see 9.4). The second is derived from the Request-URI.

NOTE 2 If originalCalledNr and originalDiversionReason are present, three targeted-to URIs should be included in the History-Info header in the INVITE request. The first is derived from the originalCalledNr element and contains a Reason header derived from the originalDiversionReason element (see 9.4). The second is derived from the divertingNr element and contains a Reason header derived from the diversionReason element (see 9.4). The last is derived from the Request-URI.

10.6 Scenario C2

Call diverted in SIP network to QSIG network.

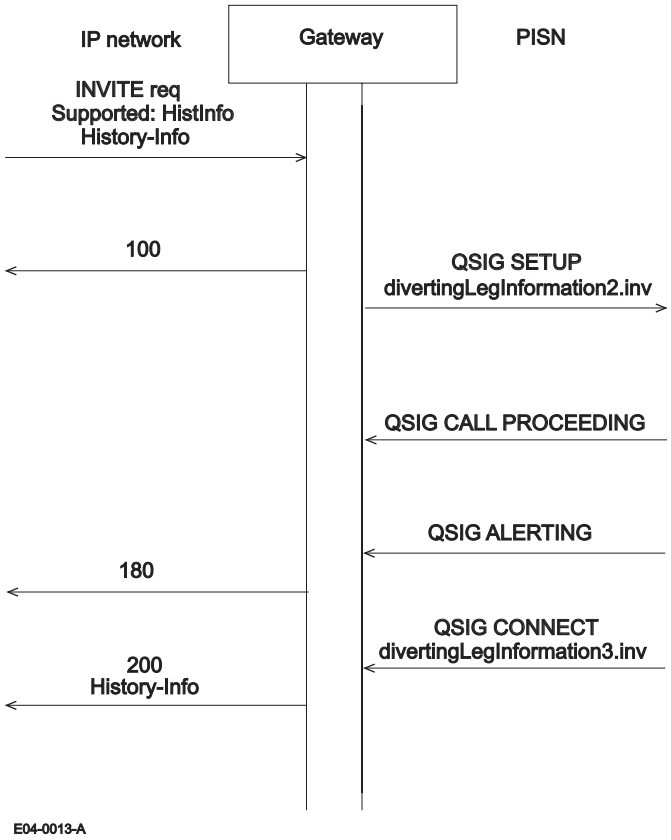

Figure 13 – Example of scenario C2

NOTE 1 divertingNr and diversionReason are derived from the penultimate targeted-to URI and its Reason header in the History-Info header. See 9.3 for deriving diversionReason.

NOTE 2 originalCalledNr and originalDiversionReason are derived from first targeted-to URI and its Reason header respectively in the History-Info header if there are more than two URIs present in that header. Otherwise these elements are omitted.

NOTE 3 The History-Info header may be sent earlier in a provisional response (e.g., in 180 or 183). However, it must also be included in the 200 response.

NOTE 4 Inclusion of History-Info in a response will depend on privacy considerations, including presentationAllowed indicator in divertingLegInformation3 invoke.

10.7 Scenario A1 followed by B1

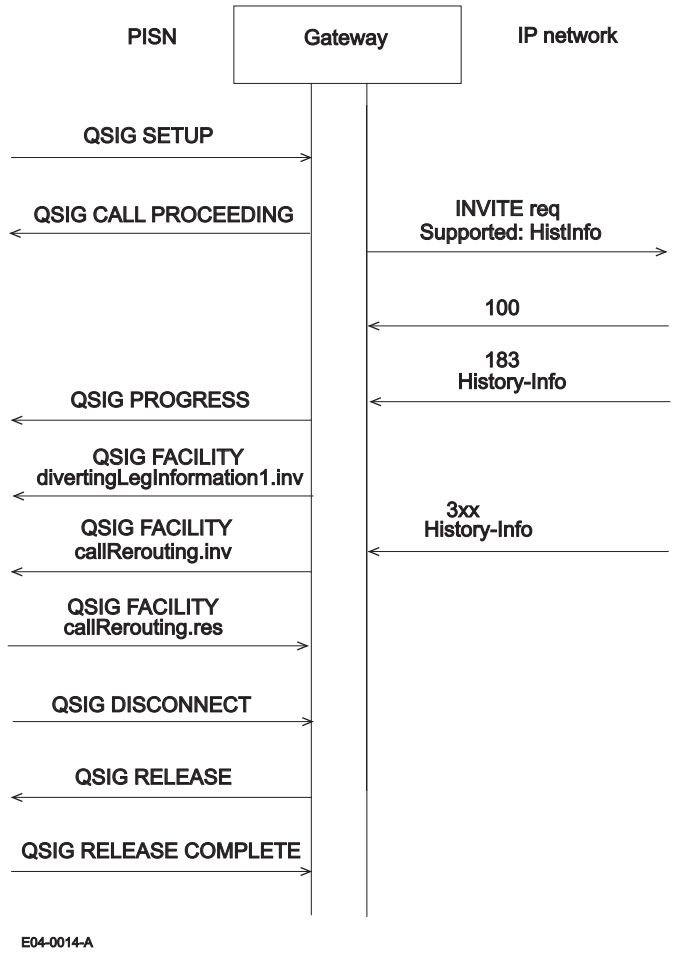

Figure 14 – Example of scenario A1 followed by B1

NOTE 1 The sending of PROGRESS on receipt of a SIP 183 response is dependent on the conditions specified in [6].

NOTE 2 The History-Info in the 3xx response reflects previous retargets, not any retarget suggested by the 3xx response.

10.8 Scenario A2 followed by scenario B2

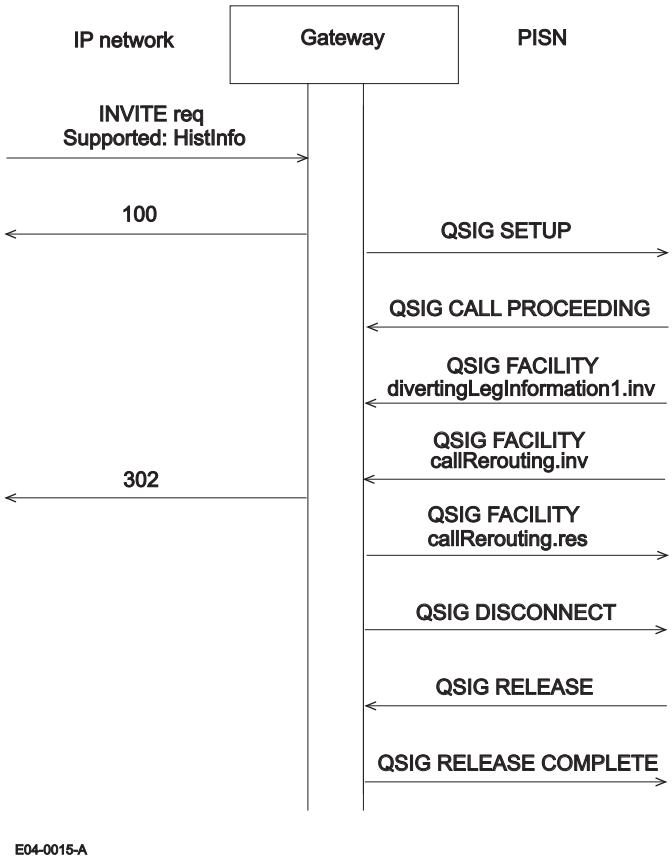

Figure 15 – Example of scenario A2 followed by B2

NOTE No History-Info is sent back because no divertingLegInformation3.inv has been received and therefore the privacy situation is uncertain.

10.9 Scenario C1 followed by scenario A1

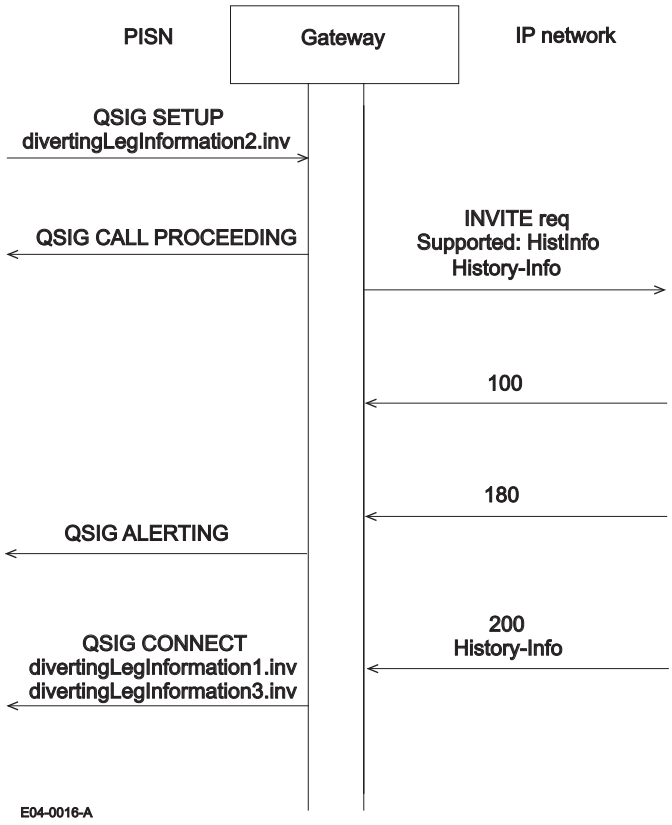

Figure 16 – Example of scenario C1 followed by A1

NOTE This is similar to scenario C1 alone, except that scenario A1 applies for mapping History-Info in the 200 response (or a provisional response) to information in the divertingLegInformation1 invoke. Care should be taken only to map information relating to diversions in the IP network, not information derived from divertingLegInformation2 invoke.

10.10 Scenario C2 followed by scenario A2

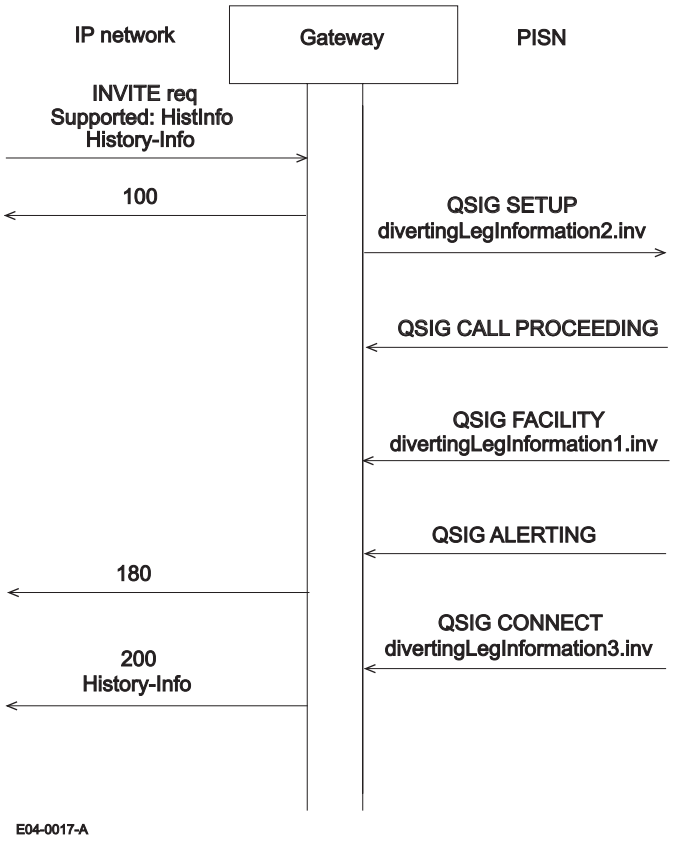

Figure 17 – Example of scenario C2 followed by A2

NOTE The History-Info header in the 200 response should reflect both information from the History-Info header received in the INVITE request and information derived from the divertingLegInformation1.inv. However, if information in the divertingLegInformation1 or divertingLegInformation3 invoke indicates that privacy is required for user C's number, then this will limit information that can be provided in the History-Info header.

10.11 Scenario C1 followed by scenario B1

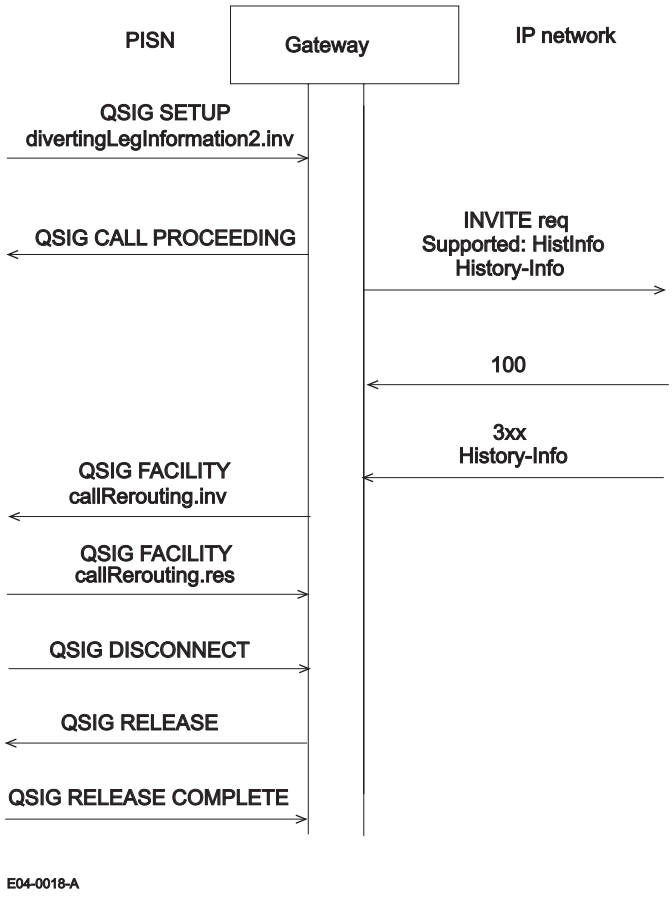

Figure 18 – Example of scenario C1 followed by B1

10.12 Scenario C2 followed by scenario B2

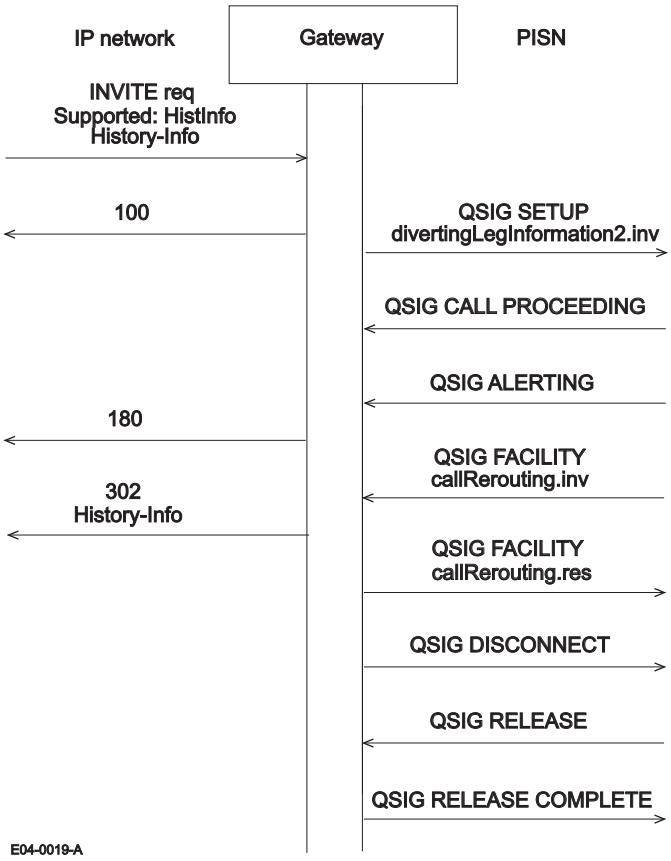

Figure 19 – Example of scenario C2 followed by B2

NOTE The History-Info in the 302 response reflects that received in the INVITE request.

11 Security considerations

The security considerations of [11], [14] and [6] apply.

Privacy of diversion information is an issue dealt with separately in [5] and [14] for QSIG and SIP respectively. It is important that when interworking between QSIG and SIP the privacy measures of each network are not compromised.

For QSIG, these privacy measures are in the form of indicators in certain APDUs, and the requirements of this document prevent disclosure to the SIP network of information marked as subject to privacy in the QSIG network, except when being forwarded within the same domain to an entity capable of providing a privacy service as defined in [12]. In this case, if the information is disclosed it is marked as being subject to privacy, so that it can be removed if the request or response leaves that domain.

For SIP, privacy depends on the withholding of private diversion-related information or, within a single domain, marking it as subject to privacy. Therefore if the gateway does receive such information it will be marked as subject to privacy. The gateway may disclose this information to the QSIG network only if the QSIG network is in the same domain, in which case the gateway will set the appropriate QSIG privacy indicators to prevent subsequent disclosure outside the domain.

ICS 33.040.35

Price based on 35 pages