ETSI TS 101 884 V1.1.1 (2002-09)

Technical Specification

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology Mapping; Implementation of TIPHON architecture using SIP

Reference

DTS/TIPHON-03018

Keywords

architecture, IP, SIP, telephony, VoIP

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.fr

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).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

Introduction

The SIP profile contained in the present document is derived from examination of:

- the capabilities required by TS 101 878 [6] for the support of TIPHON as identified in TR 101 300 [4];
- the TIPHON baseline architecture described in TS 101 314 [1]; and
- the primitives, parameters and procedures defined in TS 101 882 [7].

The documents listed above are compared and evaluated against the IETF protocols SIP [SIP], SDP [SDP] and DNS [DNS].

The relationship between the TIPHON documents can be better seen in the figure 1.

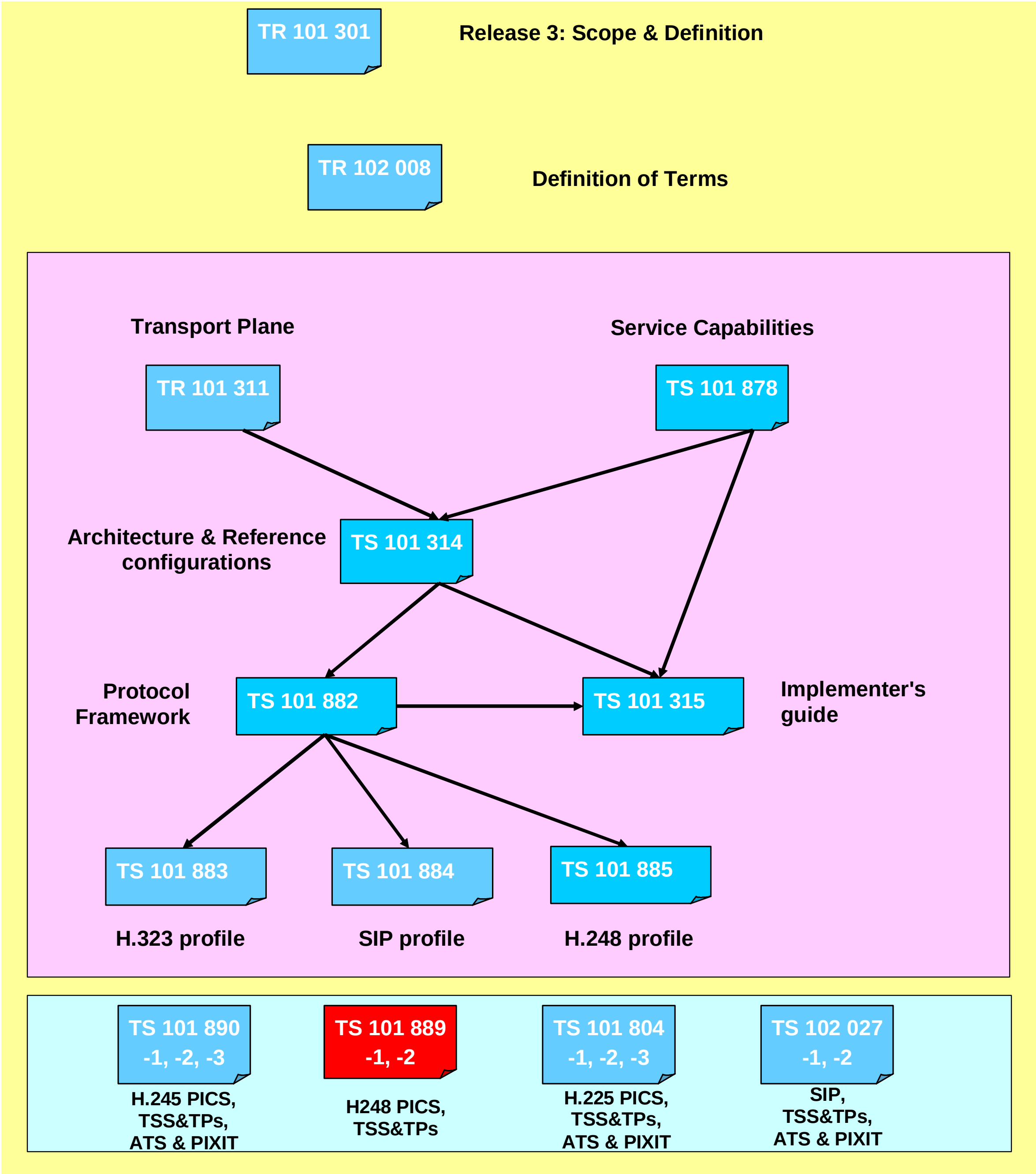


Figure 1: Relationship with other TIPHON Release 3 documents

- TR 101 311 [11] provides the requirements on the transport plane.
- TS 101 878 [6] defines service capabilities that are used in the TIPHON Release 3 for a simple call.
- TS 101 882 [7] provides the Protocol Framework based on the TIPHON Release 3 architecture to implement the simple call service capabilities as defined in the present document.
- TS 101 315 [5] is an implementer's guide that shows how to use of the meta-protocol to realize the capabilities as defined in TS 101 878 [6].
- TS 101 883 [12] provides the protocol mappings for the ITU-T H-323 profile.
- TS 101 884 (the present document) provides the protocol mappings for the SIP profile.

- TS 101 885 [13] provides the protocol mappings for the ITU-T H-248 profile.
- TS 101 314 [1] provides the architecture and reference configurations for TIPHON Release 3.

1 Scope

The present document describes how the SIP and SDP protocols can be used to implement TIPHON architecture, as defined in [5], and the Context and Behaviour of Meta-Protocol, as defined in [7].

The scope of the present document is limited to the mapping of the following parts of Meta-Protocol to SIP:

- Registration Meta-Protocol;
- Call Control Meta-Protocol;
- Bearer Control Meta-Protocol.

The present document is applicable to equipment performing the roles of terminal, Registration server, proxy Application Server, and gateway, and also to entities within the IP network that are necessary to support the TIPHON Release 3.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] ETSI TS 101 314: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Abstract Architecture and Reference Points Definition; Network Architecture and Reference Points".

[2] IETF RFC 3261: "SIP: Session Initiation Protocol".

[3] IETF RFC 2327: "SDP: Session Description Protocol".

[4] ETSI TR 101 300: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Description of Technical Issues".

[5] ETSI TS 101 315: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Functional entities, information flow and reference point definitions; Guidelines for application of TIPHON functional architecture to inter-domain services".

[6] ETSI TS 101 878: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Capability Definition; Service Capabilities for a simple call".

[7] ETSI TS 101 882: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Protocol Framework Definition; General (meta-protocol)".

[8] IETF RFC 3262: "Reliability of Provisional Responses in Session Initiation Protocol (SIP)".

[9] ETSI TR 101 301: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Release Definition; TIPHON Release 3 Definition".

[10] ETSI TR 102 008: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Terms and Definitions".

[11] ETSI TR 101 311: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Independent requirements definition; Transport Plane".

[12] ETSI TS 101 883: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology Mapping; Implementation of TIPHON architecture using H.323".

[13] ETSI TS 101 885: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology Mapping; Technology Mapping of TIPHON reference point N to H.248/MEGACO protocol".

[14] ETSI TS 101 890 (all parts): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology Compliance Specifications; TIPHON profile for ITU-T H.245".

[15] ETSI TS 101 889-1: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology Compliance Specification; TIPHON profile for ITU-T H.248; Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification".

[16] ETSI TS 101 889-2: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology Compliance Specification; TIPHON profile for ITU-T H.248; Part 2: Test Suite Structure and Test Purposes (TSS&TP) specification".

[17] ETSI TS 101 804 (all parts): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology compliance specifications; Part 1: Revision/Update of H.225.0 Protocol Implementation Conformance Statement (PICS) proforma specification for Terminal, Gatekeeper and Gateway".

[18] ETSI TS 102 027-1: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Technology Compliance Specification; Draft IETF SIP RFC2543bis-04; Part 1: Test Suite Structure and Test Purposes (TSS&TP) specification".

[19] ETSI TR 101 877: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Requirements Definition Study; Scope and Requirements for a Simple call".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 101 877 [19] and TS 101 878 [6] apply.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

API Application Programming Interface
ASN.1 Abstract Syntax Notation One
B2BUA Back-to-Back User Agent
BC Bearer Control
CC Call Control
FE Functional Entity
FG Functional Grouping
GFG Gateway Functional Group
GoS Grade of Service
ICF Inter-Connect Function
IP Internet Protocol
IPTN IP Telephony Network
ISDN Integrated Services Digital Network
MC Media Control
MPMU Meta Protocol Message Unit
MSC Message Sequence Chart
NFG Network Functional Group

PCM	Pulse Code Modulation
PDU	Protocol Data Unit
RpoA	Registration point of Attachment
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SAP	Service Access Point
SC	Service Control
SCN	Switched Circuit Networks
SDL	Specification and Description Language
SpoA	Service point of Attachment
SLA	Service Level Agreement
SL	Service Layer
TCC-SAP	TIPHON Call Control SAP
TE	Terminal Equipment
TFG	Terminal Functional Group
TLL-SAP	TIPHON Lower Layer SAP
TRL	TIPHON Resource Location
TR-SAP	TIPHON Registration SAP
TT-SAP	TIPHON Transport SAP
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
URI	Uniform Resource Identifier

4 Implementation of TIPHON functional architecture using SIP

The SIP technology includes two protocols of interest to TIPHON:

- SIP - As defined in SIP RFC [2] this is often used as a client/server based call control protocol.
- SDP - A Bearer Control protocol, as defined in IETF RFC 2327 [3].

SIP identifies a number of functional entities: SIP User Agents (UA), SIP registrar, SIP servers, SIP proxies and SIP gateways. The present document describes the behaviour of, and the communication between these functional entities in the context of TIPHON.

TS 101 314 [1] defines a number of reference points and Functional Entities (FE). These reference points and Functional Entities need to be mapped to SIP based architecture before behaviours and message flows can be defined. For this purpose, an introduction to the SIP Architecture is given below, along with its mapping to TIPHON functional architecture.

4.1 SIP functional architecture

The SIP Architecture has the following functional elements, as defined in [2].

User Agent (UA): The user agent is the functional entity that may initiate or respond to a SIP request.

In a TIPHON compliant system, the SIP User Agent (UA) shall provide the functionality of the terminal functional group. The terminal functional group performs the roles of the terminal registration functional group, originating terminal functional group and the terminating terminal functional group. The reference points S1, SC1 and N1 are regarded as internal to the TE. The UA may use the DNS server.

Back-to-Back User Agent (B2BUA): B2BUA is a logical entity that receives a request and processes it as a User Agent Server (UAS). In order to determine how a request should be answered, it acts as a User Agent Client (UAC) and generates requests. Unlike a proxy server (stateless), it maintains a dialogue state, and must participate in all requests sent on the dialogues it has established. TIPHON recommends the use of a B2BUA, as network functional groupings involved in providing a service.

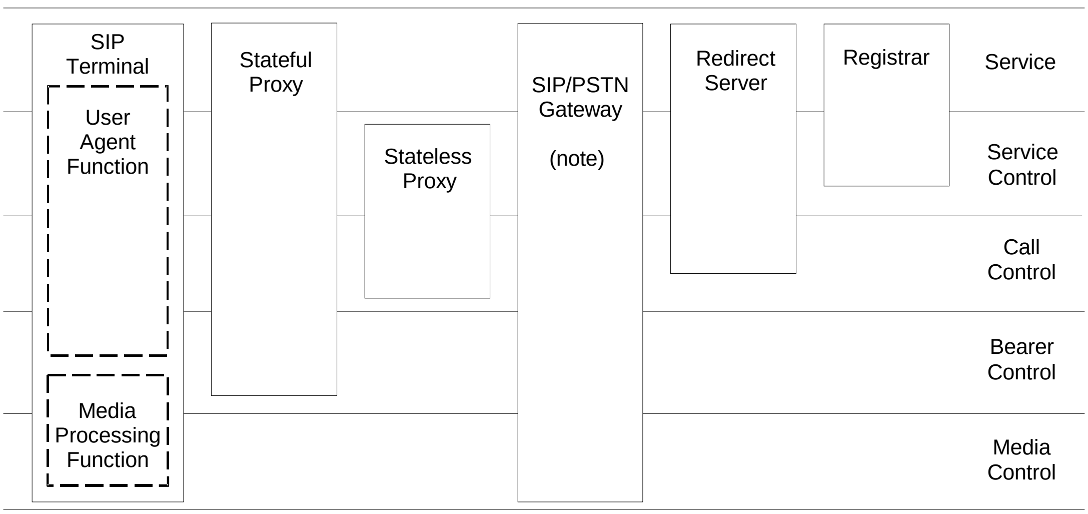
SIP Server: A SIP server provides a service to SIP user agents and/or proxies and other servers. An example of such a server can be a redirect server.

Proxy server: A proxy server acts as both the client and server: It receives a request from an entity, and initiates a request on behalf of the requesting entity, hence acting as a server for the requesting entity.

- **Registration server:** The registration server processes registration requests; as a minimum this involves updating the users contact list and responding to the originator of the request. Typically a registration server is co-located with either the proxy or the redirect server, and may be adapted to perform location-based services.

- **SIP gateway:** A SIP gateway acts as an interworking medium between the PSTN and IP networks. It provides an interworking between the SIP and other call control protocols, such as ISUP, as well as interworking between the TDM and IP media flows.

Figure 2 shows how the SIP functional elements map onto the functional layers in the IP Telephony Application plane.



NOTE: Compound gateway.

Figure 2: The SIP example mapped onto the IP telephony application plane

The UA maps to Service, Service Control (SC), Call Control (CC), and Bearer Control (BC) layers.

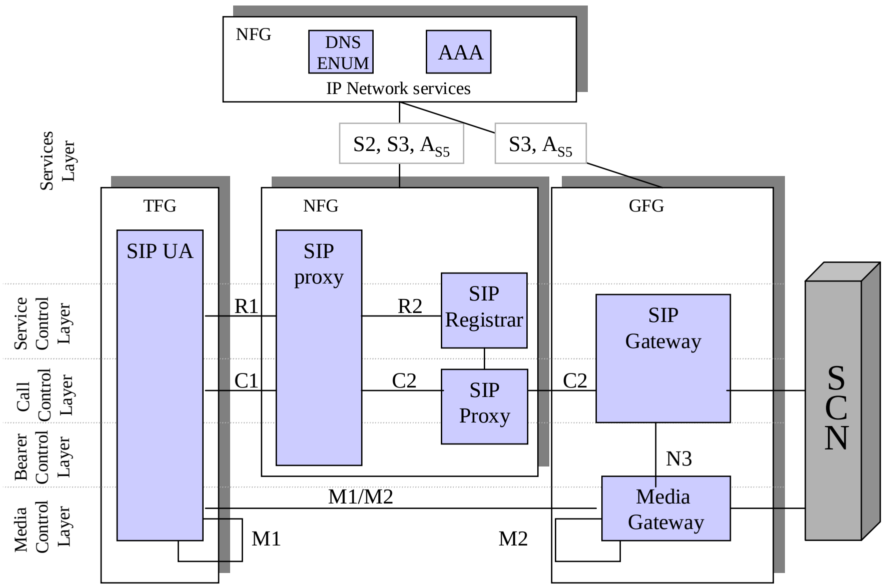
The statefull proxy maps to the TIPHON service and call control layer.

The SIP PSTN gateway covers all TIPHON layers.

The redirect server works at TIPHON Service Control layer.

The registrar works at TIPHON Service and Service Control layer.

Figure 3 shows the SIP entities and how they map to the functional layers and the Functional Groups (FG) defined in [1].



NOTE: All entities in an IP network "normally" use the DNS service. In the context of the present document only relations to the DNS with ENUM extensions are shown.

Figure 3: SIP Architecture mapped to the TIPHON Functional layers and functional groups

The SIP proxy, SIP server, SIP gateway and the SIP Registration Server shall provide the functionality required in the Network Functional Group (NFG). Reference point S2, S3 and A_{S5} are between the Network Functional Group and other IP Network services e.g. DNS. The Network Functional Group may play the roles of an originating Network Functional Group, an intermediate Network Functional Group or a terminating Network Functional Group.

NOTE: The Network Functional Group may include Media Control Functional Entities, e.g. for giving announcements, mixing media streams etc. This is, however, out of scope of the present document.

The present document describes the mapping of functional architecture [1], as well as the context, behaviour and procedures [7] that the SIP and SDP protocols must adhere to, to be TIPHON compliant. In TIPHON Release 3, SIP is mapped to reference points R1, R2, C1, C2, where R1 and R2 refer to the registration reference points, whereas C1 and C2 refer to call & bearer control reference points. The R and C reference points will be dealt with separately in the present document, because of the different nature of services they provide.

5 Registration

This clause applies to SIP terminals, SIP proxies and SIP registrars and describes how the SIP [2] shall be used in order to implement the registration meta-protocol defined in the annex A of TS 101 882 [7].

SIP [2] defines how a user registers with a SIP registrar in one service provider's domain. The present document extends this registration procedure to also include the registration of users via another service provider's domains.

NOTE 1: The intention of this clause is not repeat the SIP RFC [2] text, but to select options and to clarify relations with TIPHON architecture in TS 101 314 [1], and the registration meta protocol in TS 101 882 [7].

Two registration scenarios shall be supported:

- The "user at home" scenario; and
- The "roaming user" scenario.

NOTE 2: For more details and examples of the two scenarios see TS 101 315 [5].

The registration meta-protocol defines three steps for a user to access a service application:

1) location of the Registration point of Attachment (RpoA);

2) registration; and

3) attachment to the service application.

The objective with the step 1 is to locate the Registration point of Attachment. This step may be implemented using DHCP. This step is out of scope of the present document.

Step 2 is a "Single log-on" procedure where a user registers to one registrar and receives tickets for all service applications available to the user. SIP does not support the "Single log-on" procedure at present, hence out of scope of the present document.

Step 3 describes how users attach to (or detach from) a service application. In the context of the present document the service application is the VoIP service application based on SIP. Therefore, the SIP registrant registers with a SIP registrar providing both the registration and VoIP services.

Figure 4 shows how TS 101 882 [7] M-PDUs is mapped to corresponding SIP [2] methods.

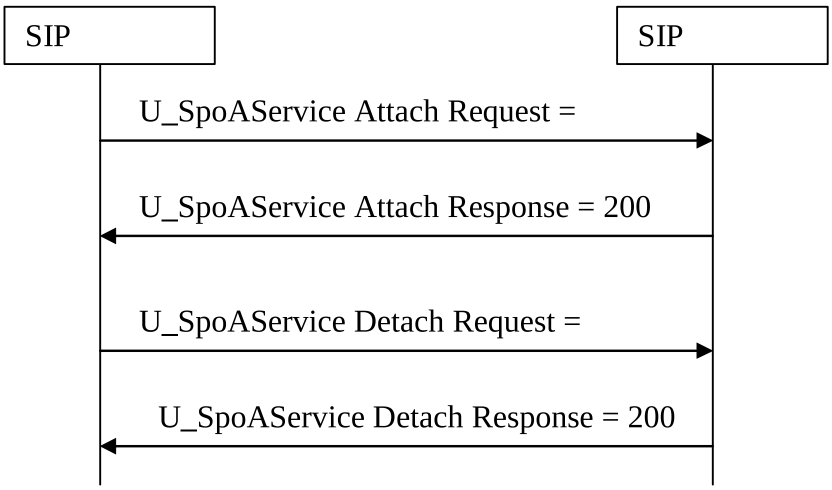


Figure 4: Mapping of TS 101 882 [7] M-PDUs to SIP [2] methods

Figure 5 shows the message flow for the "user at home" scenario where the SIP terminal registers directly to the SIP registrar in the home network without involving intermediate networks. The information flows between the SIP terminal and the SIP registrar in the home network flows on TIPHON reference point R1.

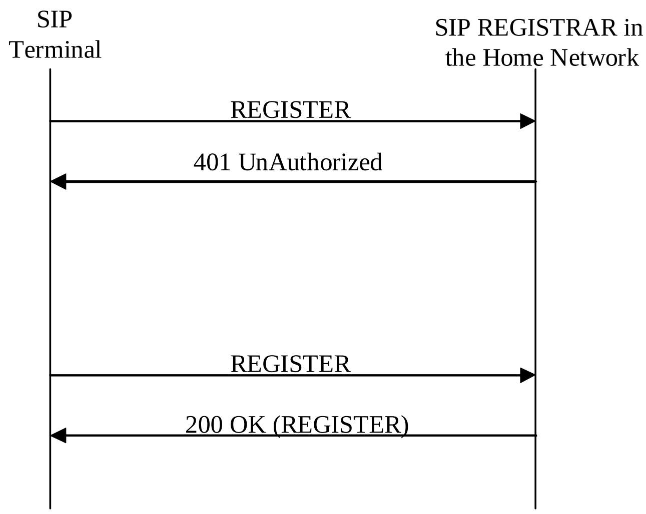


Figure 5: "User at home" registration

The SIP terminal sends the REGISTER message to the SIP registrar in the home network. The SIP registrar in the home network returns a `'401 Unauthorized'` response in order to authenticate the user. The `'401 Unauthorized'` response includes a challenge. The SIP terminal sends (for the second time) the REGISTER message to the SIP registrar in the home network. The REGISTER message now includes the response to the challenge. The SIP registrar in the home network acknowledges the registration by means of the `'200 OK'` final response.

Figure 6 shows the message flow for the "Roaming user" scenario, where the SIP terminal registers with the SIP registrar in the home network, via a SIP proxy in the serving network and a SIP proxy in the intermediate network. The information flows between the SIP terminal and the SIP proxy in the serving network flows on TIPHON reference point R1. The information flows between the SIP proxies in the serving network and in the intermediate network and the SIP registrar in the home network flows on TIPHON reference point R2.

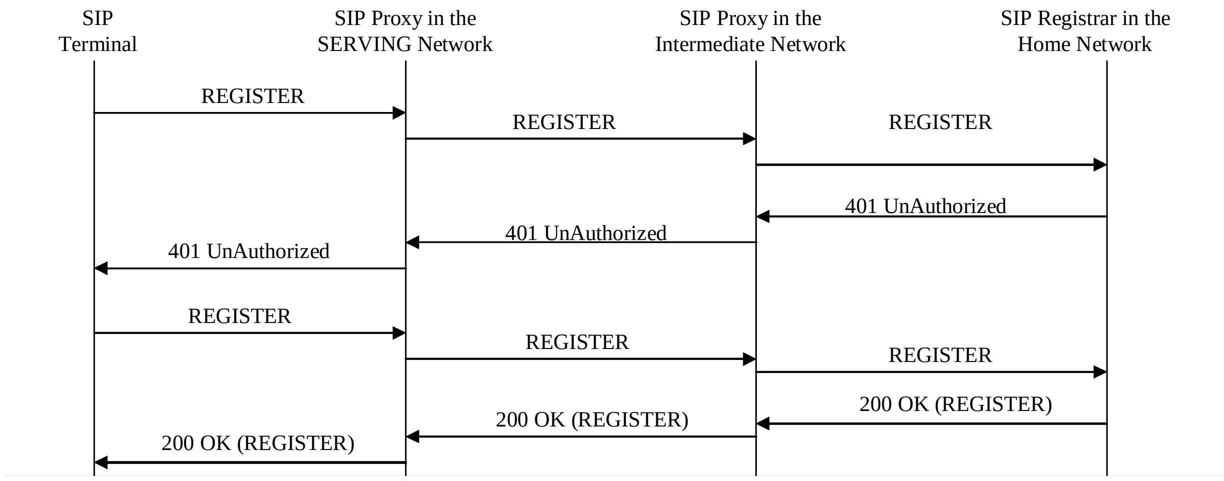


Figure 6: "Roaming user" registration

The SIP terminal sends the REGISTER message to the SIP proxy in the serving network. The SIP proxy forwards the message to a SIP proxy in the intermediate network which forwards the REGISTER message to the SIP registrar in the home network.

NOTE 3: The above behaviour assumes that a bilateral agreement exists between the serving network and the intermediate network and between the intermediate network and the home network. The handling of bilateral agreements and how they are stored is out of the scope of the present document.

The SIP registrar in the home network returns a `"401 Unauthorized"` response in order to authenticate the user.

The `"401 Unauthorized"` response includes a challenge.

The `"401 Unauthorized"` response is returned (via the SIP proxies in the intermediate network and the serving network) to the SIP terminal.

The SIP terminal sends (for the second time) a REGISTER message towards the SIP registrar in the home network (via the SIP proxy in the serving network and the intermediate network).

This REGISTER message now includes the response to the challenge.

The SIP registrar in the home network acknowledges the registration by means of the `'200 OK'`.

The following clause describes the behaviour in the SIP terminal, the SIP proxy in the serving network, the SIP proxy in the intermediate network and the SIP registrar in the home network when a user attach to and detach from the VoIP service application.

5.1 Adding contact addresses

The REGISTER message is used to register new contact addresses. The same message may (at the same time) be used to refresh existing contact addresses and remove existing contacts. For simplicity this clause assumes that the REGISTER message only includes contact addresses to be refreshed.

5.1.1 Procedures in the SIP terminal

This clause applies to all SIP terminals.

5.1.1.1 Normal procedure

The SIP terminal shall register with a SIP registrar as described in [2] clause 10 "*Registrations*" with the clarifications below.

The user shall register one or more contact addresses where he is reachable. Registrations are additive i.e. the user may add more contacts addresses to an already active registration.

The following procedures take place for the registration to be complete (see figures 5 and 6 for an overview of the message flow).

The REGISTER message shall be coded as defined in SIP [2] clause 10.2 "*Construction of the REGISTER request*" with the following clarifications:

- The `'TO"` header field shall include the public identity of the user. The public identity shall be in the format of a SIP-URL or a TEL-URL.
- The `'FROM"` header field shall include the same public identity as in `'TO"` header field.

NOTE 1: The `'FROM"` header field may (in the case of a 3rd party registration) be different from the user identity in the `'TO"` header field (`'TO"` represents a user being registered; `'FROM"` represents a user initiating registration). However, the TIPHON Release 3 does not support a 3rd party initiated registration.

- The `'REQUEST-URI"` in the format of the SIP URL, shall be the domain name of the SIP registrar in the home network.
- The SIP terminal may include a suggestion for how long the registration shall be valid in either the `'EXPIRE"` header field or in the `'EXPIRE"` parameter in the `'CONTACT"` header field. In case the SIP terminal does not include a value, the one hour shall be assumed; and
- at least one `'CONTACT"` header field shall be included.

NOTE 2: If no `'CONTACT"` header field is included in the REGISTER message the SIP registrar returns all active "bindings" for the user identity in the `'TO"` header field. A "binding" is a combination of a user identity and one contact address.

The REGISTER message shall be sent to the SpoA. In the context of the present document the SpoA may be a SIP proxy in a serving network or the SIP registrar in the home network.

The SIP terminal may obtain the address to the SpoA in one of the following ways:

- by means of a "Single log-on" procedure. Out of scope of the present document;
- by manual configuration in the SIP terminal; or
- by using the multicast procedure defined in [2] clause 10.2.5 "*Discovering a registrar*".

In the case the SpoA address is in the format of a URI (i.e. not an IP address) the SIP terminal shall use the DNS to resolve the URI to an IP address each time a REGISTER message is sent (this is also true for retransmitted REGISTER messages).

The SIP terminal shall supervise the reception of a response message to the REGISTER message.

On receipt of a `'401 Unauthorized'` response the SIP terminal shall provide credentials (see [2] clause 20.3 "*Proxy to User Authentication*") and retransmit the REGISTER message.

The retransmitted REGISTER message shall:

- be constructed as described earlier in this clause; and
- include the `'PROXY-AUTHORIZATION"` where 'username' parameter is the User's private identity (i.e. the private user identity of the user identity in the `'FROM"` header field).

NOTE 3: The above authentication scheme only authenticates the user. In the case the SIP registrar should be authenticated the clause 22.3.2.1 "*Registration*" is recommended.

On receipt of the `'200 OK'` final response the SIP terminal shall stop time supervision of the response to the REGISTER message and start timers for refreshing the registrations according to the 'EXPIRE' header field or according to the 'expire' parameter in the `'CONTACT"` header field.

The SIP terminal shall store the IP address (received from DNS when resolving the SpoA address in an URI format) used when sending the REGISTER message. The SIP terminal shall use this IP address for future request towards the home network (with the exception of REGISTER request messages).

See annex A for details on REGISTER message and its contents.

5.1.1.2 Exceptional procedures in terminals

Upon receipt of 3XX, 4XX (with the exception of the `'401 Unauthorized"` or 5XX responses to the REGISTER message, procedures according to [2] clause 8.1.4 "*Processing Responses*" shall apply.

If the supervision timer for responses on the REGISTER message expires the SIP terminal shall retransmit the REGISTER message.

5.1.2 Procedures in the SIP registrar and in the SIP proxy

A server may be designed to act as a SIP registrar or a SIP proxy (in the serving network as well as in the intermediate network). This implies that on the receipt of the REGISTER message in the SIP registrar the server needs to decide whether it should act as a SIP registrar in the home network or as a SIP proxy in a serving network or in an intermediate network. This shall be done in the following way:

On receipt of the REGISTER message the SIP registrar shall verify that the 'Request-URI' header field includes a domain name within its authority.

If the `'REQUEST-URI"` header field includes a domain name within its authority the SIP REGISTRAR shall act as a SIP registrar and the procedures in clause 5.1.2.1 shall apply.

If the `'REQUEST-URI"` header field does not includes a domain name within its authority the SIP registrar shall act as a SIP proxy and the procedures in clause 5.1.2.2 shall apply.

5.1.2.1 Procedures at SIP registrar in home network

The procedures of this clause apply, when a SIP registrar in the home network receives a REGISTER message with one or more *new* contact addresses included.

5.1.2.1.1 Normal procedures

On receipt of the REGISTER message the SIP registrar in the home network shall follow the procedures in [2] clause 10.3 "*Processing REGISTER Requests*" with the clarifications below.

- The SIP registrar shall verify that the user is one of its subscribers. The verification is based on the `'TO"` header field.
- The SIP registrar shall verify that the user identity in the `'FROM"` header field is authorized to register.

NOTE: The above is especially important when the SIP registrar allows 3rd party registration. However, since the TIPHON Release 3 does not include 3rd party registrations the `'TO"` header field and the `'FROM"` header field are the same.

- The SIP registrar shall authenticate the registrant. The authentication is based on the `'AUTHORIZATION"` header field.
- If the authentication is successful, the SIP registrar shall successfully register each combination of user identity/contact address that can be created by combining the user identity in the `'TO"` field with each received `'CONTACT"` header field.

Once the registrant is verified and authenticated, the registrar shall respond with a `'200 OK'` response. The `'200 OK'` response shall include header fields according to [2] clause 10.3 "*Processing the REGISTER Request*", bullet 8.

See annex A for details on `'200 OK'` (REGISTER RESPONSE) message and its contents.

5.1.2.1.2 Exceptional procedures

The SIP registrar shall follow the procedures as described in the [2] clause 10.3 "*Processing the REGISTER Request*" with the following clarification:

If the REGISTER message does not include any authentication information the REGISTER message shall return a `'401 Unauthorized".`

The `'401 Unauthorized"` response shall:

- include `'WWW-AUTHENTICATE"` header field; and
- the `'algorithm"` parameter set to MD5.

5.1.2.2 Procedures in the SIP proxy

The procedures of this clause apply, when a SIP proxy in the serving network or in the intermediate network receives a REGISTER message.

5.1.2.2.1 Normal procedures

On receipt of the REGISTER message procedures in [2] clause 16 "*Proxy Behaviour*" applies with the clarifications below.

The `'REQUEST-URI"` in the REGISTER message shall be analysed in order to determine the address of the next-hop location. The next-hop location may be the SIP registrar in the home network or another SIP proxy in an intermediate network. When the analysis results in an address in a URI format the DNS shall be used to resolve the URI to an IP address.

NOTE 1: The next-hop analysis is based on bilateral agreements between the serving network and intermediate networks and between intermediate networks and the home network. How those agreements are accessible from the SIP proxy is out of the scope of the present document.

NOTE 2: The next-hop location is always determined based on the `'REQUEST-URI"` header field since the SIP RFC [2] does not allow the `'ROUTE"` header field in the REGISTER message.

The SIP proxy shall process the REGISTER message as defined in [2] clause 16.5 "*Request processing*" with the following clarifications:

- the `'REQUEST-URI"` header field shall not be modified;
- each `'CONTACT"` header field shall be modified/replaced to include the host address of the SIP proxy;

NOTE 3: The above behaviour will allow future SIP requests (sent towards the SIP terminal) to be routed through the SIP proxy giving the SIP proxy the possibility to fork requests to all contact addresses within e.g. a private IP network.

- the REGISTER message shall be sent to the address of the next-hop location; and
- a supervision timer started in order to supervise a response.

On receipt of the `'200 OK'` response the SIP proxy procedures in [2] clause 16.6 "*Response processing*" applies with the following clarifications:

- `'CONTACT"` header fields from the original REGISTER message shall be stored (together with the User identity in the `'TO"` header field) and serve as a local location database for incoming SIP requests e.g. the INVITE message;
- the list of `'CONTACT"` header fields shall be restored (i.e. SIP proxy portion of the address shall be removed);
- send the `'200 OK'` response towards the SIP terminal; and
- clear all resources used during the registration.

The SIP proxy shall store the next-hop location IP address in the local location database together with the stored binding.

5.1.2.2.2 Exceptional procedures

If the SIP proxy does not have a business agreement suitable to forward the REGISTER message to a next-hop location (either another SIP proxy in an intermediate network or the SIP registrar in the home network), the SIP proxy shall decline the registration request, and respond with `'403 Forbidden'` message.

If the REGISTER message does not include `'CONTACT"` header fields the SIP proxy shall send the REGISTER to the next-hop location and start a supervision timer for the response.

On receipt of 3xx, 4xx or 5xx responses procedure in the SIP RFC [2] clause "*Response processing*" applies.

If the supervision timer (for the supervision of a response to the REGISTER message) expires the SIP proxy shall silently clear all reserved resources.

5.2 Refreshing contact addresses

This clause describes how registered contact addresses shall be refreshed.

Contact addresses are refreshed by means of the REGISTER message. The same message may (at the same time) be used to add new contact addresses and remove existing contacts. For simplicity this clause assumes that the REGISTER message only includes contact addresses to be refreshed.

5.2.1 Procedures in the SIP terminal

Before an active registration for a contact address ceases to be valid the SIP terminal shall refresh the registration according to the procedures in [2] clause 10.2.4 "*Refreshing Bindings*" and in clause 5.1.1 of the present document.

5.2.2 Procedures in the SIP registrar

The same procedure as in clause 5.1.2.1 of the present document shall apply.

5.2.3 Procedures in the SIP proxy

The same procedures as in clause 5.1.2.2 of the present document shall apply.

5.3 Removing contact addresses

This clause describes how users may detach from the SpoA.

The SIP RFC [2] does not allow the SIP registrar to "detach from a user". Instead the SIP registrar or a SIP proxy may silently discard all (or some) bindings (a binding is the combination of a public user identity and a contact address) created during the registration process.

The REGISTER message is used to detach from the SpoA. The same message may (at the same time) be used to add new contact addresses, refresh existing contact addresses and remove existing contacts. For simplicity this clause assumes that the REGISTER message only includes contact addresses to be removed.

5.3.1 Procedures in SIP terminal

The procedures in this clause apply to all SIP terminals.

5.3.1.1 Normal procedure

The SIP terminal shall initiate deregistration according to the procedures in the SIP RFC [2] clause 10.2.2 "*Removing bindings*" with the following clarifications.

- The SIP terminal shall wait for a confirmation, i.e. the `'200 OK'` response, from the SIP registrar, confirming the successful removal of the contact addresses; and
- the SIP terminal shall start a supervision timer supervising the response from the registrar.

On receipt of the `'200 OK'` response the SIP terminal shall regard all contact addresses (received in the REGISTER message) as deregistered with the exceptions of the contact addresses returned in the `'CONTACT"` header fields `'200 OK'` response.

5.3.1.2 Exceptional procedures

On expiry of the timer (supervising responses to the REGISTRATION message) the SIP terminal should retransmit the REGISTER message.

NOTE: The SIP terminal only needs to retransmit the REGISTRATION message in the case there are still active registrations for a contact address.

5.3.2 Procedures in the SIP registrar

5.3.2.1 Normal Procedure

This clause applies for the SIP registrar in the home network.

The procedures in the SIP RFC [2] clause 10.3 "*Processing Registration requests*" shall apply with the following clarification:

- The `'200 OK'` response shall include all active bindings i.e. the deregistered bindings should not be in the list.

5.3.2.2 Exceptional procedure

All other exceptional procedure according to the SIP RFC [2] clause 10.3 "*Processing REGISTER requests*".

5.3.3 Procedures in the SIP proxy

This clause applies for SIP proxies in the serving network and in the intermediate network when a REGISTER request is received when all or some of the bindings shall be removed.

5.3.3.1 Normal procedures

On receipt of the REGISTER message procedures in the SIP RFC [2] clause 16 "*Proxy Behaviour*" applies with the clarifications below.

The SIP proxy shall implement the stateful behaviour during the registration.

The `'REQUEST-URI"` in the REGISTER message shall be analysed in order to determine the address of the next-hop location. The next-hop location may be the SIP registrar in the home network or another SIP proxy in an intermediate network.

NOTE 1: The next-hop analysis is based on bilateral agreements between the serving network and intermediate networks and between intermediate networks and the home network. How those agreements are accessible from the SIP Server is out of scope of the present document.

NOTE 2: The next-hop location is always determined based on the `'REQUEST-URI"` header field since the SIP RFC [2] does not allow the `'ROUTE"` header field in the REGISTER message.

The SIP proxy shall process the REGISTER message as defined in [2] clause 16.5 "*Request processing*" with the following clarifications:

- the `'REQUEST-URI"` header field shall not be modified;
- the `'RECORD-ROUTE"` header field shall not be modified;
- the `'ROUTE"` header field shall not be updated;
- each `'CONTACT"` header field shall be modified to include the host address of the SIP proxy;
- the `'REGISTER"` message shall be sent to the address of the next-hop location; and
- a supervision timer started in order to supervise a response.

On receipt of the `'200 OK'` response the SIP proxy procedures in [2] clause 16.6 "*Response processing*" apply with the following clarifications:

- the SIP proxy shall remove (from the local location database) all non-active registration;
- send the `'200 OK'` response towards the SIP terminal; and
- clear all resources used during the registration.

5.3.3.2 Exceptional procedures

If the SIP proxy does not have a business agreement suitable to forward the REGISTER message to a next-hop location (either another SIP proxy in an intermediate network or the SIP registrar in the home network), the SIP proxy shall decline the registration request, and respond with `'403 Forbidden'` message.

On receipt of 3xx, 4xx or 5xx responses, procedure in [2] clause "*Response processing*" applies.

If the supervision timer (for the supervision of a response to the REGISTER message) expires the SIP proxy shall silently clear all resources used by the session.

6 Simple Call Application

The intentions with this clause are to describe the simple call application using procedures in [2] and map those procedures to the architecture of TS 101 314 [1] and to the Meta-protocol in TS 101 882 [7] annex B "*Meta Protocol at reference point C"*.

Two scenarios shall be supported:

- the "user at home" scenario; and
- the "roaming user" scenario.

NOTE: For details about the two scenarios (including some examples) see the TS 101 315 [5].

6.1 General behaviour

This clause describes some general behaviour during call establishment.

6.1.1 Timers

This clause applies to the SIP terminal, the SIP proxy in the serving network, the SIP proxy in the intermediate network and the SIP proxy in the home network.

Timers shall be implemented according to the SIP RFC [2] clause 17.1.1 "*INVITE Client Transaction*" with the clarifications below:

- The value of T1 shall be 500 ms.

6.1.1.1 Timer A

The timer A is a retransmission timer and shall be started upon a request message related to call establishment i.e. an INVITE, a CANCEL, a BYE, an ACK or a PRACK message and stopped on receipt of any response.

On timer expiry procedures in [2] clause 17.1.1.1 "*Formal description*" shall apply. This implies that the request will be transmitted 7 times before the timer B (see clause 6.1.1.2 "*Timer B*" of the present document) expires.

6.1.1.2 Timer B

The timer B is a timer supervising any response to a request. Timer B shall be started when a request is sent, and stopped when receiving a response to the request. This implies that if a SIP proxy forks a request a timer B shall supervise each request.

NOTE: Timer B corresponds to the timer TC001 in TS 101 882 [7] with a value of 32 s (64 × T1).

On expiry of timer B the actual leg (on which the request is sent) shall be cleared. This may imply that a whole call is cleared depending on the situation. For example if a SIP proxy receives a PRACK from the called party and sends it towards the calling party. On timer B expiry the leg towards the calling party is cleared. A call without a calling party seems to be useless thus the SIP proxy clears the leg towards the called party (in this case by means of a CANCEL) message.

6.1.1.3 Timer C

Timer C is a timer supervising a final response to an INVITE message in a SIP proxy. The timer is started when the INVITE message is sent and stops when a final response is received.

On expiry of timer C procedures in SIP RFC [2] clause 16.7 "*Processing timer C*" shall apply.

The value of C is 3 minutes.

6.1.1.4 Timer D

Timer D is a timer supervising a final response to an INVITE message in a SIP terminal. The timer is started when the INVITE message is sent and stops when a final response is received.

On expiry of timer D the call shall be cancelled by means of a CANCEL request towards the called party.

The value of C is 3 minutes.

6.1.2 100rel (early media)

The SIP RFC [2] allows extensions. One extension (included in the standard RFC) is the 100rel [8]. The SIP terminal and the SIP gateway shall support the 100rel [8] extension. This implies that:

- the INVITE message shall include the `'SUPPORTED"` header field with the value 100rel;
- any provisional response shall include the `'REQUIRE"` header field with the value 100rel when SDP is included;
- on receipt of a provisional response (indicating 100rel as required) the PRACK [8] message shall be sent;
- on receipt of the PRACK message in a SIP terminal or in the SIP gateway the `'200 OK'` message shall be returned;

SIP proxies controlling media flows through ICF shall support the 100rel extension. This implies that:

- On receipt of a provisional response with SDP, included bearer related information shall be communicated to the ICF and the resulting modification of the SDP shall be included in the provisional response towards the calling party. For more information about ICF related functionality see clause 6.1.3 "Resource reservation at ICF" of the present document.

6.1.3 Resource Reservation at ICF

This clause applies to the SIP proxy in the serving network, the SIP proxy in the intermediate network and the SIP proxy in the home network.

If a proxy requires the media to flow through an intermediate ICF the procedures below applies.

NOTE: The reference point between the proxy and the ICF is the N2 reference point. The message flow over the N2 reference point is out of scope of the present document. See TS 101 314 [1] for more information about ICF and the reference point N2.

6.1.3.1 Normal procedure

On receipt of the INVITE message the SIP proxy shall inform its ICF about the bearer information received in the SDP. The ICF may return modified bearer information.

The SIP proxy shall replace the SDP received in the INVITE with modified bearer information received from the ICF and include the modified SDP in the INVITE message towards the called party.

On receipt of the SDP in a provisional (reliable) response or the `'200 OK'` final response the SIP proxy shall inform its ICF about the bearer information received in the SDP. The ICF may return modified bearer information.

The SIP proxy shall replace the SDP received in a provisional (reliable) response or the `'200 OK'` final response with modified bearer information received from the ICF and include the modified SDP in the response towards the calling party.

6.1.3.2 Exceptional procedures

On receipt of more than one SDP answer the SIP proxy shall store each SDP response.

NOTE: In case more than one provisional response with SDP is received its ICF shall be notified for each one of them (resulting in more than one reservation path in e.g. a firewall).

On receipt of an ACK message from the SIP terminal the SIP proxy shall associate (and use) the corresponding SDP answer (received in a provisional response or in the `'200 OK'` final response).

6.2 Procedures for Call Set-up at the calling party's SIP terminal

This clause shall apply for all SIP terminals initiating a call.

Before a user may initiate a call (in [2] defined as a "session") the User shall register according to the procedures described in clause 5 of the present document.

For procedures related to timer A, B and D see clause 6.1.1 "*Timers*".

For procedures related to the 100rel extension see clause 6.1.2 "*100rel (early media*)".

6.2.1 Call establishment

The SIP terminal shall initiate the call by means of the INVITE message. The INVITE message shall be created according to [2] clause 13.2.1 "*Creating the Initial INVITE*" and clause 8.1.1 "*Generating the Request*" with the clarifications below:

- the `'REQUEST-URI"` shall be set to the value of the URI in the `'TO"` header field;
- the `'TO"` header field is a public identity identifying the called party. It shall be in the format of a SIP-URL;
- the `'FROM"` header field is a public identity identifying the calling party. It shall be in the format of an SIP-URL;
- the `'MAX-FORWARDS"` header field shall be initiated with the value 70;
- the `'CONTACT"` header field shall be a contact address registered for the public identity in the `'FROM"` header field;
- the INVITE shall use the first SDP offer/answer model and include SDP (offer) in the message body;
- if authentication is required, the INVITE message shall include the `'AUTHORIZATION"` header field. The "username" in the `'AUTHORIZATION"` header field shall include the private identity of the calling party;
- the SIP terminal shall send the INVITE message to the IP address stored during registration i.e. the same address to where the last REGISTER message was sent (and a `'200 OK'` final response received from).

On receipt of provisional responses the procedures in [2] clause 13.2.2 "*Processing INVITE Responses*" shall apply with the following clarification:

- On receipt of the `'180 Ringing'` response, the human user shall be informed that the called party has been located and notified of an incoming call.

NOTE: The method deployed (audio or visual) to inform the user is outside the scope of the present document. Procedures as per SIP RFC [2] shall apply upon receipt of `'180 Ringing'`.

On receipt of the `'200 OK'` normal SIP RFC [2] procedures shall apply.

6.2.2 Call Clear Down

The SIP terminal may initiate release of a call using the BYE message according to the procedures in [2] clause 15.1.2 "*UAC Behaviour*":

- the SIP terminal shall use the CANCEL request message before the call is answered (active);
- the SIP terminal shall use the BYE request message during an active call;
- the SIP terminal shall not send any media after that the BYE/CANCEL message is sent; and
- the `'TO"`, `'FROM"`, `'CALLID"` and the `'REQUEST-URI"` header fields shall be the same as in the original INVITE message while the `'CSEQ"` header field shall be set according to [2] clause 12.2.1.1 "*Generating the Request*".

On receipt of a BYE request the SIP terminal procedures in [2] clause 15.1.2 "*UAS Behaviour*" shall apply.

NOTE: The receiver of a request (in this the BYE request) is a User Agent Server (UAS), by definition in SIP.

6.2.3 Exceptional procedures

If authentication is required the SIP terminal receives the `'407 Proxy authentication required'` response. On receipt of the `'407 Proxy authentication required'` response the SIP terminal shall retransmit the INVITE message according to clause 6.2.1 of the present document but this time include the `'AUTHORIZATION"` header field.

On receipt of more than one SDP answer the SIP terminal shall store each SDP response.

On receipt of more than one `'200 OK'` response to the INVITE message the SIP terminal shall select one response and initiate clearing of the non-selected `'200 OK'` responses. The SIP terminal shall use the corresponding SDP answer (received in a provisional response).

On receipt of 3xx, 4xx, 5xx and 6xx final response messages the procedures in the SIP RFC [2] clause 13.2.2 "*Processing INVITE Responses*" shall apply.

If the SIP terminal is unable to match the BYE message with an existing call the SIP terminal shall reject the BYE with the `'481 Call/Transaction Does Not Exist'` final response.

6.3 Procedures in the Serving and intermediate network (calling party)

This clause applies to SIP proxies in the serving network and in the intermediate network of the calling party.

NOTE: The SIP terminology for the SIP proxy in the serving network and in the intermediate network is "outbound proxy".

For procedures related to timer A, C and D see clause 6.1.1 "*Timers*" of the present document.

For procedures related to the 100rel extension see clause 6.1.2 "*100rel (early media)*".

For procedures related to the ICF see clause 6.1.3 "*Resource Reservation at ICF*" of the present document.

6.3.1 Call establishment

The SIP proxy shall follow the procedures described in [2] clause 16 "*Proxy behaviour*" with the following clarifications:

- the SIP proxy shall perform the "Reasonable Syntax check" and the "Max-Forward check" as defined in SIP RFC [2] clause 16.3 "*Request validation*";
- the SIP proxy shall identify the registration using the `'FROM"` header field and the `'CONTACT"` header field and use the IP address stored in the local location database during the registration as the "next-hop location";

- the SIP proxy shall use the same `'REQUEST-URI"` for the outgoing INVITE message as received in the incoming INVITE message;
- the SIP proxy shall place itself in the `'RECORD-ROUTE"` (considering the handling of the `'RECORD-ROUTE"` header field as defined in [2] clause 16.4 "*Making a Routing decision*");
- the SIP proxy shall process the INVITE message as described in [2] clause "*Request Processing*"; and
- finally, the INVITE message is sent to the next-hop location.

On receipt of provisional responses the serving network and the intermediate network shall forward the message towards the SIP terminal according to [2] clause 16.6 "*Response Processing*".

6.3.2 Call clearing

The SIP proxy in the serving network or in the intermediate network shall participate in the call clearing as described in [2] clause 16 "*Proxy Behaviour*".

6.3.3 Exceptional procedures

On receipt of a 3xx, a 4xx, a 5xx or a 6xx final response message procedures in SIP RFC [2] clause 16.6 "*Response processing*".

6.4 Procedures in the SIP proxy in the home network (Calling Party)

This clause applies to SIP proxies in the serving network and in the intermediate network of the calling party.

NOTE: The SIP RFC [2] terminology for the SIP proxy in the home network is "inbound proxy".

For procedures related to timer A, C and D see clause 6.1.1 "*Timers*" of the present document.

For procedures related to the 100rel extension see clause 6.1.2 "*100rel (early media)*".

For procedures related to the ICF see clause 6.1.3 "*Resource Reservation at ICF*" of the present document.

6.4.1 Call establishment

On the receipt of the INVITE message in the SIP proxy in the home network procedures described in [2], clause 16 "*Proxy Behaviour*" applies with the clarification below:

- the SIP proxy shall perform the "Reasonable Syntax Check" and the "Max-Forward check" as defined in [2] clause 16.3 "*Request validation*";
- the calling user shall be authenticated. The calling user is identified by the user's private identity in the "username" parameter of the `'AUTHORIZATION"` header field;
- the SIP proxy shall determine next-hop location based on the contents of the `'TO"` header field;
- the `'REQUEST-URI"` header field shall be checked for the destination address and any service code. The service code may represent the request for a number of services including, but not limited to:
  - carrier selection;
  - priority call; or
  - emergency call.

NOTE 1: The routing to the next-hop location outside the home network domain assumes that a business agreement exists between the home network and the next-hop location, which is outside the scope of the present document.

- the SIP proxy shall send an INVITE message to the next-hop location with a contents as described in [2] clause 16.5 "*Request processing*" with the following clarifications:
  - the SIP proxy shall place itself in the `'RECORD-ROUTE"` (considering the handling of the `'RECORD-ROUTE"` header field as defined in [2] clause 16.4 "*Making a Routing decision*");
  - the `'REQUEST-URI"` should include the address of the called party;

NOTE 2: The normal case is that the `'REQUEST-URI"` includes the identity of the called party. However, in some cases the `'REQUEST-URI"` may be modified (e.g. include a service code) in order to route the call along another path than normally, e.g. when a number is ported.

- the INVITE message shall be sent to the next-hop location; and
- on receipt of provisional response messages to the INVITE, procedures according to [2] clause 16.6 "*Response Processing*" shall apply.

6.4.2 Call Clearing

The SIP proxy in the serving network or in the intermediate network shall participate in the call clearing as described in [2] clause 16 "*Proxy Behaviour*" with the clarifications below.

On receipt of the BYE or the CANCEL message from the called party the SIP proxy shall authenticate the User using the `'AUTHORIZATION"` header field where the "username" is the private identity of the user.

6.4.3 Exceptional procedures

If the Authentication fails, the SIP proxy in the home network shall reject the INVITE, CANCEL and the BYE messages using the `'407 Proxy authentication required'` response message. The `'PROXY-AUTHENTICATE'` header field shall include the `'digest"` parameter and a challenge.

On receipt of 3xx, 4xx, 5xx and 6xx series responses normal procedures described in [2] clause 16.6 "*Response Processing*" shall apply.

6.5 Procedures at the SIP proxy in the Intermediate network

The procedures in this clause shall apply for all SIP proxies in the intermediate network between the Originating Network and the Terminating Network.

There may be zero or more SIP proxies in intermediate networks involved in a call. The role of a SIP proxy in an intermediate network is to receive a request, make a routing decision, and forward the request to the next-hop location. The SIP proxy shall stay in the call-signalling path.

NOTE: The SIP terminology for the SIP proxy in the intermediate network is "outbound proxy".

For procedures related to timer A, C and D see clause 6.1.1 "*Timers*" of the present document.

For procedures related to the 100rel extension see clause 6.1.2 "*100rel (early media)*".

For procedures related to the ICF see clause 6.1.3 "*Resource Reservation at ICF*" of the present document.

6.5.1 Call establishment

On receipt of the INVITE request the SIP proxy in the intermediate network shall follow the procedures described in [2] clause 16 "*Proxy behaviour*" with the clarifications below.

- The SIP RFC [2] clause 16.3 "*Request validation*" describes how the received message shall be checked. The SIP proxy shall perform the following checks:
  - Reasonable syntax check; and
  - Max-Forward check.

- The SIP proxy shall determine next-hop location as described in [2] clause 16.4 "*Making a routing decision*" based on the `'REQUEST-URI"`; and
- the SIP proxy shall forward the INVITE message to the next-hop location using the received INVITE message as the input and modify the INVITE message as described in [2] clause 16.5 "*Request processing*" with the following clarifications:
  - a `'RECORD-ROUTE"` header field shall be inserted by the SIP proxy; and
  - the SIP proxy shall return a `'100 Trying'` response to the sender (previous-hop) of the INVITE message.

On receipt of provisional responses procedures according to the SIP RFC [2] shall apply.

6.5.2 Call clearing

The SIP proxy in the serving network or in the intermediate network shall participate in the call clearing as described in [2] clause 16 "*Proxy Behaviour*".

6.5.3 Exceptional procedures

On receipt of 3xx, 4xx, 5xx and 6xx series responses normal procedures described in [2] clause 16.6 "*Response Processing*" shall apply.

6.6 Procedures at the SIP proxy in the home network (called party)

This clause applies to the SIP proxy in the home network for the called party.

NOTE: The SIP [2] terminology for the SIP proxy in the home network is "inbound proxy".

The SIP proxy in the home network shall authenticate the previous SIP proxy (e.g. the SIP proxy in the intermediate network) by means outside the scope of the present document. In case the SIP proxy cannot allow the call a relevant reject response shall be returned.

For procedures related to timer A, C and D see clause 6.1.1 "*Timers*" of the present document.

For procedures related to the 100rel extension see clause 6.1.2 "*100rel (early media)*".

For procedures related to the ICF see clause 6.1.3 "*Resource Reservation at ICF*" of the present document.

6.6.1 Call establishment

On receipt of the INVITE message the SIP proxy shall follow the procedures in [2] clause 16 "*Proxy Behaviour*" with the following clarifications:

- the SIP proxy shall perform the "Reasonable Syntax Check" and "Max-Forward check" as defined in [2] clause 16.3 "*Request validation*";
- the SIP proxy shall determine the next-hop based on stored contact addresses for the identity in the `'TO"` header field. If the user is registered with more than one contact address more than one next-hop location may be found;
- the SIP proxy shall place itself in the `'RECORD-ROUTE"` (considering the handling of the `'RECORD-ROUTE"` header field as defined in [2] clause 16.4 "*Making a Routing decision*");
- the SIP proxy shall send an INVITE message to each next-hop location and replace the received `'REQUEST-URI"` with the next-hop location address (in the form of a SIP-URL). If more than one next-hop location is present INVITE messages shall be sent according to the `'q"` value in the contact address (stored during registration). This implies that INVITE messages may be sent in serial or in parallel (forking).

On receipt of provisional response, messages to the INVITE procedures according to [2] clause 16.6 "*Response Processing*" shall apply.

On receipt of the `'200 OK'` final response procedures according to [2] shall apply with the clarification below.

- The `'200 OK'` shall be forwarded towards the calling party;
- if more than one INVITE was sent, the extra INVITE message(s) shall be cancelled according to the procedures in [2] clause 16.9 "*CANCEL Processing*"; and
- forward any `'200 OK'` final responses received after cancellation of extra INVITE message has been initiated.

6.6.2 Call clearing

The SIP proxy in the serving network or in the intermediate network shall participate in the call clearing as described in SIP RFC [2] clause 16 "*Proxy Behaviour*" with the clarifications below.

- On receipt of the BYE message from the called party the SIP proxy shall authenticate the User using the `'AUTHORIZATION"` header field where the "username" is the private identity of the user.

6.6.3 Exceptional procedures

The SIP proxy in the home network shall locate the called party using the registration information in the registrar. If the called party is not registered, and no supplementary service is available to handle unregistered users, then the Call shall be rejected, and an appropriate final response shall be sent back to the caller. The supplementary service may be to forward the call to a voice mail box; or

on receipt of 3xx, 4xx, 5xx and 6xx series responses normal procedures described in [2] clause 16.6 "*Response Processing*" shall apply. However the SIP proxy may invoke a supplementary service e.g. forward the call on busy, no answer, etc. Handling of supplementary service is out of scope of the present document.

If the authentication fails, the SIP proxy in the home network shall reject the BYE messages using the `'407 Proxy authentication required'` response message. The 'PROXY-AUTHENTICATE' header field shall include the `'digest"` parameter and a challenge.

6.7 Procedures in the Serving and intermediate network (called party)

This clause applies to SIP proxies in the serving network and in the intermediate network of the called party.

NOTE: The SIP [2] terminology for the SIP proxy in the serving network and in the intermediate network is "outbound proxy".

For procedures related to timer A, C and D see clause 6.1.1 "*Timers*" of the present document.

For procedures related to the 100rel extension see clause 6.1.2 "*100rel (early media)*".

For procedures related to the ICF see clause 6.1.3 "*Resource Reservation at ICF*" of the present document.

6.7.1 Call establishment

The SIP proxy shall follow the procedures described in SIP RFC [2] clause 16 "*Proxy behaviour*" with the following clarifications:

- the SIP proxy shall perform the "Reasonable Syntax check" and the "Max-Forward check" as defined in [2] clause 16.3 "*Request validation*";
- the SIP proxy shall replace the `'REQUEST-URI"` for the INVITE message with the stored contact address of the called party;
- the SIP proxy shall place itself in the `'RECORD-ROUTE"` (considering the handling of the `'RECORD-ROUTE"` header field as defined in [2] clause 16.4 "*Making a Routing decision*");

- the SIP proxy shall process the INVITE message as described in the SIP RFC [2] clause "*Request Processing*"*;* and
- finally, the INVITE message is sent to the IP address of the called party, determined by the contact address.

On receipt of provisional responses the serving network and the intermediate network shall forward the message towards the SIP terminal according to [2] clause 16.6 "*Response Processing*".

6.7.2 Call clearing

The SIP proxy in the serving network or in the intermediate network shall participate in the call clearing as described in SIP RFC [2] clause 16 "*Proxy Behaviour*".

6.7.3 Exceptional procedures

On receipt of a 3xx, a 4xx, a 5xx or a 6xx final response message procedures in SIP RFC [2] clause 16.6 "*Response processing*".

6.8 Procedures at the called party's SIP terminal

This clause applies to SIP terminals capable of receiving calls.

NOTE: The procedure in the terminal includes user interactions outside the scope of the present document. The procedure in the SIP terminal also includes communication with the lower layers of the SIP terminal (e.g. select codec etc) over the N1 reference point. The message flow over the reference point N1 is out of scope of the present document thus not described. For more details about possible user interactions and message flows over the N1 reference point see the TS 101 314 [1].

For procedures related to timer A, C and D see clause 6.1.1 "*Timers*" of the present document.

6.8.1 Call establishment

On receipt of the INVITE message procedures described in SIP RFC [2] clause 13.3 "*Callee Processing*" with the clarifications below.

- The SIP terminal shall:
  - generate a `'100 Trying'` response;
  - process the request (this includes checking the SDP offer received in the INVITE message); and
  - inform the user of the arrival of the call.

The SIP terminal shall return a `'180 Ringing'` provisional response.

The SIP terminal shall wait for an indication from the user that the user wishes to accept the call.

When such an indication is received the procedures in SIP RFC [2] clause 13.3.1.4 "*The INVITE is accepted*" shall apply with the following clarifications:

- `'200 OK'` final response shall be returned carrying the SDP answer.

6.8.2 Call clearing

The SIP terminal may initiate release of a call using the BYE message according to the procedures in the SIP RFC [2] clause 15.1.2 "*UAC Behaviour*".

NOTE: The sender of a request (in this case the BYE request) is by definition a SIP UAC.

- The SIP terminal shall use the BYE request message during an active call;
- the SIP terminal shall not send any media after that the BYE message is sent; and

- the `'TO"`, `'FROM"`, `'CALLID"` and the `'REQUEST-URI"` header fields shall be the same as in the original INVITE message while the `'CSEQ"` header field shall be set according to the SIP RFC [2] clause 12.2.1.1 "*Generating the Request*".

On receipt of a BYE request the SIP terminal procedures in [2] clause 15.1.2 "*UAS Behaviour*" shall apply.

6.8.3 Exceptional procedures

The behaviour in the SIP terminal is implementation dependent.

- The SIP terminal may implement services allowing the SIP terminal to redirect incoming calls;
- the user may reject the call due to many reasons;
- the set of codecs may not match the codec set received in the SDP offer.

Whatever reasons, the procedures in SIP RFC [2] clauses 13.3.1.2 "*The INVITE is redirected*" or 13.3.1.3 "*The INVITE is rejected*" shall apply.

If the INVITE message is received without SDP the call shall be rejected with the `'400 Bad request'` response.

If the SIP terminal is unable to match the BYE message with an existing call the SIP terminal shall reject the BYE with the `'481 Call/Transaction Does Not Exist'` final response.

6.9 Procedures at the SIP gateway: IP to SCN

This clause shall apply for all SIP gateways terminating calls to SCN.

This clause describes the behaviour at a SIP gateway for terminating. The SIP gateway is connected to the SCN. The protocol used between the SCN and the SIP gateway is out of scope of the present document. However, when required for readability reasons some generic SCN terminology is used to describe the behaviour of SCN.

For procedures related to timer A, B and D see clause 6.1.1 "*Timers*" of the present document.

For procedures related to the 100rel extension see clause 6.1.2 "*100rel (early media)*" of the present document.

6.9.1 Call establishment

On receipt of the INVITE message the procedures in SIP RFC [2] clause 13.3 "*Callee Processing*" with the clarifications below.

- The SIP gateway shall:
  - generate a `'100 Trying'` response;
  - process the request (this includes checking the SDP offer received in the INVITE message); and
- the SIP terminal shall return a `'183 Progress'` provisional response.

The `'183 Progress'` provisional response shall be sent reliably. This implies that the `'REQUIRED"` header field shall indicate 100rel, see clause 6.1.2 "*100rel (early media)*" of the present document.

On receipt of the PRACK message the call shall be initiated towards the SCN. The SIP gateway shall:

- use the `'REQUEST-URI"` header field (as base) for the *`'called party number'`* information element towards the SCN; and
- use the `'FROM"` header field (as the base) for the `'calling party number'` information element towards the SCN.

NOTE 1: The `'FROM"` header field can only be used when the INVITE is received from a trusted SIP proxy. If the SIP proxy is not trusted a default gateway *calling party number* information element is used instead.

On receipt of an alerting indication from SCN (traditional an ALERTING, an ACM or a CPG message depending on scenario) the SIP gateway shall return a `'180 Alerting'` provisional response.

NOTE 2: Provisional reliable responses are only required for responses carrying SDP.

On receipt of an answer indication from the SCN (traditional a CONNECT, an ANM or a CON message depending on scenario) the SIP gateway shall send a `'200 OK'` final response towards the calling party according to procedures in SIP RFC [2] clause 13.3.1.4 "*The INVITE is accepted*".

6.9.2 Call clearing

The SIP gateway may initiate release of a call using the BYE message according to the procedures in the SIP RFC [2] clause 15.1.2 "*UAC Behaviour*".

NOTE: The sender of a request (in this case the BYE request) is by definition a SIP UAC.

- The SIP gateway shall use the BYE request message during an active call;
- the SIP gateway shall not send any media after the BYE message has been sent; and
- the `'TO"`, `'FROM"`, `'CALLID"` and the `'REQUEST-URI"` header fields shall be the same as in the original INVITE message while the `'CSEQ"` header field shall be set according to 2] clause 12.2.1.1 "*Generating the Request*".

On receipt of a BYE request, procedures in [2] clause 15.1.2 "*UAS Behaviour*" shall apply.

On receipt of a CANCEL request procedures in [2] clause 15 "*Terminating a Session*" shall apply.

6.9.3 Exceptional Procedures

The SIP gateway may reject the call due to many reasons. Reasons for rejecting an INVITE request can be that the set of codecs does not match the codec set received in the SDP offer, etc. Whatever reasons the procedures in SIP RFC [2] clauses 13.3.1.2 "*The INVITE is redirected*" or 13.3.1.3 "*The INVITE is rejected*" shall apply.

If the INVITE message is received without SDP the call shall be rejected with the `'400 Bad request'` response.

If the SIP terminal is unable to match the BYE message with an existing call the SIP terminal shall reject the BYE with the `'481 Call/Transaction Does Not Exist'` final response.

6.10 Procedures for Call Set-up at SIP gateway: SCN to IP

This clause shall apply for all SIP gateways initiating a call.

This clause describes the behaviour at a SIP gateway for establishing a call. The SIP gateway is connected to the SCN. The protocol used between the SCN and the SIP gateway is out of scope of the present document. However, when required for readability reasons some generic SCN terminology is used to describe the behaviour of SCN.

For procedures related to timer A, B and D see clause 6.1.1 "*Timers*" of the present document.

For procedures related to the 100rel extension see clause 6.1.2 "*100rel (early media)*" of the present document.

6.10.1 Call establishment

The SIP gateway shall initiate the call by means of the INVITE message. The INVITE message shall be created according to the SIP RFC [2] clause 13.2.1 "*Creating the Initial INVITE*" and clause 8.1.1 "*Generating the Request*" with the clarifications below:

- the `'REQUEST-URI"` shall be based on the value in the *called party number* information element received from the SCN. The `'REQUEST-URI"` shall be in the format of a TEL-URL;

- the `'TO"` header field is a public identity identifying the called party. It shall be in the format of a SIP-URL and based on the *called party number* information element (*called party* number@domain) where the "domain" is based on information retrieved from a database (e.g. a number portability database or a pre-configured database where number plans and number ranges are associated with a specific domain);
- the `'FROM"` header field is a public identity identifying the calling party. It shall be in the format of an SIP-URL and based on the *calling party number* information element (*calling party number@gateway)*. In the case SCN indicates a restriction to display the contents of the *calling party number* a meaningless URI shall be used instead, see SIP RFC [2] clause 8.1.1.3 "*From*";
- the `'MAX-FORWARDS"` header field shall be initiated with the value 70;
- the `'CONTACT"` header field shall be the address of the SIP gateway (*sip://gateway*);
- the INVITE shall use the first SDP offer/answer model and include SDP (offer) in the message body;
- if authentication is required, the INVITE message shall include the `'AUTHORIZATION"` header field. The "username" in the `'AUTHORIZATION"` header field shall include the private identity of the calling party;

NOTE 1: The "username" in this case is the name of the SIP gateway.

- the SIP gateway shall send the INVITE message to a pre-configured IP address (based on information retrieved from a database e.g. a number portability database or a pre-configured database where number plans and number ranges are associated with a specific domain) or the IP address received from the DNS using the `'REQUEST-URI"` header field (this implies that a DNS with ENUM functionality is present).

On receipt of provisional responses the procedures in SIP RFC [2] clause 13.2.2 "*Processing INVITE Responses*" shall apply with the following clarification:

- on receipt of the `'180 Ringing'` response the SCN shall be informed that the called party has been located and notified of the incoming call. This notification includes an inband ringing tone applied by the gateway, towards the calling party.

NOTE 2: The message to be used on the SCN side is out of scope of the present document. However, traditional messages like ALERTING, ACM or CPG may be appropriate.

On receipt of the `'200 OK'` normal SIP RFC [2] procedures shall apply.

6.10.2 Call clearing

The SIP gateway may clear an ongoing call according to the procedures described in the SIP RFC [2] clause 15.1.1 "*UAC behaviour*" with the clarifications below:

- the SIP gateway shall use the CANCEL request message before the call is answered (active);
- the SIP gateway shall use the BYE request message during an active call;
- the SIP gateway shall not send any media after that the BYE/CANCEL message has been sent; and
- the `'TO"`, `'FROM"`, `'CALLID"` and the `'REQUEST-URI"` header fields shall be the same as in the original INVITE message while the `'CSEQ"` header field shall be set according to 2] clause 12.2.1.1 "*Generating the Request*".

6.10.3 Exceptional procedures

If authentication is required the SIP gateway receives the `'407 Proxy authentication required'` response. On receipt of the `'407 Proxy authentication required'` response the SIP gateway shall retransmit the INVITE message according to clause 6.2.1 (in the present document) but this time include the `'AUTHORIZATION"` header field.

NOTE: The above is based on bilateral business agreement (out of scope of the present document) where the SIP proxy sending the `'407 Proxy authentication required'` and the SIP gateway shares a secret and the "username" is the agreed name of the SIP gateway.

On receipt of more than one SDP answer the SIP gateway shall store each SDP response.

On receipt of more than one `'200 OK'` response to the INVITE message the SIP gateway shall select one response and initiate clearing of the non-selected `'200 OK'` responses. The SIP terminal shall use the corresponding SDP answer (received in a provisional response).

On receipt of 3xx, 4xx, 5xx and 6xx final response messages the procedures in the SIP RFC [2] clause 13.2.2 "*Processing INVITE Responses*" shall apply.

Annex A (normative): Mapping of TIPHON Registration Meta-protocol to SIP

A.1 Registration Messages Mapping

Table A.1 shows the mapping of TIPHON Registration meta-protocol messages to the SIP messages.

Table A.1: Mapping of SIP messages to TIPHON Registration MPMUs

TIPHON message	SIP messages
U-SpoAServiceAttachRequest	REGISTER
D_SpoAServiceAttachResponse	200 OK, 300, 301, 302
D-SpoAServiceAttachReject	400, 401, 402, 403, 407, 415, 500, 503, 504
U_SpoAServiceDetachRequest	REGISTER (EXPIRE = 0)
D_SpoAServiceDetachResponse	200 OK

A.2 Detailed mapping of TIPHON Registration parameters to SIP

Table A.2: Mapping of SIP to U_SpoAServiceAttachRequest

TIPHON message & parameters			Status	SIP message & Parameters
U_SpoAServiceAttachReq				REGISTER
Registration ID			M	
	Registrar ID		M	Req URI
	Registrant ID		M	TO
	Registrar Location		M	
		Protocol ID	M	SIP/2.0/UDP
		Name/Address	M	URI
		Port	O	Port number (= 5060)
Service Request Ticket			M	NOT SUPPORTED
	Registrar ID		M	'host part' of Request-URI
	Registrant ID		M	User part of 'TO" header
	Service Credentials		M	
		Service App ID	M	Implicit in Server ID
		SpoA	M	Request-URI
		Start Time	M	Implicit in EXPIRES
		Stop Time	M	Implicit in EXPIRES
		Crypto Digest	O	
	Crypto Digest		O	

Table A.3: Mapping of SIP to D_SpoAServiceAttachResponse

TIPHON parameters				SIP Parameters
D_SpoAServiceResponse				200 OK, 300, 301, 302
Registration ID			M	
	Registrar ID		M	'host part' of Request-URI
	Registrant ID		M	User part of 'TO" header
	Registrar Location		M	
		Protocol ID	M	SIP/2.0
		Name/Address	M	URI
		Port	O	Port number (5060)
Service Request Ticket			M	NOT SUPPORTED
	Registrar ID		M	'host part' of Request-URI
	Registrant ID		M	User part of 'TO" header
	Service Credentials		M	NOT SUPPORTED
		Service App ID	M	Implicit in Server ID
		SpoA	M	Request-URI
		Start Time	M	Implicit in EXPIRES
		Stop Time	M	Implicit in EXPIRES
		Crypto Digest	O	
	Crypto Digest		O	

Table A.4: Mapping of SIP to D_SpoAServiceReject

TIPHON parameters				SIP Parameters
'D_SpoAServiceReject'				4, 5, 6 series responses
Registration ID			M	
	Registrar ID		M	'host part' of Request-URI
	Registrant ID		M	User part of 'TO" header
	Registrar Location		M	
		Protocol ID	M	SIP/2.0
		Name/Address	M	URI
		Port	O	Port number (5060)
Service Reject Reason			M	
	Service Application ID		M	Implicit in Server ID
	Reject Reason		M	
		Reason	M	400 401 402 403 407 415 500 503 504
		Diagnostic	O	Information headers in the above responses
		Free Text	O	Above Reasons in Text

Table A.5: Mapping of SIP to U_SpoAServiceDetachRequest

TIPHON Message				SIP Message
U_SpoAServiceDettachReq				REGISTER (Expires = 0)
Registration ID			M	
	Registrar ID		M	'host part' of Request-URI
	Registrant ID		M	User part of 'TO" header
	Registrar Location		M	
		Protocol ID	M	SIP/2.0
		Name/Address	M	URI
		Port	O	Port number (5060)
Service Request Ticket			M	NOT SUPPORTED
	Registrar ID		M	'host part' of Request-URI
	Registrant ID		M	User part of 'TO" header
	Service Credentials		M	NOT SUPPORTED
		Service App ID	M	Implicit in Server ID
		SpoA	M	Request-URI
		Start Time	M	Implicit in EXPIRES
		Stop Time	M	Implicit in EXPIRES
		Crypto Digest	O	
	Crypto Digest		O	

Table A.6: Mapping of SIP to D_SpoAServiceDettachResponse

TIPHON parameters				SIP Parameters
D_SpoAServiceDettachResponse				200 OK
Registration ID			M	
	Registrar ID		M	'host part' of Request-URI
	Registrant ID		M	User part of 'TO" header
	Registrar Location		M	
		Protocol ID	M	SIP/2.0
		Name/Address	M	URI
		Port	O	Port number (5060)
Service Detach Flag			M	Implicit in 200 OK

Annex B (normative): Mapping of SIP to TIPHON Call Control meta-protocol

This clause shows the mapping of SIP to TIPHON Call Control Meta-Protocol.

Table B.1: Mapping of SIP to U_CallRequest

TIPHON message:				Information elements in SIP Message
U_Call Request			Status	INVITE
Call Id			M	Call ID
Calling Party Restriction			M	Anonymous header (note 1)
Calling Party Id			C	FROM
called party Id			M	TO
Call priority			O	Priority
Operator Selection (C2)			O	NOT SUPPORTED
Service Offer Ticket	Registrant ID		M	NOT SUPPORTED (note 2)
	Registrar Id		M	
	Service Credentials	Service App Id	M	
		spoA	M	
		Start Time	M	
		Stop Time	M	
		Crypto Digest	O	
	Crypto Digest		O	
NOTE 1: 'Anonymous' header is an extension defined by the DSC Cable labs. NOTE 2: Service offer Ticket is not supported by SIP. NOTE 3: Bearer ID missing from the MPMU.				

Table B.2: Mapping of SIP to D_Call Request

TIPHON message:		Information elements in SIP Message
D_Call Request	Status	INVITE
Call Id	M	Call ID
Calling Party Restriction	C	Anonymous header (note)
Calling Party Id	O	FROM
called party Id	M	TO
Call priority	O	Priority
NOTE: 'Anonymous' header is an extension defined by the DSC Cable labs.		

Table B.3: Mapping of SIP to NW_CallRequest

TIPHON message:		Information elements in SIP Message
NW_Call Request	Status	INVITE
Call Id	M	Call ID
Calling Party Restriction	C	Anonymous header (note)
Calling Party Id	C	FROM
called party Id	M	TO
Call priority	M	Priority
NOTE: 'Anonymous' header is an extension defined by the DSC Cable labs.		

Table B.4: Mapping of SIP to D_Call Reject

TIPHON message:		Information elements in SIP Message
D_Call Reject	Status	4,5,6 series responses
Call Id	M	Call ID
Call Reject Reason	M	Note
NOTE: See Reject reasons in table 20.		

Table B.5: Mapping of SIP to D_Call Report

TIPHON message:			Information elements in SIP Message
D_Call Report		Status	100, 180, 183, 484 responses
Call Id		M	Call ID
Report Reason		M	
	Address Complete		183 SESSION IN PROGRESS
	Address Incomplete		484 ADDRESS INCOMPLETE
	Call Proceeding		100 TRYING
	Call Alerting		180 RINGING
Report Parameters		C	

Table B.6: Mapping of SIP to NW_Call Report

TIPHON message:			Information elements in SIP Message
NW_Call Report		Status	100, 180, 183, 484 responses
Call Id		M	Call ID
Report Reason		M	
	Address Complete		183 SESSION IN PROGRESS
	Address Incomplete		484 ADDRESS INCOMPLETE
	Call Proceeding		100 TRYING
	Call Alerting		180 RINGING
Report Parameters		C	

Table B.7: Mapping of SIP to U_Call Alert

TIPHON message:		Information elements in SIP Message
U_Call Alert	status	180 RINGING
Call ID	M	Call ID

Table B.8: Mapping of SIP to U_CCAdditional Digits

TIPHON message:		Information elements in SIP Message
U_CCAdditional Digits	status	Subsequent INVITE Note
Call ID	M	Call ID
Additional Digits	M	…
NOTE: The subsequent INVITE contains the Additional digits.		

Table B.9: Mapping of SIP to U_Call Connect

TIPHON message:		Information elements in SIP Message
U_Call Connect	status	200 OK
Call ID	M	Call ID

Table B.10: Mapping of SIP to D_Call Connect

TIPHON message:		Information elements in SIP Message
D_Call Connect	status	200 OK
Call ID	M	Call ID

Table B.11: Mapping of SIP to NW_Call Connect

TIPHON message:		Information elements in SIP Message
NW_Call Connect	status	200 OK
Call ID	M	Call ID

Table B.12: Mapping of SIP to Bearer Request

TIPHON message:					Information elements in SIP Message
Bearer Request				status	SDP in INVITE message
Bearer ID				M	SESSION ID in the 'O' field
Uplink Bearer Descriptor	Service Class			M	NOT SUPPORTED
	Flow Descriptor	Codec Descriptor		M	'FMT list' sub field in 'Media Announcement' 'm' field.
		Delay Budget		M	NOT SUPPORTED
		Frames Per Packet		M	NOT SUPPORTED
		Transport Descriptor	Max Codec Gross Bit Rate	M	??
			Remainder Delay Budget	M	NOT SUPPORTED
			Packet Rate	M	NOT SUPPORTED
			Packet Delay Variation	M	NOT SUPPORTED
			Packet Loss	M	NOT SUPPORTED
			Originator Mpoa	M	CONNECTION DATA
			Destination MpoA	M	Provided in the 200 OK response.

Table B.13: Mapping of SIP to Bearer Confirm

TIPHON message:					Information elements in SIP Message
Bearer Confirm				status	SDP in 200 OK message
Bearer ID				M	SESSION ID in the 'O' field
Uplink Bearer Descriptor	Service Class			M	NOT SUPPORTED
	Flow Descriptor	Codec Descriptor		M	'FMT list' sub field in 'Media Announcement' 'm' field.
		Delay Budget		M	NOT SUPPORTED
		Frames Per Packet		M	NOT SUPPORTED
		Transport Descriptor	Max Codec Gross Bit Rate	M	NOT SUPPORTED
			Remainder Delay Budget	M	NOT SUPPORTED
			Packet Rate	M	NOT SUPPORTED
			Packet Delay Variation	M	NOT SUPPORTED
			Packet Loss	M	NOT SUPPORTED
			Originator Mpoa	M	Provided in the INVITE request.
			Destination MpoA	M	CONNNECTION DATA

Table B.14: Mapping of SIP to Call Control and Registration Meta-Protocol parameters

TIPHON Parameters				SIP parameters
Bearer ID				SDP: Session ID
Bearer Descriptor				
	Service Class (Range)			NOT SUPPORTED
	Flow Descriptor			
		Codec Descriptor		SDP: 'm' (Media Announcement) 'FMT' sub-field.
		Delay Budget		NOT SUPPORTED
		Frames Per Packet		NOT SUPPORTED
		Transport Descriptor		
			Max Codec Gross Bit Rate	NOT SUPPORTED
			Remainder Delay Budget	NOT SUPPORTED
			Packet Rate	NOT SUPPORTED
			Packet Delay Variation	NOT SUPPORTED
			Packet Loss	NOT SUPPORTED
			Originator MpoA	SDP: Connection Data
			Destination MpoA	Provided in 200 OK response
Call ID				Call ID
Calling Party ID				FROM
Calling Party Restriction	Identity Available			Not Supported
	Identity Unavailable			Not Supported
Call Priority (Range)				Priority (Free Text)
called party ID				TO
Client Detach Flag				Implicit in 200 OK
Error Type				4, 5, 6 Classifications
	Source			Source Deduced by Error Type
		Call Control		= same as above
		Bearer Control		= same as above
		Media Control		= same as above
		Transport Control		= same as above
		…		
	Severity			NOT SUPPORTED
		Fatal Error		
		Warning		
		Information		
		…		
	Reason			Following Reasons are Supported
		No Error		
		User ID Unknown		404 NOT FOUND
		User ID Incomplete		484 ADDRESS INCOMPLETE
		Option Not Supported		406 NOT ACCEPTABLE
		QoS not Supported		NOT SUPPORTED
		Priority not Supported		NOT SUPPORTED
		Codec not Supported		NOT SUPPORTED
		Too many parameters		413 Request Entity Too Large
		Missing Parameters		400 Bad Request
		Permission denied		NOT SUPPORTED
		Invalid Ticket		401 UnAuthorized
		Busy		486 Busy Here
		No response		480 Temporarily Unavailable
		User moved		410 Gone
		Service not available		503 Service Unavailable
		Resource not available		NOT SUPPORTED
		QoS not Available		NOT SUPPORTED
		Priority Not available		NOT SUPPORTED
		Codec Not available		NOT SUPPORTED
		…		
Network Data				NOT SUPPORTED
Network Location Data				NOT SUPPORTED
Network Routing Number				'Contact' 3XX response
Operator Selection Indicator				NOT SUPPORTED

TIPHON Parameters			SIP parameters
Party ID			TO, FROM
	E164		Tel URI
		NoA (Range)	NOT SUPPORTED
		Screening Indicator	NOT SUPPORTED
		Digits	Supported
	URL		URL
	Display Name		Display Name in 'FROM"
Registration ID			
	Registrar ID		Request URI
	Registrar Location		SIP/2.0/UDP(/TCP) ; Req URI (Domain Part) ; Port (= 5060)
	Registrant ID		TO
Registration Mode			NOT SUPPORTED
	Initial Registration		
	Refresh Registration		
Registration Removed Flag			Implicit in 200 OK
Report Type			
	Address Complete		183 Session in Progress
	Address Incomplete		484 Address Incomplete
	Call Proceeding		100 Trying
	Call Alerting		180 Ringing
	…		
RpoA			Request URI
Service Application type			NOT SUPPORTED
Service Attach Flag			Implicit in 200 OK
Service Detach Flag			Implicit in 200 OK
Service Offer Ticket (Type)			NOT SUPPORTED
	Registrant ID		
	Registrar ID		
	Service Credentials		
		Service App ID	
		SpoA	
		Start Time	
		Stop Time	
		Crypto Digest	
	Crypto Digest		
Service Request Ticket (See Ticket Type)			NOT SUPPORTED
Service Reject Reason Type			Supported
	Service Application ID Type		NOT SUPPORTED
	Reject Reason (See Error Type)		Supported (see Error Type)
SpoA			Request URI
Ticket/Token Type (see Service offer ticket Type)			

Annex C (informative): Services Supported by SIP in TIPHON Release 3

Service Supported by SIP in Release 3 (based on the capabilities supported in this profile).

Table C.1: Services Supported by SIP in TIPHON Release 3

Service	Status	Comments
Simple Call Setup without ICF	Supported	
Simple Call Setup with ICF	Supported	
Support for Intra Domain QoS	Not Supported	
Support for CLIP/CLIR	Not Supported	
Billing		
Legal Intercept	Partially Supported	Intercept Media path setup via ICF
SCN Interworking	Partially Supported	
VoIP interconnect -supporting NAT - Supporting QoS	Partially Supported Supported Not Supported	
Roaming	Supported	
Number Portability	Partially Supported	QoR, ACQ Supported
Priority Calls	Partially Supported	Need clarification on Authorization
Emergency Calls	Supported	
Carrier Selection	Partially Supported	Supported by the use of 'prefix' (service code). No Service indicator in SIP

Annex D (normative): Minimum set of SIP Messages and Parameters required in TIPHON R3

Table D.1 shows the minimum set of messages (Request/Response) for TIPHON release 3.

Table D.1: SIP messages required in TIPHON Release 3

Methods	ACK
	Provisional ACK (PRACK)
	BYE
	CANCEL
	INVITE
	OPTIONS
	REGISTER
Responses	100 Trying
	180 Ringing
	183 Session Progress
	200 OK
	300 Multiple Choice
	301 Moved Permanently
	302 Moved Temporarily
	400 Bad Request
	401 UnAuthorized
	404 Not Found
	406 Not Acceptable
	410 Gone
	480 Temporarily Not Available
	484 Address Incomplete
	503 Service Unavailable
	603 Decline

Table D.2: SIP headers required in TIPHON Release 3

SIP header	SIP status
Accept	M
Accept Encoding	M
Accept Language	M
Call ID	M
Call Seq	M
CONTACT	M
CONTENT TYPE	M
CONTENT LENGTH	M
EXPIRES	O
FROM	M
MAX FORWARDS	O
PROXY AUTHORIZATION	O
PROXY AUTHENTICATE	M
PRIORITY	O
RECORD Route	O
REQUIRE	O
SUPPORTED (option tag: 100rel)	O
TO	M
VIA	M
WWW-Authenticate	M

Annex E (informative): Capabilities missing from SIP and SDP

The following is the list of enhancements required in SIP to support the TIPHON architecture as defined in [1].

Table E.1: Capabilities missing from SIP

TIPHON capabilities missing in SIP		Comments
Allowed Services (audio, video, data, other)		
Caller location		
Calling number presentation	Identity Available	
	Identity Unavailable	
Error Reason	Codec Not Available	
	Codec Not Supported	
	No Error	
	Option Not Supported	
	Priority Not Supported	
	QoS Not Supported	
	QoS Not Available	
	Resources Not Available	
	Priority Not Available	
Nature of Address		
Number of digits required (numbering plan)		
Network Data		
Network Location Data		
Presentation number presentation and restriction		
Requested services		
Registration Mode		
Screening Indicator		
Sending complete indication		
Service offer Ticket		
Service Application ID		
Service Application Type		
Service details		
Severity Level of Error		
Supplementary services details		

Table E.2: Capabilities missing from SDP

Capabilities missing from SDP	Comments
Delay Budget	
Frames per packet	
Maximum Codec Gross Bit Rate	
Packet Delay Variation	
Packet Rate	
Packet Loss	
Remainder Delay Budget	
Service Class	

Annex F (informative): SIP flows for scenarios 0 to 3

F.1 Scenario 0

The TIPHON scenario 0 describes communications between two IP terminals, in this case, two SIP terminals/clients. The Two SIP terminals/clients could either be located in one domain, or in two different domains.

Calling party	Originating Network	Intermediate Network	Terminating Network	Called party

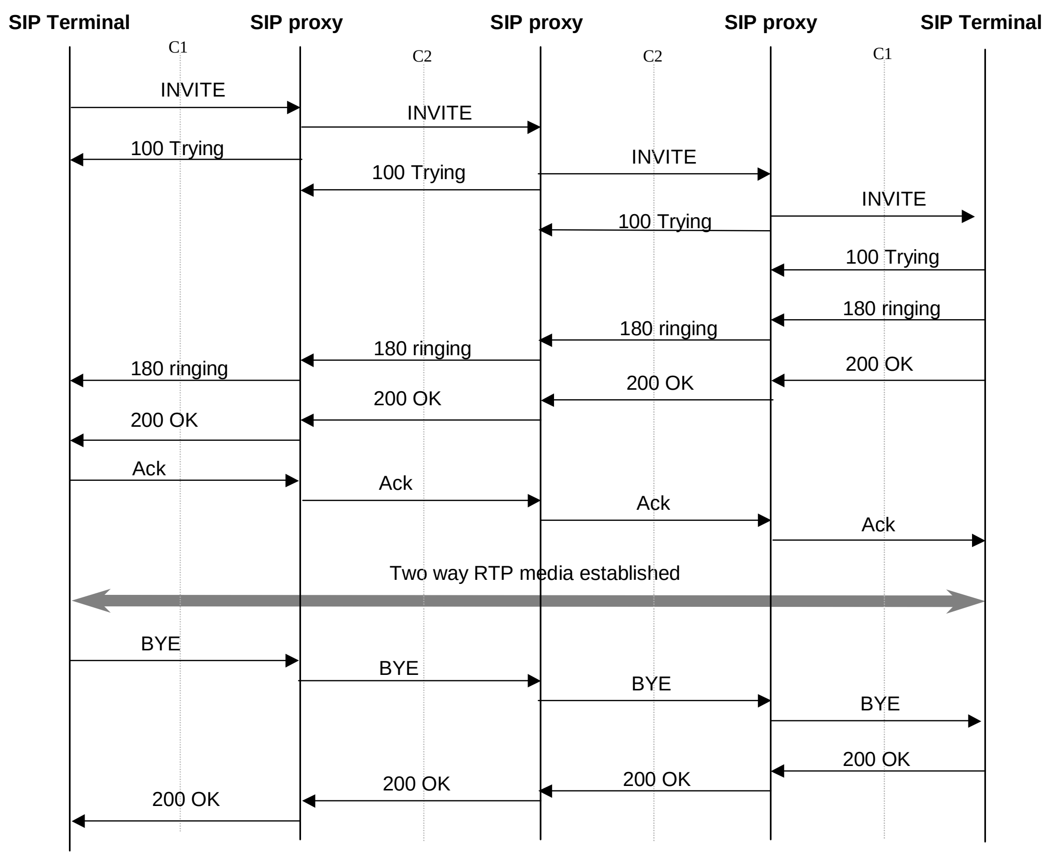
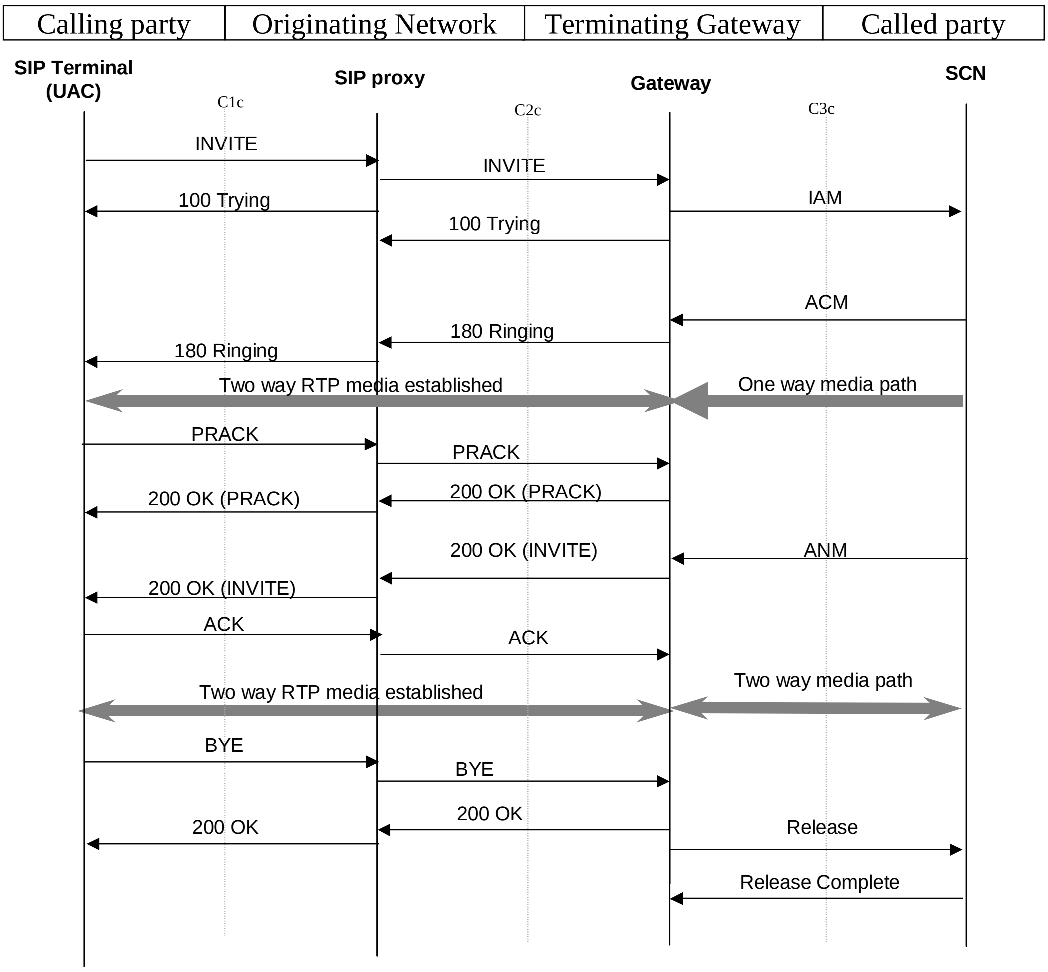


Figure F.1: SIP flow for scenario 0

F.2 Scenario 1

In this scenario, calls originate from the SIP terminal and terminate on the SCN. A Gateway Functional Grouping is required to provide the interworking between the SCN and the IP Networks.

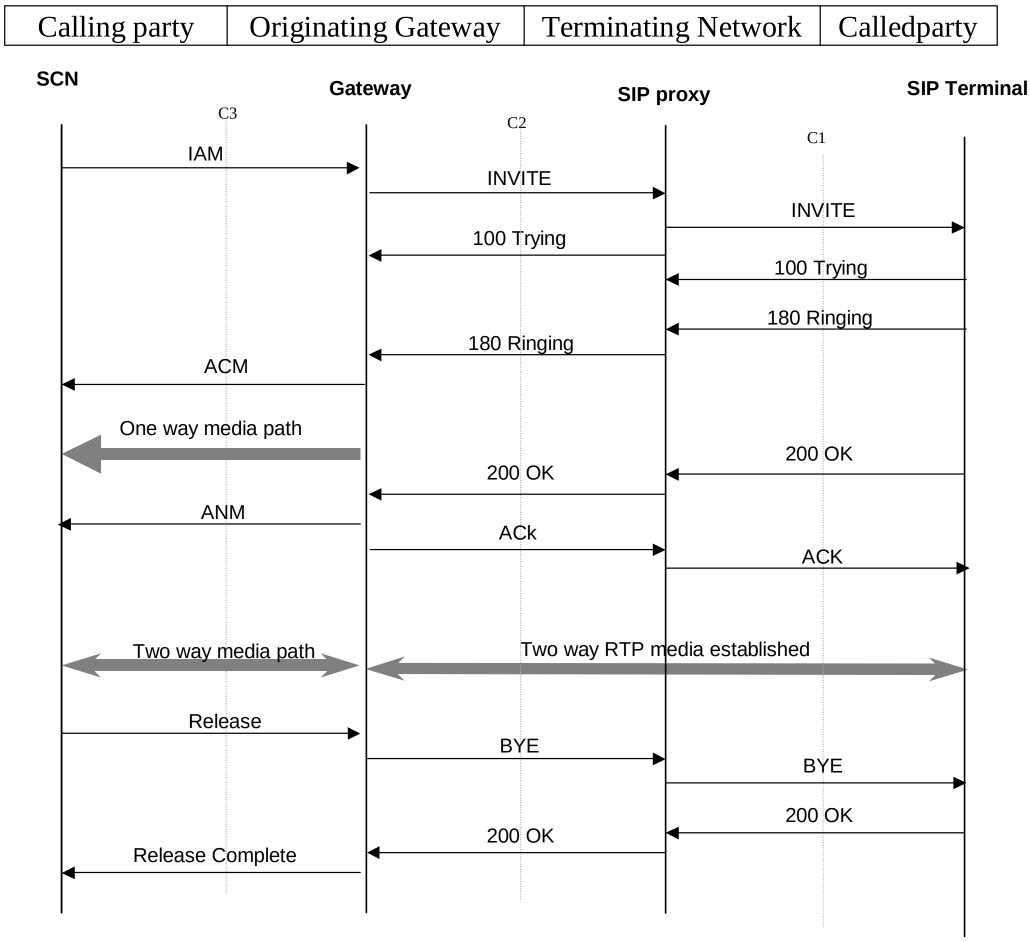


NOTE: The 180 Ringing includes the SDP answer, which means that the media can be trough-connected prior to the answer.

Figure F.2: SIP flow for scenario 1

F.3 Scenario 2

The Calls originate from a SCN and terminate in an IP Network. A Gateway Functional Grouping is required to provide the interworking between the SCN and IP networks.

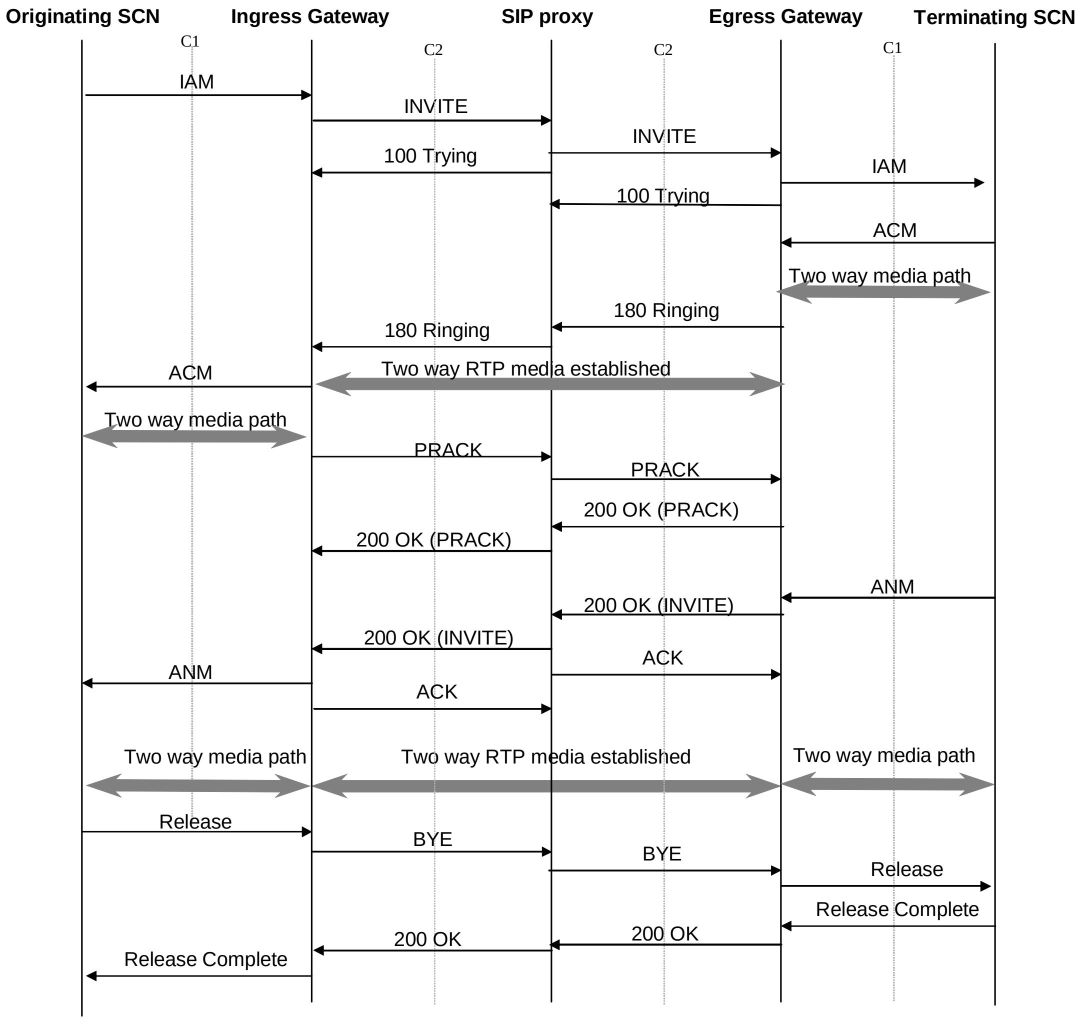


NOTE: The gateway applies the ringing tone towards the calling user in the SCN.

Figure F.3: SIP flow for scenario 2

F.4 scenario 3

The calls originate from a SCN and terminate in a SCN, with the intermediate network being an IP based network.



NOTE: The `'180 Ringing'` includes the SDP answer, which means that the media can be trough-connected in both directions prior to the answer.

Figure F.4: SIP flow for scenario 3

Annex G (informative): Bibliography

ETSI TS 102 027-2: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Technology Compliance Specification; Draft IETF SIP RFC2543bis-04; Part 2: Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT) proforma specification".

ETSI TS 101 329-2: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; End-to-end Quality of Service in TIPHON systems; Part 2: Definition of speech Quality of Service (QoS) classes".

List of figures

List of tables

History

Document history		
V1.1.1	September 2002	Publication