FFT Doc 11.001 v1.1 (June 2012)

French Federation of Telecommunications
Standards Committee
IP Interconnection Working Group
Architecture Sub-group

IP interconnection

Interface specification based on SIP-I

French Federation of Telecoms

Internet

http://www.fftelecom.org

Table of Contents

1. Context

1.1 Purpose

The purpose of this document is to define the SIP-I/SDP interconnection interface for the interconnection between two French Operators for basic telephony services with deterministic charging or non-deterministic charging.

This document supports the following basic call capabilities:
- Calls addressing E.164 numbers
- Calls addressing national short codes (French specific non E.164 numbers),
- 3.1 kHz audio services (i.e. narrow-band voice, analog fax and modem data),
- Wideband voice (7 kHz) based on G.722, or WB_AMR codec
- 64 kbit/s unrestricted digital information services,
- en bloc address signalling,
- early in-band information (early media),
- in-band transport of DTMF tones and information (telephone event).

and the following supplementary services (see [SPIROU] for the complete list of services):
- Calling Line Identification Presentation (CLIP),
- Calling Line Identification Restriction (CLIR),
- Call Forwarding,
- Call Hold,
- Call Waiting,
- User to user information,
- Terminal portability,
- etc…

1.2 Standards

As a rule, the interconnection between two mobile networks using SIP-I shall comply with [3GPP TS.29.231] with the clarifications and exceptions detailed in the present specification.

The interconnection between two fixed networks using SIP-I shall comply with [ITU-T Q.1912.5] Profile C with the clarifications and exceptions detailed in the present specification.

Note: the present document applies to all types of SIP-I interconnection.

This document also describes some optional features of interest to this specification. Other optional features are considered out of the scope of this document but may be considered on a bilateral basis.

2. References

Some of the references listed below are mandatory and others are optional as described within the core of the document.

[RFC2046]	IETF RFC 2046 “Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types”
[RFC2976]	IETF RFC 2976 "The SIP INFO Method"
[RFC3204]	IETF RFC 3204 “MIME media types for ISUP and QSIG Objects”
[RFC3261]	IETF RFC 3261 "Session Initiation Protocol (SIP)"
[RFC3262]	IETF RFC 3262 "Reliability of Provisional Responses in the Session Initiation Protocol (SIP)"
[RFC3264]	IETF RFC 3264 "An Offer/Answer Model with the Session Description Protocol (SDP)"
[RFC3311]	IETF RFC 3311 "The Session Initiation Protocol (SIP) UPDATE method"
[RFC3312]	IETF RFC 3312 "Integration of Resource Management and Session Initiation Protocol (SIP)"
[RFC3323]	IETF RFC 3323 "A Privacy Mechanism for the Session Initiation Protocol (SIP)"
[RFC3325]	IETF RFC 3325 "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".
[RFC3326]	IETF RFC 3326 "The Reason Header Field for the Session Initiation Protocol (SIP)"
[RFC3407]	IETF RFC 3407 "Session Description Protocol (SDP) Simple Capability Declaration"
[RFC3556]	IETF RFC 3556 “Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth”
[RFC3966]	IETF RFC 3966 "The tel URI for Telephone Numbers"
[RFC4028]	IETF RFC 4028 "Session Timers in the Session Initiation Protocol (SIP)"
[RFC4040]	IETF RFC 4040 “RTP Payload Format for a 64 kbit/s Transparent Call”
[RFC4566]	IETF RFC 4566 "Session Description Protocol (SDP)"
[RFC4733]	IETF RFC 4733 "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals"
[TS 24.528]	3GPP Technical Specification 24.528 "TISPAN, Common basic communication procedures; Protocol specification"
[TS 29.231]	3GPP Technical Specification 29.231 “Application of SIP-I Protocols to Circuit Switched (CS) core network architecture; Stage 3”
[Q.1912.5]	ITU-T Recommendation Q.1912.5 “Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part”
[G.711]	ITU-T Recommendation " Pulse code modulation (PCM) of voice frequencies"
[G.729]	ITU-T Recommendation "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)"
[G.729 Annex A]	ITU-T Recommendation Annex A "Reduced complexity 8 kbit/s CS-ACELP speech codec"
[TS 26.071]	3GPP Technical Specification 26.071 “Mandatory speech CODEC speech processing functions; AMR speech Codec; General description”
[TS 26.171]	3GPP Technical Specification 26.171 “Speech codec speech processing functions; Adaptive Multi-Rate - Wideband (AMR-WB) speech codec; General description”
[G.722]	ITU-T Recommendation G.722 “7 kHz audio-coding within 64 kbit/s”
[SPIROU]	http://www.arcep.fr/fileadmin/reprise/dossiers/spectech/spirouen.zip

3. Glossary

CLIP	Calling Line Identity Presentation
CLIR	Calling Line Identity Restriction
DTMF	Dual-Tone Multi-Frequency
ISUP	ISDN User Part
MIME	Multipurpose Internet Mail Extensions
NNI	Network To Network Interface
SIP	Session Initiation Protocol
SIP-I	SIP with encapsulated ISUP
SDP	Session Description Protocol
SPIROU	Signalisation Pour l’Interconnexion des Réseaux Ouverts
SCTP	Stream Control Transport Protocol
TCP	Transport Control Protocol
UDP	User Datagram Protocol
URI	Uniform Resource Identifier

4. SIP signalling messages

The SIP messages and headers specified in this section must be encoded, filled and handled as specified in the referenced standard in which they are defined.

Request-URI in all SIP requests must be coded and filled according to [RFC3261] and as stated in section 9 for the initial INVITE message.

4.1 Definitions

"Reception" and "Transmission" directions refer to the direction of the messages.

In reception direction, "Supported" means that the header can be present in the message and if received, it must be handled according to the standard. "Mandatory" means that the recipient expects the header to be present. “Not applicable” means that the reception of the header can not occur according to the current specification. By symmetry “Not applicable” is relative only to headers with the status “not sent” in emission.

In transmission direction, "May be sent" means that the header can be present or omitted depending on the transaction or the call context. "Mandatory" means that the header is always present. "Not sent" means that the header shall not be sent.

4.2 Transport protocol

UDP is supported and required for carrying SIP messages.

> *Note: According to IETF [RFC3261], TCP must be supported. This requirement arises out of the need to handle large messages.*

In addition to the transport modes mandated by [RFC3261], the “UDP only” mode with IP fragmentation shall be supported.

SCTP transport may be used for carrying SIP messages.

4.3 SIP methods and headers

4.3.1 SIP methods

Table 1 contains the SIP methods required to support the capabilities and services identified in section 1.1.

Mandatory methods
INVITE
RE-INVITE
INFO
ACK
BYE
CANCEL
OPTIONS (NOTE)

Table 1: Mandatory SIP methods

NOTE – It is mandatory to support OPTIONS in the reception direction only.

Support for methods not listed in Table 1 is optional, as the Update method which may be used if the optional keep-alive mechanism for active SIP sessions as defined in the [RFC4028] is used on bilateral agreement (see §17.1).

4.3.2 Header fields for ISUP MIME bodies

For the purpose of this specification the Content-Type header field associated with the ISUP MIME body shall be supplied as follows:

Content-Type: application/ISUP; version= spirou;

The Content-Disposition header field associated with the ISUP MIME body shall be set as follows:

Content-Disposition: signal; handling = required.

4.3.3 ISUP SPIROU message encapsulation status

This table describes the encapsulation status for all ISUP SPIROU messages. It complies with Q.1912.5 and extends Q.1912.5 with SPIROU specific messages (ITX and TXA).

SPIROU ISUP message	Encapsulation status
Initial Address Message	Encapsulated according to Q.1912.5 § 5.4.1.3
Subsequent Address Message	Encapsulated according to Q.1912.5 § 5.4.1.3
Connect	Encapsulated according to Q.1912.5 § 5.4.1.3
Answer	Encapsulated according to Q.1912.5 § 5.4.1.3
Address complete	Encapsulated according to Q.1912.5 § 5.4.1.3
Call Progress	Encapsulated according to Q.1912.5 § 5.4.1.3 or §5.4.3.2
Release	Encapsulated according to Q.1912.5 § 5.4.1.3
Reset Circuit	Not encapsulated (Q.1912.5 §5.4.3.1)

Confusion	May be encapsulated according to Q.1912.5 §5.4.3.2
Suspend	Encapsulated according to Q.1912.5 §5.4.3.2
Resume	Encapsulated according to Q.1912.5 §5.4.3.2
Blocking	Not encapsulated (Q.1912.5 §5.4.3.1)
Blocking Acknowledgement	Not encapsulated (Q.1912.5 §5.4.3.1)
Continuity Check Request	Not encapsulated (Q.1912.5 §5.4.3.1)
Continuity	Not encapsulated (Q.1912.5 §5.4.3.1)
Unblocking	Not encapsulated (Q.1912.5 §5.4.3.1)
Unblocking Acknowledgement	Not encapsulated (Q.1912.5 §5.4.3.1)
Facility	Encapsulated according to Q.1912.5 §5.4.3.2
Segmentation	Not encapsulated (Q.1912.5 §5.4.3.3)
Loop Prevention	Encapsulated according to Q.1912.5 §5.4.3.2. (NOTE)
Release Complete	Encapsulated according to Q.1912.5 §5.4.3.4
ITX	Encapsulated according to Q.1912.5 §5.4.3.2
TXA	Encapsulated according to Q.1912.5 §5.4.3.2

Table 2: ISUP message encapsulation status

NOTE - A bilateral agreement is a prerequisite for the support of the Loop Prevention SPIROU message.

4.3.4 Network behaviour in reception

*4.3.4.1 **Method inspection***

If a SIP method received is recognized but not supported, it shall be rejected as defined in [RFC3261] by a 405 "Method not allowed" response.

If a SIP method received is not recognized (i.e. not implemented), it shall be rejected as defined in [RFC3261] by a 501 "Not Implemented" response.

*4.3.4.2 **Status code inspection***

If a non-supported error response is received in a SIP message then the relative call or transaction fails. The list of the supported responses with their detailed handling and of the Not applicable responses is given in section 4.3.6.3, Table 3.
If a non-recognized final response, i.e. not referenced in the section 4.3.6.3 Table 3, is received in a SIP message then it shall be treated as being equivalent to the x00 response code of that class.
If a non-recognized provisional response different than 100 final response, i.e. not referenced in the section 4.3.6.3 Table 3, is received in a SIP message then it shall be treated as being equivalent to a 183 (Session Progress).

*4.3.4.3 **Header inspection in requests***

If a non-supported SIP header or parameter is received in a SIP request, it shall be ignored unless its corresponding option tag is present in the Require header. The headers or parameters that are not

mentioned in the tables from section 4.3.6 to section 4.3.11 are considered as Not applicable headers or parameters.
If a mandatory header is absent or malformed in the request, the request shall be rejected as defined in [RFC3261].

4.3.4.4 <u>Header inspection in responses</u>

If a non-supported SIP header or parameter is received in a SIP response, it shall be ignored. The headers or parameters that are not present in the tables from section 4.3.6 to section 2 are considered as non-supported headers or parameters.

If a header necessary for processing the response is absent or malformed in a provisional response, the response shall be discarded.

If a header necessary for processing the response is absent or malformed in a final response except a 2XX response, the response shall be treated as the 500 "Server Internal Failure" response.

If a header necessary for processing the response is absent or malformed in a final 2XX response to an INVITE request, the response shall be acknowledged by sending an ACK and then the dialog shall be terminated.

NOTE – The behaviour in case of receipt of “Not applicable” SIP signalling element is not defined in this specification since this is relative to a context out of the scope of the current document.

4.3.5 Network behaviour in emission

By default only the SIP signalling element (methods, headers, header parameters, response status codes, option tags, …) defined and authorized (mandatory or optional) as described within the current specification can be sent.
Nevertheless according to bilateral agreements, SIP signalling elements not defined or not authorized in the current specification can be exchanged over the interconnection interface.

4.3.6 Initial INVITE method

The initial INVITE request is mandatory as defined in [RFC3261].

4.3.6.1 <u>SIP request handling</u>

The handling of this request is compliant with [RFC3261].

4.3.6.2 <u>Supported headers in the request</u>

Table 3 gives the header status in the initial INVITE for both reception and transmission directions.

Header name	Reference	Reception	Transmission
Accept	[RFC3261]	Supported	May be sent
Allow	[RFC3261]	Supported	May be sent
Call-ID	[RFC3261]	Mandatory	Mandatory
Contact	[RFC3261]	Mandatory	Mandatory
Content-Disposition	[RFC3204]	Mandatory	Mandatory
Content-Length	[RFC3261]	Supported	May be sent
Content-Type	[RFC3261]	Mandatory	Mandatory
CSeq	[RFC3261]	Mandatory	Mandatory
From	[RFC3261]	Mandatory	Mandatory
Max-Forwards	[RFC3261]	Mandatory	Mandatory
MIME-Version	[RFC3261]	Supported	May be sent
Min-SE	[RFC4028]	Supported	May be sent
Record-Route	[RFC3261]	Not applicable	Not sent
Route	[RFC3261]	Supported	May be sent
Session-Expires	[RFC4028]	Supported	May be sent
Supported	[RFC3261]	Supported	May be sent
Require	[RFC3261]	Not applicable	Not sent
To	[RFC3261]	Mandatory	Mandatory

Via	[RFC3261]	Mandatory	Mandatory
Privacy	[RFC3323]	Supported and ignored. See section 16.1.	May be sent. See section 16.1.
P-Asserted-Identity	[RFC3325]	Supported and ignored. See section 16.1.	May be sent. See section 16.1.

Table 3: Supported SIP headers in the initial INVITE request

4.3.6.3 <u>SIP response handling</u>

SIP responses are handled according to [RFC3261] with the clarifications given in the table below. If a non-supported error response is received, then the relative call or transaction fails.

SIP response		Reception	Transmission
1xx	100 Trying	Supported	May be sent
	180 Ringing	Supported	Sent when the called user is notified for the incoming call.
	181 Call is being forwarded	Not applicable	Not sent
	182 Queued	Not applicable	Not sent
	183 Session Progress	Supported	May be sent
2xx	200 OK	Supported	Sent when the call is answered.
3xx		Not applicable	Not sent
4xx	400 Bad Request	Supported. The related call or transaction fails.	May be sent
	401 Unauthorized	Not applicable	Not sent
	402 Payment Required	Not applicable.	Not sent
	403 Forbidden	Supported. The related call or transaction fails.	May be sent
	404 Not Found	Supported. The related call or transaction fails.	May be sent
	405 Method Not Allowed	Supported	May be sent
	406 Not Acceptable	Supported. The related call or transaction fails.	May be sent
	407 Proxy Authentication Required	Not applicable	Not sent
	408 Request Timeout	Supported	May be sent
	410 Gone	Supported. The related call or transaction fails.	May be sent
	413 Request Entity Too Large	Supported The related call or transaction fails. The request is not retried.	May be sent
	414 Request-URI Too Long	Supported. The related call or transaction fails.	May be sent
	415 Unsupported Media Type	Supported. The related call or transaction fails. The request is not retried.	May be sent
	416 Unsupported URI Scheme	Supported. The related call or transaction fails. The request is not retried.	May be sent
	420 Bad Extension	Supported. The related call or transaction fails. The request is not retried.	May be sent
	421 Extension Required	Not applicable	Not sent
	422	Supported	May be sent

SIP response		Reception	Transmission
	Session Interval Too Small		
	423 Interval Too Brief	Not applicable.	Not sent
	480 Temporarily Unavailable	Supported. The related call or transaction fails.	May be sent
	481 Call/Transaction Does Not Exist	Supported. The related call or transaction fails.	May be sent
	482 Loop Detected	Supported. The related call or transaction fails.	May be sent
	483 Too Many Hops	Supported. The related call or transaction fails.	May be sent
	484 Address Incomplete	Supported. The related call or transaction fails.	May be sent
	485 Ambiguous	Not applicable	Not sent
	486 Busy here	Supported. The related call or transaction fails.	May be sent
	487 Request Terminated	Supported. The related call or transaction fails.	May be sent
	488 Not acceptable here	Supported. The related call or transaction fails.	Sent if the received request contains an SDP offer proposing non supported media format or IP version.
	491 Request Pending	Supported. For re-INVITE request, the behaviour recommended in [RFC3261]/14.1 on reception of this response is supported.	May be sent. For re-INVITE request, the behaviour recommended in [RFC3261]/14.1 on reception of this response is supported.
	493 Undecipherable	Supported. The related call or transaction fails	May be sent
5xx		Supported. The related call or transaction fails.	May be sent*
6xx	600 Busy Everywhere	Supported. The related call or transaction fails.	May be sent
	603 Decline	Supported. The related call or transaction fails.	May be sent
	604 Does Not Exist Anywhere	Supported. The related call or transaction fails.	May be sent
	606 Not Acceptable	Supported. The related call or transaction fails.	May be sent

Table 4: Handling of SIP responses

*: if the maximum number of simultaneous sessions is exceeded, a 503 response shall be sent with the reason phrase "Exceeded outbound of the service agreement".

4.3.6.4 Supported headers in the responses

Table 5 gives the header status in the SIP responses to the initial INVITE request for both reception and transmission directions.

Header name	Reference	Response code	Reception	Transmission
Accept	[RFC3261]	18X /200	Supported	May be sent
Accept	[RFC3261]	415	Mandatory	Mandatory
Allow	[RFC3261]	405	Mandatory	Mandatory
Allow	[RFC3261]	All codes	Supported	May be sent
Call-ID	[RFC3261]	All codes	Mandatory	Mandatory
Contact	[RFC3261]	1xx (other than 100)	Supported	May be sent

Header name	Reference	Response code	Reception	Transmission
Contact	[RFC3261]	200	Mandatory	Mandatory
Content-Disposition	[RFC3204]	All codes	Mandatory if an ISUP body is present	Mandatory if an ISUP body is present
Content-Length	[RFC3261]	All codes	Supported	May be sent
Content-Type	[RFC3261]	All codes	Mandatory if the body is not empty.	Mandatory if the body is not empty.
CSeq	[RFC3261]	All codes	Mandatory	Mandatory
From	[RFC3261]	All codes	Mandatory	Mandatory
Min-SE	[RFC4028]	422	Supported	May be sent
Reason	[FRC3326]	All codes	Supported	May be sent
Record-Route	[RFC3261]	18x 2xx	Not applicable	Not sent
Require	[RFC3261]	18x	Not applicable	Not sent
Require	[RFC3261]	200	Supported	May be sent
Session-Expires	[RFC4028]	200	Supported	May be sent
Supported	[RFC3261]	200	Supported	May be sent
To	[RFC3261]	All codes	Mandatory	Mandatory
Unsupported	[RFC3261]	420	Mandatory	Mandatory
Via	[RFC3261]	All codes	Mandatory	Mandatory

Table 5: Supported SIP headers in the responses to the initial INVITE request

4.3.7 Re-INVITE method

The re-INVITE request shall be supported as defined in [RFC3261].

4.3.7.1 __SIP request handling__

The handling of this request shall be compliant with [RFC3261].

4.3.7.2 __Supported headers in the request__

Table 6 gives the header status in the re-INVITE request for both reception and transmission directions.

Header name	Reference	Reception	Transmission
Accept	[RFC3261]	Supported	May be sent
Allow	[RFC3261]	Supported	May be sent
Call-ID	[RFC3261]	Mandatory	Mandatory
Contact	[RFC3261]	Mandatory	Mandatory
Content-Disposition	[RFC3204]	Mandatory if an ISUP body is present	Mandatory if an ISUP body is present
Content-Length	[RFC3261]	Supported	May be sent
Content-Type	[RFC3261]	Mandatory if the body is not empty	Mandatory if the body is not empty
CSeq	[RFC3261]	Mandatory	Mandatory
From	[RFC3261]	Mandatory	Mandatory
Max-Forwards	[RFC3261]	Mandatory	Mandatory
MIME-Version	[RFC3261]	Supported	May be sent
Min-SE	[RFC4028]	Supported	May be sent
Route	[RFC3261]	Supported	May be sent
Session-Expires	[RFC4028]	Supported	May be sent
Supported	[RFC3261]	Supported	May be sent
Require	[RFC3261]	Not applicable	Not sent
To	[RFC3261]	Mandatory	Mandatory

Via	[RFC3261]	Mandatory	Mandatory

Table 6: Supported SIP headers in the re-INVITE request

4.3.7.3 SIP response handling

The handling of the responses shall be compliant with [RFC3261].

1xx responses different from 100 are not expected for the re-INVITE request.

4.3.7.4 Supported headers in the responses

Table 7 gives the header status in the SIP responses to the re-INVITE request for both reception and transmission directions.

Header name	Reference	Response code	Reception	Transmission
Accept	[RFC3261]	200	Supported	May be sent
Accept	[RFC3261]	18X	Supported	May be sent
Accept	[RFC3261]	415	Supported	May be sent
Allow	[RFC3261]	405	Mandatory	Mandatory
Allow	[RFC3261]	All codes	Supported	May be sent
Call-ID	[RFC3261]	All codes	Mandatory	Mandatory
Contact	[RFC3261]	1xx	Supported.	May be sent
Contact	[RFC3261]	200	Supported	May be sent
Content-Disposition	[RFC3204]	All codes	Mandatory if an ISUP body is present.	Mandatory if an ISUP body is present.
Content-Length	[RFC3261]	All codes	Supported	May be sent
Content-Type	[RFC3261]	200	Mandatory if the body is not empty.	Mandatory if the body is not empty.
CSeq	[RFC3261]	All codes	Mandatory	Mandatory
From	[RFC3261]	All codes	Mandatory	Mandatory
Require	[RFC3261]	18x	Supported	May be sent
Min-SE	[RFC4028]	422	Supported	May be sent
Require	[RFC3261]	200	Supported	May be sent
Session-Expires	[RFC4028]	200	Supported	May be sent
Supported	[RFC3261]	200	Supported	May be sent
To	[RFC3261]	All codes	Mandatory	Mandatory
Unsupported	[RFC3261]	420	Mandatory	Mandatory
Via	[RFC3261]	All codes	Mandatory	Mandatory

Table 7: Supported SIP headers in the responses to the re-INVITE request

4.3.8 CANCEL method

The CANCEL request shall be supported as defined in [RFC3261].

4.3.8.1 SIP request handling

The handling of this request shall be compliant with [RFC3261].

4.3.8.2 Supported headers in the request

Table 8 gives the header status in the SIP CANCEL request for both reception and transmission directions.

Header name	Reference	Reception	Transmission
Call-ID	[RFC3261]	Mandatory	Mandatory
Content-length	[RFC3261]	Supported	May be sent
CSeq	[RFC3261]	Mandatory	Mandatory
From	[RFC3261]	Mandatory	Mandatory
Max-Forwards	[RFC3261]	Mandatory	Mandatory
Reason	[RFC3326]	Supported	May be sent

Header name	Reference	Reception	Transmission
Route	[RFC3261]	Supported	May be sent
To	[RFC3261]	Mandatory	Mandatory
Via	[RFC3261]	Mandatory	Mandatory

Table 8: Supported SIP headers in the CANCEL request

Both SIP status codes and ITU-T Q.850 cause values in decimal representation are supported in the Reason header, according to [RFC3326].

4.3.8.3 <u>SIP response handling</u>

The handling of the responses shall be compliant with [RFC3261].

4.3.8.4 <u>Supported headers in the responses</u>

Table 9 gives the header status in the responses to the CANCEL request for both reception and transmission directions.

Header name	Reference	Response code	Reception	Transmission
Call-ID	[RFC3261]	All codes	Mandatory	Mandatory
Content-Length	[RFC3261]	All codes	Supported	May be sent
CSeq	[RFC3261]	All codes	Mandatory	Mandatory
From	[RFC3261]	All codes	Mandatory	Mandatory
To	[RFC3261]	All codes	Mandatory	Mandatory
Via	[RFC3261]	All codes	Mandatory	Mandatory

Table 9: Supported SIP headers in the SIP responses to the CANCEL request

4.3.9 ACK method

The ACK request shall be supported as specified in [RFC3261].

4.3.9.1 <u>SIP request handling</u>

The handling of this request shall be compliant with [RFC3261].

4.3.9.2 <u>Supported headers in the request</u>

Table 10 gives the header status in the ACK request for both reception and transmission directions.

Header name	Reference	Reception	Transmission
Call-ID	[RFC3261]	Mandatory	Mandatory
Contact	[RFC3261]	Supported	May be sent
Content-length	[RFC3261]	Supported	May be sent
Content-type	[RFC3261]	Mandatory if the body is not empty	Mandatory if the body is not empty
CSeq	[RFC3261]	Mandatory	Mandatory
From	[RFC3261]	Mandatory	Mandatory
Max-Forwards	[RFC3261]	Mandatory	Mandatory
MIME-Version	[RFC3261]	Supported	May be sent
Route	[RFC3261]	Supported	May be sent
To	[RFC3261]	Mandatory	Mandatory
Via	[RFC3261]	Mandatory	Mandatory

Table 10: Supported SIP headers in the ACK request

4.3.10 BYE method

The BYE request shall be supported as specified in [RFC3261].

4.3.10.1 <u>SIP request handling</u>

The handling of this request shall be compliant with [RFC3261].

4.3.10.2 <u>Supported headers in the request</u>

Table 11 gives the header status in the BYE request for both reception and transmission directions.

Header name	Reference	Reception	Transmission
Accept	[RFC3261]	Supported	May be sent
Allow	[RFC3261]	Supported	May be sent
Call-ID	[RFC3261]	Mandatory	Mandatory
Content-length	[RFC3261]	Supported	May be sent
Content-type	[RFC3261]	Mandatory if the body is not empty	Mandatory if the body is not empty
Content-Disposition	[RFC3204]	Mandatory if an ISUP body is present	Mandatory if an ISUP body is present
CSeq	[RFC3261]	Mandatory	Mandatory
From	[RFC3261]	Mandatory	Mandatory
Max-Forwards	[RFC3261]	Mandatory	Mandatory
MIME-Version	[RFC3261]	Supported	May be sent
P-Asserted-Identity	[RFC3261]	Supported and ignored. See section 16.1.	May be sent. See section 16.1.
Reason	[RFC3326]	Supported	May be sent
Route	[RFC3261]	Supported	May be sent
To	[RFC3261]	Mandatory	Mandatory
Via	[RFC3261]	Mandatory	Mandatory

Table 11: Supported SIP headers in the BYE request

Both SIP status codes and ITU-T Q.850 cause values in decimal representation shall be supported in the reason header, according to [RFC3326].

4.3.10.3 SIP response handling

The handling of the responses shall be compliant with [RFC3261].

4.3.10.4 Supported headers in the responses

Table 12 gives the header status in the SIP responses to the BYE request for both reception and transmission directions.

Header name	Reference	Response code	Reception	Transmission
Accept	[RFC3261]	415	Mandatory	Mandatory
Allow	[RFC3261]	All codes	Supported	May be sent
Call-ID	[RFC3261]	All codes	Mandatory	Mandatory
Content-Disposition	[RFC3204]	200	Mandatory if an ISUP body is present	Mandatory if an ISUP body is present
Content-Length	[RFC3261]	All codes	Supported	May be sent
Content-Type	[RFC3261]	All codes	Supported	May be sent
Cseq	[RFC3261]	All codes	Mandatory	Mandatory
From	[RFC3261]	All codes	Mandatory	Mandatory
MIME-Version	[RFC3261]	All codes	Supported	May be sent
To	[RFC3261]	All codes	Mandatory	Mandatory
Via	[RFC3261]	All codes	Mandatory	Mandatory

Table 12: Supported SIP headers in the responses to the BYE request

4.3.11 OPTIONS method

The OPTIONS method shall be supported as specified in [RFC3261].

4.3.11.1 SIP request handling

The handling of this request shall be compliant with [RFC3261].

4.3.11.2 Supported headers in the request

Table 13 gives the header status in the OPTIONS request for both reception and transmission directions.

Header name	Reference	Reception	Transmission
Accept	[RFC3261]	Supported	May be sent

Header name	Reference	Reception	Transmission
Allow	[RFC3261]	Supported	May be sent
Call-ID	[RFC3261]	Mandatory	Mandatory
Content-length	[RFC3261]	Supported	May be sent
Content-Type	[RFC3261]	Supported	May be sent
CSeq	[RFC3261]	Mandatory	Mandatory
From	[RFC3261]	Mandatory	Mandatory
Max-Forwards	[RFC3261]	Mandatory	Mandatory
MIME-Version	[RFC3261]	Supported	May be sent
P-Asserted-Identity	[RFC3325]	Supported and ignored. See section 16.1.	May be sent. See section 16.1.
To	[RFC3261]	Mandatory	Mandatory
Via	[RFC3261]	Mandatory	Mandatory

Table 13: Supported SIP headers in the OPTIONS request

4.3.11.3 <u>SIP response handling</u>

The handling of the responses shall be compliant with [RFC3261].

4.3.11.4 <u>Supported headers in the responses</u>

Table 14 gives the header status in the SIP responses to the OPTIONS request for both reception and transmission directions.

Header name	Reference	Response code	Reception	Transmission
Accept	[RFC3261]	200	Supported	May be sent
Allow	[RFC3261]	All codes	Supported	May be sent
Call-ID	[RFC3261]	All codes	Mandatory	Mandatory
Content-length	[RFC3261]	All codes	Supported	May be sent
Content-Type	[RFC3261]	All codes	Supported	May be sent
CSeq	[RFC3261]	All codes	Mandatory	Mandatory
From	[RFC3261]	All codes	Mandatory	Mandatory
Supported	[RFC3261]	200	Supported	May be sent
To	[RFC3261]	All codes	Mandatory	Mandatory
Unsupported	[RFC3261]	420	Mandatory	Mandatory
Via	[RFC3261]	All codes	Mandatory	Mandatory

Table 14: Supported SIP headers in the responses to the OPTIONS request

4.3.12 INFO method

The INFO method shall be supported as specified in [RFC2976].

4.3.12.1 <u>SIP request handling</u>

The handling of this request shall be compliant with [RFC3261] and [RFC2976].

4.3.12.2 <u>Supported headers in the request</u>

Table 15 gives the header status in the INFO request for both reception and transmission directions.

Header name	Reference	Reception	Transmission
Accept	[RFC2976]	Supported	May be sent
Call-ID	[RFC2976]	Mandatory	Mandatory
Content-Length	[RFC2976]	Supported	May be sent
Content-Type	[RFC2976]	Mandatory	Mandatory
CSeq	[RFC2976]	Mandatory	Mandatory
From	[RFC2976]	Mandatory	Mandatory
Max-Forwards	[RFC2976]	Supported	May be sent
MIME-Version	[RFC3261]	Supported	May be sent
Route	[RFC2976]	Supported	May be sent
To	[RFC2976]	Mandatory	Mandatory

Header name	Reference	Reception	Transmission
Via	[RFC2976]	Mandatory	Mandatory
Content-Disposition	[RFC3204]	Mandatory	Mandatory

Table 15: Supported SIP-I headers in the INFO request

4.3.12.3 *SIP responses handling*

The handling of the responses is compliant with [RFC3261] and [RFC2976].

4.3.12.4 *Supported headers in the responses*

Table 16 gives the headers supported in the SIP responses to the INFO request for both reception and transmission directions.

Header name	Reference	Response code	Reception	Transmission
Call-ID	[RFC2976]	All codes	Mandatory	Mandatory
CSeq	[RFC2976]	All codes	Mandatory	Mandatory
From	[RFC2976]	All codes	Mandatory	Mandatory
To	[RFC2976]	All codes	Mandatory	Mandatory
Unsupported	[RFC2976]	420	Mandatory	Mandatory
Via	[RFC2976]	All codes	Mandatory	Mandatory

Table 16: Supported SIP-I headers in the responses to the INFO request

4.4 SIP headers compact form

Sending and receiving SIP headers using the compact form as defined in [RFC3261] is optional.

4.5 Maximum message size

The size of SIP messages should not exceed 2048 bytes.

The size of SDP bodies should not exceed 1024 bytes.

5. Message bodies

In the context of this document, the only SIP message body types supported are
- SDP (application subtype "application/sdp"),
- ISUP (application subtype "application/isup"),

When SDP and ISUP bodies are present in the same message, the body is a multipart MIME.

It is required the Content-Type header for multipart entities to comply with the syntax defined in the [RFC2046] §5.1.1. Especially the use of the "boundary" parameter is required. In reception both formats of the “boundary” parameter, with and without quotes, shall be supported.

6. ISUP version

It is required to comply with ISUP SPIROU signalling capabilities as defined by ARCEP.

7. Encapsulation/de-encapsulation rules

It is required to comply with the procedure defined in ITU-T Q1912.5 with the following clarifications:

- Encapsulated ISUP parameters shall take precedence over associated SIP headers except for the Request-URI and Called Party number for which dedicated procedure apply (see identities section),
- encapsulated REL messages shall take precedence over SIP messages.

8. Supported option tags of SIP extensions

In the context of this document only the option tag “timer” is authorized, if the optional keep-alive mechanism for active SIP sessions as defined in the [RFC4028] is used on bilateral agreement (see §17.1).

9. Identities format, address parameters and signalling mode

9.1 Identities at SIP level

The identities formats supported for the Request-URI, and the From, To, and P-Asserted-Identity headers are described in the following table.

NOTE - The contents of the From, P-Asserted-Identity and Privacy header shall not take precedence over the encapsulated Calling Party Number and Generic number parameters (see CLIP/CLIR section).

The address formats supported for the Route, Via, and Contact headers are also described in the following table.
SIP URI format shall comply with [RFC3261]/19.1 and TEL URI with [RFC3966].

<table>
<tr><th colspan="2">Supported formats in reception direction (NOTE 1)</th><th colspan="2">Sent formats in sending direction (NOTE 2)</th></tr>
<tr><td>From</td><td>1. SIP URI like globalnumber@domainname with user=phone
2. SIP URI like globalnumber@IP_address with user=phone
3. Tel URI in global number format</td><td>From</td><td>1. SIP URI like globalnumber@domainname with user=phone
2. SIP URI like globalnumber@IP_address with user=phone
3. Tel URI in global number format</td></tr>
<tr><td>To
(for E.164 subscriber numbers)
(NOTE 4)</td><td>1. SIP URI like globalnumber@domainname with user=phone
2. SIP URI like globalnumber@IP_address with user=phone
3. Tel URI in global number format</td><td>To
(for E.164 subscriber numbers)</td><td>1. SIP URI like globalnumber@domainname with user=phone
2. SIP URI like globalnumber@addresse_IP with user=phone
3. Tel URI in global number format</td></tr>
<tr><td>To
(for national short codes)</td><td>1. SIP URI in local number format @domainname (or @IP_address) with user=phone
2. Tel URI in local number format</td><td>To
(for national short codes)</td><td>1. SIP URI in local number format @domainname (or @IP_address) with user=phone
2. Tel URI in local number format</td></tr>
<tr><td>P-Asserted-Identity</td><td>1. SIP URI like globalnumber@domainname with user=phone
2. SIP URI like globalnumber@IP_address with user=phone
3. Tel URI in global number format</td><td>P-Asserted-Identity</td><td>1. SIP URI like globalnumber@domainname with user=phone
2. SIP URI like globalnumber@IP_address with user=phone
3. Tel URI in global number format</td></tr>
<tr><td>Request-URI
(for E.164 subscriber numbers)
(NOTE 4)</td><td>1. SIP URI like globalnumber@domainname with user=phone
2. SIP URI like globalnumber@IP_address with user=phone
3. Tel URI in global number format</td><td>Request-URI
(for E.164 subscriber numbers)</td><td>1. SIP URI like globalnumber@domainname with user=phone
2. SIP URI like globalnumber@IP_address with user=phone
3. Tel URI in global number format</td></tr>
<tr><td>Request-URI
(for national short codes)</td><td>1. SIP URI in local number format @domainname (or @IP_address) with user=phone
2. Tel URI in local number format</td><td>Request-URI
(for national short codes)</td><td>1. SIP URI in local number format @domainname (or @IP_address) with user=phone
2. Tel URI in local number format</td></tr>
<tr><td>Via</td><td>IP_address / port</td><td>Via</td><td>IP_address / port</td></tr>
<tr><td>Route</td><td>SIP URI (NOTE 3)</td><td>Route</td><td>SIP URI (NOTE 3)</td></tr>
<tr><td>Contact</td><td>SIP URI (NOTE 3)</td><td>Contact</td><td>SIP URI (NOTE 3)</td></tr>
<tr><td colspan="4">NOTE 1 – In the receiving direction, when several formats are listed (e.g. 1. 2. 3…), this means that all formats must be supported.

NOTE 2 – In the sending direction, when several formats are listed, this means that at least one format of the list must be supported.

NOTE 3 – The use of a FQDN instead of an IP address must be agreed between both connecting parties beforehand.

NOTE 4 - Encapsulated "Called Party Number" parameter can contain carrier code signals (see next table)</td></tr>
</table>

Table 17: Supported format identities

Moreover, the following principles shall be taken into consideration:

- Global-number format shall be used for E.164 subscriber numbers as described in [RFC3966]. Carrier codes shall not be part of the global number (see encapsulated “Called Party Number”).
- Local-number format shall be used for national short codes (French specific non E.164 numbers) as described in [RFC3966].
- In Global-number format, the "+" is mandatory in front of the number as described in [RFC3966]
- The telephone number must contain only digits.
- End-to-end delivery of the display-name received over the interconnection interface is not guaranteed.
- For E.164 subscriber numbers, Request-URI and To identities contain the called party number in the form of a global number. When it belongs to the French numbering range, the E.164 number shall comply with one of the following formats:
    - +CCZABPQMCDU or,
    - +CC(number portability prefix)ZABPQMCDU, with
        - CC is “33” or the country code allocated to a DOM, and
        - (number portability prefix) is a number portability prefix as defined by the French regulation authority.
- For national short codes (French specific non E.164 numbers), Request-URI and To identities contain the called party number in the form of a local-number as described in [RFC3966], including a phone-context parameter set to "+33" or the country code allocated to a DOM.

Neither call setup nor proper CLIP/CLIR service operation can be guaranteed if the recommended formats in this section are not respected.

The "en bloc" signalling mode shall be used, i.e. the entire called party number shall be included into a single INVITE request. Overlap operations are optional and out of the scope of this document.

9.2 Identities encapsulated at ISUP level

The identities encapsulated at ISUP level shall comply with SPIROU format specifications with the following clarifications:

Supported "Nature of Address" values in reception direction (NOTE 1)		**Sent "Nature of Address" values in sending direction (NOTE 2)**	
Called party number (for E.164 subscriber numbers) (NOTE 3)	1. national number with number portability prefix (recommended) or without 2. international number 3. national number with transit network selection 4. international number with transit network selection	Called party number	1. national number with number portability prefix (recommended) or without 2. international number 3. national number with transit network selection 4. international number with transit network selection
Called party number (for national short codes) (NOTE 4)	1. special number (Service Spécial)	Called party number (for national short codes)	1. special number (Service Spécial)
Calling party number	1. national number 2. international number	Calling party number	1. national number 2. international number
Generic number	1. national number 2. international number	Generic number	1. national number 2. international number
Original Called Number	1. national number 2. international number	Original Called Number	1. national number 2. international number
Redirecting Number	1. national number 2. international number	Redirecting Number	1. national number 2. international number
NOTE 1 – In the receiving direction, when several formats are listed (e.g. 1. 2. 3…), this means that all formats must be supported. NOTE 2 - In the sending direction, when several formats are listed, this means that at least one format of the list must be supported. NOTE 3 – Corresponds to cases where the Request-URI and To identities are in global-number format (E.164 number). For calls with carrier selection, the carrier code signals are included in the encapsulated ISUP Called Party Number as specified by SPIROU but shall not appear in the Request-URI and To header. NOTE 4 – Corresponds to cases where the Request-URI and To identities are in local-number format (e.g. short number used for Value Added Services).			

Table 18: Supported format identities

10. Media session management

SDP offer/answer exchange shall be performed according to [RFC3261], [RFC3264] and [RFC4566].

SDP information is only supported in the body of INVITE, re-INVITE, ACK, 200 OK (INVITE, re-INVITE) and 18x (INVITE) messages.

At minimum, the SDP parameters used in [RF3264] shall be supported.

Mechanisms and parameters defined for preconditions [RFC3312] and for SDP simple capability declaration [RFC3407] are optional.

10.1 Media session establishment

10.1.1 Initial INVITE message

This section assumes offer/answer rules solely based on [RFC3261] and RFC3264]. Additional offer/answer rules defined in [RFC3262] and [RFC3311] may be used by bilateral agreement but are out of the scope of this document.

In the context of SIP-I, initial INVITE messages shall contain an SDP offer.

Initial INVITE messages with an SDP offer shall not be coded with the address of connection (c= line) set to 0.0.0.0.

The SDP answer shall be present in the 200 OK response.

10.1.2 Codec negotiation rules

In a media stream "m=" line, codecs shall be listed in order of preference for SDP negotiation, the first codec format listed being the preferred one.

If an SDP answer is received indicating support of more than one codec different from "telephone-event" among those proposed in the SDP offer, only the first one shall be considered. To switch to another proposed media format of the SDP answer other than "telephone-event", a SDP re-negotiation shall be performed (see section 10.2).

The "a=ptime" is a media attribute which indicates the desired packetization interval that the end point would like to consider in reception for a specific media stream (but not for a specific codec). If the information is available, it is recommended to send the "ptime" parameter over the interconnection interface. The recommended packetisation times for codecs are described in section 11.

If there are no media formats in common in the SDP offer received in:

- an initial INVITE or re-INVITE, it shall be rejected by a 488 "Not acceptable here" response;
- a 200 OK response to the Re-INVITE message, the call shall be released.

10.1.3 Early media

Early media indication is supported through encapsulated ISUP information, more precisely in the “Optional Backward Call Indicators” or "Event information" ISUP parameters which indicate if there is in-band information or not.

10.2 Media session modification

Once the session is established, the modification of the parameters of the media session shall be supported through the re-INVITE message according to [RFC3261].

10.3 Terminating a session

The procedures used to terminate a session are described in [RFC3261] and ITU-T Q.1912.5 Profile C.

10.4 RTP/RTCP packet source

In a session, the same IP address and port number shall be used to send and receive RTP packets (symmetric IP address and port number).

> *Note: The port number for sending/receiving RTCP packets SHALL be equal to "the port number negotiated for RTP" + 1.*

The [RFC3556] defining SDP Bandwidth Modifiers for RTCP bandwidth can be optionally supported on bilateral agreement.

11. Voice codecs

11.1 Narrow band codecs

For mobile-mobile direct interconnection, when TrFO is activated on both sides, the following codecs are recommended:

- UMTS_AMR; SCS=12,2 ; ACS=12,2, OM = no ; MACS=1
- UMTS_AMR2; SCS=12,2 ; ACS=12,2, OM = no ; MACS=1

Otherwise, the recommended voice codecs to be used over the IP interconnection interface are G.711 A law (Payload Type=8) and G.729 (with or without annex A, Payload Type=18).

The recommended packetization delay for G.711 is 20ms.

The packetization delay for G.729 should be discussed on a bilateral basis. If no bilateral agreement is found the 20ms packetization delay should be used.

If no bilateral agreement is found on the voice codec to be supported, by default G.711 A law with a 20ms paquetization delay is used.

Further guidelines on codecs and transcoding can be found in section 20.

11.2 Wide band codecs

For mobile-mobile direct interconnection, when TrFO is activated on both sides, the following wideband codec configuration is recommended:

- WB_AMR, configuration 0 (6.6 kbps, 8.85 kbps, 12.65 kbps)

For fix-fix interconnection, the following wideband codec configuration is recommended:

- G.722 (Payload Type=9)

For fix-mobile interconnection, wide band voice currently requires transcoding between WB_AMR and G.722. This should be discussed on a bilateral basis.

The recommended packetization delay for G.722 is 20ms.

12. 64 kbit/s transparent calls

When the encapsulated ISUP “Transmission Medium Requirement” parameter is set to “64 kbit/s unrestricted”, the SDP contain Clearmode codec [RFC4040] as described in table 6 of ITU-T Q.1912.5.

13. DTMF transport

DTMF transport using telephone events [RFC4733] shall be supported.

If the use of the DTMF is in the scope of the call context the support of "telephone-event" must be indicated during the SDP offer/answer exchange. If the use of the DTMF is out of the scope of the call context (e.g. 64 kbit/s transparent calls) the support of "telephone-event" indicated during the SDP offer/answer exchange is optional.

"Telephone-event" media format for DTMF is used to carry DTMF digits in-band as defined in [RFC4733]. The encoding of the related SDP body must be done according to [RFC4733], which moreover defines the RTP payload format for DTMF digits, and with the following precisions:

- fmtp attribute must be used in order to declare the list of supported DTMF events
- Only events 0 through 15 are supported
- DTMF RTP packets must use the same sequence number and timestamp references used for media audio RTP packets

14. FAX Modem

Fax modem calls are supported by default by using the G.711 codec without media session modification

NOTE – This means that fax modem calls must be established with G.711 as the initial negotiated codec.

Alternatively, T.38 mode or Clearmode codec can be used if agreed by both connecting parties.

V.152 is optional.

15. Data Modem

Data modem calls are supported by using the G711 codec without media session modification.

NOTE – This means that data modem calls must be established with G.711 as the initial negotiated codec.

Alternatively, Clearmode codec or V.152 may be used if agreed by both connecting parties.

16. Supplementary services

16.1 CLIP/CLIR

CLIP/CLIR service is based on encapsulated ISUP information only. Corresponding SIP headers may be present in messages but shall be ignored by the recipient.

16.2 Call forwarding services

Call forwarding services are based on encapsulated ISUP information only. Corresponding SIP headers (e.g. diversion header, or History-Info) may be present in messages but shall be ignored by the recipient.

The call shall not have been diverted more than 5 times before being sent towards the SIP-I interconnection interface, i.e. the ISUP SPIROU Redirection Counter information parameter shall not exceed 5.

An anti-loop mechanism shall be used to avoid loops between the two interconnected networks. In this sense the redirection counter, mandatory for Call forwarding services according to SPIROU standard (SPIROU 1998-013), shall be sent with reliable information.

16.3 Call Hold

Call Hold service is based on encapsulated ISUP information only. Corresponding SDP parameters may be present in messages but shall not override the contents of encapsulated ISUP information.

16.4 Other supplementary services

Other SPIROU supplementary service are based on encapsulated ISUP information only. Corresponding SIP headers may be present in messages but shall not override the contents of encapsulated ISUP information.

17. Keep alive

17.1 Keep alive for active SIP sessions

A keep alive mechanism can be used to check that communications are still active. It can be performed either by sending periodic OPTIONS messages or as defined in [RFC4028] and [RFC3311]. The support for either of these methods is optional.

When OPTIONS method is used, an OPTIONS message is sent for each confirmed dialog:

- If a response is sent back, the communication is considered still active.
- If no response is sent back, an OPTIONS message may be sent again. Then, if again no response is received, the call is released.

The delay between two OPTIONS messages depends on the equipment configuration.

Acknowledgment of OPTIONS messages shall be supported as defined in [RFC3261].

17.2 Keep alive for interconnection signalling links

A similar keep alive mechanism can be used to monitor the general status of the signalling links between connecting equipments. In this case, OPTIONS or INVITE messages are sent as standalone requests.

18. Ringback tone

The ringback tone shall be delivered as media (i.e. using the voice codec) over the interconnection interface by the called party side.

19. Differences with 3GPP/TISPAN standards (informative)

This section outlines difference with standards, for the convenience of the reader. This section is informative only:

- SCTP transport is optional in this document (mandatory according to 3GPP TS.29.231),
- Support of [RFC3262], [RFC3311], [RFC3312], [RFC4715] and [RFC5079] is optional in this document (mandatory according to 3GPP TS.29.231),
- 3GPP extensions defined in section 6 of 3GPP TS.29.231 are optional,
- According to ITU-T Q.1912.5 (Profile C), SIP information must prevail over ISUP information encapsulated. However, since SIP is more open than ISUP and could potentially entail a loss of information between two CS networks (e.g. failures causes), this specification makes a different choice and ISUP information encapsulated shall prevail over SIP information (except for the Request-URI).
- UDP transport for SIP with IP fragmentation is not standard.

20. Codecs and transcoding guidelines (informative)

This section focuses on the narrow band voice codecs that should be used over the IP interconnection interface between two mobile Circuit Switched (CS) R4 networks, two fixed VoIP networks or between a fixed VoIP and a mobile CS R4 network.

From the IP interconnection interface perspective, the media end points in mobile CS networks are the transcoding units located in the mobile MGWs in case of 3G access or in the TRAU in case of 2G access. These transcoding units provide the conversion between G.711 codec and mobile compressed speech codecs (e.g. GSM FR, AMR…). In a direct mobile CS to mobile CS IP interconnection scenario, when TrFO capabilities are supported end-to-end, the media end point can be the mobile device itself.

In fixed VoIP networks there are several possible media end points that need to be considered from the IP interconnection interface perspective: VoIP terminals, IPBXs and MGWs.

In France, the two most common voice codecs used by fixed VoIP media end points are G.711 A law and G.729 (with or without Annex A). G.711 sets the voice quality reference for narrow-band voice codecs from the client perspective and is supported by many VoIP terminals in the consumer market. In certain circumstances however, G.711 is not used because of the lack of access bandwidth (G.711 requires around 106 kbit/s access bandwidth). This is the reason why some fixed VoIP terminals and IPBXs in the business market support exclusively G.729. Fixed MGWs that need to communicate with a wide range of fixed VoIP terminals consequently need to support both G.711 and G.729.

Guideline #1:
It should be noted that mobile MGWs and fixed MGWs are designed to perform transcoding and hence have optimized hardware for this purpose. As a consequence, if transcoding cannot be avoided for particular IP interconnection call configurations and if this configuration involves a MGW (mobile or fixed), it is then

recommended that the transcoding takes place in the MGW instead of any other dedicated network equipment.

Guideline #2:
Fixed VoIP terminals or IPBXs that support G.711 should also support G.729 (i.e. include both G.711 and G.729 in SDP offer/answer exchanges) in order to avoid the need for network-based transcoding when communicating with fixed terminals or IPBXs that support or can operate only G.729.

Guideline #3
In the situation whereby a Mobile CS network is interconnected with a fixed VoIP network or a transit network, the edge mobile MGW should be configured to support G.711 but also G.729 in case the distant media endpoint is a fixed VoIP terminal that supports or can operate only G.729.

21. Work plan for the next version (informative)

This section describes areas considered for further study and that will be addressed in the next version of this specification.

22. History

History of the present document		
V0.1	04/06/2010	Document creation
V0.2	22/09/2010	Document output from FFT meeting
V0.3	05/10/2010	Document input to FFT meeting
V0.4	09/11/2010	Document discussed during FFT meeting
V0.5	23/11/2010	Document input with modifications to FFT meeting
V0.6	23/11/2010	Output of meeting
V0.7	06/01/2011	Modifications based on feedback from vendors.
V1.0	Mai 2011	approved public version
V1.0.1	10/01/2012	Document input to FFT meeting of 10/01/12
V1.0.2	24/01/12	Document output from FFT meeting of 10/01/12 and additional proposals from France Télécom
V1.0.3	30/01/12	Document output from FFT meeting of 30/01/12
V1.0.4	13/02/12	Document output from FFT meeting of 13/02/12. Version sent to consultation to the FFT members and vendors.
V1.0.5	17/04/12	Modifications based on feedback from vendors and additional comments from France Télécom
V1.1	04/06/12	Approved public version