# FFT Doc 10.001 (V3.~~3~~4) (July ~~2024~~2025)

French Federation of Telecoms
Innovation & Standards Committee
IP Interconnection Working Group
Architecture Sub-group

# IP interconnection Interface specification based on SIP/SDP

***French Federation of Telecoms***

Internet
http://www.fftelecoms.org

# Table of Contents

# 1 Context

## 1.1 Purpose

The purpose of this document is to define the SIP/SDP interconnection interface for the interconnection between two French Operators for basic telephony services with deterministic charging for national and international origins and destinations.

This document supports the following basic call capabilities:

- narrowband speech and 3.1 kHz audio services (i.e. including analog fax and data modem calls),
- wideband speech,
- en bloc address signalling,
- early in-band information (forward and backward early media),
- in-band transport of DTMF tones and information (telephone-event for telephony services; G.711 in-band for M2M special usages that are not suitable with telephone-event and only for them),
- Calling party location information,
- User-to-User Information,
- Service access number before translation (for Value Added Services),
- Indication of an incoming call with international origin,
- National short numbers,
- STIR/SHAKEN call authentication.
- NG eCall,
- In-band data modem for MSD transfer
- RTT during voice calls between 2 national network operators

And the following supplementary services:

- Calling Line Identification Presentation (CLIP),
- Calling Line Identification Restriction (CLIR),
- Call Forwarding,
- Call Hold,
- Call Waiting (CW),
- Incoming Call Barring (ICB),
- Conference (CONF),
- Anonymous Call Rejection (ACR)

Important:

* In France, network operators are required to implement STIR/SHAKEN, mechanism retained by French Telcos community in Q4 of 2021 in order to authenticate the calling number displayed on called party's handset. At the time this document is edited, all impacts have not been identified yet, however a handful of comments received upon consultation leads to detail the SIP Identity header description and to list the call cases where this header is required. Clarifications or precisions related to this feature should be included in coming versions.

* Any member of FFTélécoms "IP interconnection" Working Group proposing an inter-operator interconnection voice offer based on SIP/SDP is required to ensure that its SIP interconnection specification (along with the associated test specifications) complies with the principles outlined in the current version of the FFTélécoms SIP Profile within a timeframe of 18 months. Members of the working group should respect at least a full version of the SIP profile and as much as possible the latest version. Additionally, members are strongly encouraged to include in their Specific Conditions the support and recognition of the latest profile version.

## 1.2 Standards

As a rule, the interconnection between two mobile networks shall be governed by the applicable 3GPP standards. The interconnection between two fixed networks shall be governed by the applicable TISPAN/3GPP standards.

*Note: the present document applies to all types of SIP interconnection between 2 national network operators.*

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

The table below lists the documents that are referenced in current specification. Their use depends on the context as described in dedicated sections of current specification.

| | |
|---|---|
| [Architecture V3.1_FFT] | “Architecture for IP interconnection”, FFT Doc 09.002, v3.1 |
| [ARCEP’s numbering plan] | Décision n° 2022-1583 de l’Arcep en date du 1er septembre 2022 modifiant la décision établissant le plan national de numérotation et ses règles de gestion |
| [FFTelecoms_MAN] | https://www.fftelecoms.org/man/man-mecanisme-dauthentification-des-numeros/ |
| [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" |
| [RFC3840] | IETF RFC 3840 “Indicating User Agent Capabilities in the Session Initiation Protocol (SIP))” |
| [RFC3892] | IETF RFC 3892 “The Session Initiation Protocol (SIP) Referred-By Mechanism” |
| [RFC4028] | IETF RFC 4028 "Session Timers in the Session Initiation Protocol (SIP)" |
| [RFC4032] | IETF RFC 4032 “Update to the Session Initiation Protocol (SIP) Preconditions Framework” |
| [RFC4103] | IETF RFC 4103 “RTP Payload for Text Conversation” |
| [RFC4458] | IETF RFC 4458 "Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)" |
| [RFC4566] | IETF RFC 4566 "Session Description Protocol (SDP)" |
| [RFC4733] | IETF RFC 4733 "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals" |
| [RFC5009] | IETF RFC 5009 "Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media" |
| [RFC5194] | IETF RFC5194 “"Framework for Real-Time Text Over IP Using the Session Initiation Protocol (SIP)" |
| [RFC5806] | IETF RFC 5806 "Diversion Indication in SIP" |
| [RFC6086] | IETF RFC 6086 “Session Initiation Protocol (SIP) INFO Method and Package Framework” |
| [RFC6337] | IETF RFC 6337 “Session Initiation Protocol (SIP) Usage of the Offer/Answer Model” |
| [RFC6432] | IETF RFC 6432 “Carrying Q.850 Codes in Reason Header Fields in SIP (Session Initiation Protocol) Responses” |
| [RFC6567] | IETF RFC 6567 “Problem Statement and Requirements for Transporting User-to-User Call Control Information in SIP” |
| [RFC7044] | IETF RFC 7044 “An Extension to the Session Initiation Protocol (SIP) for Request History Information” (obsoletes RFC 4244) |
| [RFC7315] | IETF RFC 7315 “Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP” |
| [RFC7433] | IETF RFC 7433 “A Mechanism for Transporting User to User Call Control Information in SIP” |
| [RFC7434] | IETF RFC 7434 ”Interworking ISDN Call Control User Information with SIP” |
| [RFC7544] | IETF RFC 7544 “Mapping and Interworking of Diversion Information between Diversion and History-Info Header Fields in the Session Initiation Protocol (SIP)” (obsoletes RFC6044) |
| [RFC7462] | IETF RFC 7462 “URNs for the Alert-Info Header Field of the Session Initiation Protocol (SIP)” |
| [RFC7913] | IETF RFC 7913 “P-Access-Network-Info ABNF Update” |
| [RFC8224] | IETF RFC 8224 “Authenticated Identity Management in the Session Initiation Protocol (SIP)” |
| [RFC8119] | IETF RFC 8119 “SIP "cause" URI Parameter for Service Number Translation” |
| [RFC8147] | IETF RFC 8147 “Next-Generation Pan-European eCall” |

| | |
|---|---|
| [RFC8224] | Authenticated Identity Management in the Session Initiation Protocol (SIP) |
| [RFC8225] | PASSporT: Personal Assertion Token |
| [RFC8226] | Secure Telephone Identity Credentials: Certificates |
| [RFC8588] | Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN) |
| [RFC9071] | RTP-Mixer Formatting of Multiparty Real-Time Text |
| [TS 24.229] | 3GPP Technical Specification 24.229 "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3" |
| [TS 24.604] | 3GPP Technical Specification 24.604 "Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification" |
| [TS 24.628] | 3GPP Technical Specification 24.628 "Common basic communication procedures using IP Multimedia (IM)Core Network (CN) subsystem; Protocol specification" |
| [TS 26.114] | 3GPP Technical Specification 26.114 "IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction" |
| [TS 26.267] | 3GPP eCall data transfer _ In-band data modem solution |
| [TS 103.919] | Emergency Communications (EMTEL); Accessibility and interoperability of emergency communications and for the answering of emergency communications by the public safety answering points (PSAPs) (including to the single European Emergency number 112) |
| [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" |
| [T.140] | ITU-T Rec. ""Protocol for multimedia application text conversation" |
| [T.140] Addendum 1 | ITU-T Rec.""Protocol for multimedia application text conversation – Addendum 1" |

# 3 Glossary

| | |
|---|---|
| CLIP | Calling Line Identity Presentation |
| CLIR | Calling Line Identity Restriction |
| DROM | Départements-Régions d'Outre-Mer (French Overseas Departments) |
| DTMF | Dual-Tone Multi-Frequency |
| IVS | In-Vehicle System |
| M2M | Machine To Machine |
| MAN | Mécanisme d'Authentification des Numéros |
| MIME | Multipurpose Internet Mail Extension |
| MSD | Minimum Set of Data |
| NNI | Network to Network Interface |
| NO | Network Operator |
| PSAP | Public Safety Access Point |
| RTT | Real-Time Text |
| SIP | Session Initiation Protocol |
| SDP | Session Description Protocol |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| STIR | Secure Telephone Identity Revisited |
| TCP | Transport Control Protocol |
| TN | Telephone Number |
| UDP | User Datagram Protocol |
| UUI | User-to-User header |
| URI | Uniform Resource Identifier |
| VAS | Value Added Services |

# 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 11 for the initial INVITE message.

## 4.1 Transport protocol

UDP is supported and required for carrying SIP messages. See Maximum message size section 4.4.

*Note: According to IETF RFC 3261, TCP must be supported. This requirement arises out of the need to handle large messages. However, the size of messages is limited in the context of this document.*

## 4.2 SIP methods and headers

### 4.2.1 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.
  If a mandatory header is absent from the SIP request, the receiving operator should reject the request and return an appropriate error response,
- Not applicable" means that the reception of the header cannot occur according to the current specification. If received, either the receiver removes the header, or it releases the call.
  By symmetry "Not applicable" is related only to headers with the status "not sent" in emission.

If a SIP header received is not defined in the corresponding header table, it is considered as "not supported" (this header may be removed without impacting the call establishment.

**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.

### 4.2.2 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 (NOTE 1) |
| ACK |
| BYE |
| CANCEL |
| OPTIONS (NOTE 2) |
| INFO (NOTE 3) |

***Table 1: Mandatory SIP methods***

NOTE 1: As stated in RFC 3261, an INVITE request sent within an existing dialog is known as a re-INVITE.

NOTE 2: It is mandatory to support OPTIONS in the reception direction only.

NOTE 3: SIP INFO is added in order to support NG eCall service. It cannot be used for any other purpose.
t
NOTE 4: 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 §19.1).

NOTE 5: When the SIP preconditions are used (see criteria in section 13.1.4.1) and only in this case, PRACK and UPDATE methods shall be supported in addition to the list of mandatory SIP methods given in Table 1.

### 4.2.3 Network behaviour in reception

#### *4.2.3.1 Method inspection*

If a SIP method received is recognized but not supported, it shall be rejected as defined in [RFC 3261] 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 [RFC 3261] by a 501 "Not Implemented" response.

#### *4.2.3.2 Status code inspection*

If a non-supported error response is received in a SIP message then the related call or transaction fails. The list of the supported and of the Not applicable responses with their detailed handling is given in section 4.2.5.3, Table 3.
If a non-recognized final response, i.e. not referenced in the section 4.2.5.3Table 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 4.2.5.3 Table 3, is received in a SIP message then it shall be treated as being equivalent to a 183 “Session Progress”.

#### *4.2.3.3 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 4.2.5 to section 4.2.10 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 [RFC 3261].

#### *4.2.3.4 Header inspection in responses*

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 4.2.5 to section 4.2.10 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.

### 4.2.4 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.

### 4.2.5 Initial INVITE method

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

#### *4.2.5.1 SIP request handling*

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

#### *4.2.5.2 Supported headers in the request*

Table 2 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 |
| Call-Info | [RFC8147] | Supported | May be sent. See section 23 |
| Contact | [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 |
| CSeq | [RFC3261] | Mandatory | Mandatory |
| Date | [RFC3261] | Supported | May be sent (with content based on time zone UTC) |
| Diversion | [RFC5806] | Supported for Call forwarding service in some conditions (see criteria in section 18.2). | May be sent for Call forwarding service in some conditions (see criteria in section 18.2). |
| From | [RFC3261] | Mandatory | Mandatory |
| History-Info | [RFC8119] | Supported for “Service access number before translation” (cf. section 8). | May be sent for “Service access number before translation” (see section 8). |
| | [RFC7044] | Supported for Call forwarding service in some conditions (see criteria in section 18.2). | May be sent for Call forwarding service in some conditions (see criteria in section 18.2). |
| Identity | [RFC8224] | Supported | Mandatory (see criteria given in section 11) |
| Max-Forwards | [RFC3261] | Mandatory | Mandatory |
| Min-SE | [RFC4028] | Supported | May be sent |
| P-Access-network-info | [3GPP TS.24.229] | Supported. See section 5 and section 6 | May be sent. See section 5 and section 6 |
| P-Asserted-Identity | [RFC3325] | Supported. See § 18.1. | May be sent. See section 18.1. |
| P-Early-Media | [RFC5009] | Supported. Only “supported” value is supported. See § 13.1.3. | May be sent. Only “supported” value is supported. See section 13.1.3. |
| P-Identity-Bypass | Cf. ‘Mode opératoire du mécanisme de confiance MAN’ [FFTelecoms_MAN] | Supported | May be sent |
| Privacy | [RFC3323] | Supported. See § 18.1. | May be sent. See § 18.1. |
| 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 |
| Recv-Info | [RFC8147] | Supported | May be sent. See section 23 |
| Require | [RFC3261] | Not applicable | Not sent |
| To | [RFC3261] | Mandatory | Mandatory |
| User-to-User | [RFC7433] | Supported. See section 7 | May be sent. See section 7 |
| Via | [RFC3261] | Mandatory | Mandatory |

***Table 2: Supported SIP headers in the initial INVITE request***

#### *4.2.5.3 SIP response handling*

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.

Multiple SIP provisional responses creating separate early dialogs, as specified in [RFC3261], are supported with the following clarifications:

- Upon receipt of provisional responses containing SDP bodies, the recipient shall use the most recent media session information received for sending media packets during the early dialog phase,
- Confirmed dialogs created by the first 200 OK response for non-existing early dialogs shall override any previously stored dialog information.

Note: Interconnected operators shall ensure that a unique media flow associated to the call is sent over the interconnection at a given time.

| 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 ** | Supported | May be 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 (note 1). | May be sent |
| | 400 Bad Number Format | Supported (note 1). | 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. (note 1). | May be sent |
| | 403 Stale date | Supported | May be sent |
| | 404 Not Found | Supported. The related call or transaction fails. (note 1). | May be sent |
| | 405 Method Not Allowed | Supported (note 1). | May be sent |
| | 406 Not Acceptable | Supported. The related call or transaction fails. (note 1). | May be sent |
| | 407 Proxy Authentication Required | Not applicable | Not sent |
| | 408 Request Timeout | Supported (note 1). | May be sent |
| | 410 Gone | Supported. The related call or transaction fails. (note 1). | May be sent |
| | 413 Request Entity Too Large | Supported The related call or transaction fails. (note 1). | May be sent |
| | 414 Request-URI Too Long | Supported. The related call or transaction fails. (note 1). | May be sent |

| SIP response | | Reception | Transmission |
|---|---|---|---|
| | 415 Unsupported Media Type | Supported.<br>The related call or transaction fails. (note 1). | May be sent |
| | 416 Unsupported URI Scheme | Supported.<br>The related call or transaction fails. (note 1). | May be sent |
| | 420 Bad Extension | Supported.<br>The related call or transaction fails. (note 1). | May be sent |
| | 421 Extension Required | Not applicable | Not sent |
| | 422 Session Interval Too Small | Supported (note 1). | May be sent |
| | 423 Interval Too Brief | Not applicable | Not sent |
| | 428 No Id Header | Supported (note 1). | May be sent |
| | 433 Anonymity Disallowed | Supported (note 1). | May be sent |
| | 436 Bad Identity Info | Supported (note 1). | May be sent |
| | 437 Unsupported Credential | Supported (note 1). | May be sent |
| | 438 Invalid Identity Header | Supported (note 1). | May be sent |
| | 480 Temporarily Unavailable | Supported.<br>The related call or transaction fails. (note 1). | May be sent |
| | 481 Call/Transaction Does Not Exist | Supported.<br>The related call or transaction fails. (note 1). | May be sent |
| | 482 Loop Detected | Supported.<br>The related call or transaction fails. (note 1). | May be sent |
| | 483 Too Many Hops | Supported.<br>The related call or transaction fails. (note 1). | May be sent |
| | 484 Address Incomplete | Supported.<br>The related call or transaction fails. (note 1). | May be sent |
| | 485 Ambiguous | Not applicable | Not sent |
| | 486 Busy here | Supported.<br>The related call or transaction fails. (note 1). | May be sent |
| | 487 Request Terminated | Supported.<br>The related call or transaction fails. (note 1). | May be sent |
| | 488 Not acceptable here | Supported.<br>The related call or transaction fails. (note 1). | Sent if the received request contains an SDP offer proposing non supported media format or IP version. |
| | 491 Request Pending | Supported.<br>For re-INVITE request, the behaviour recommended in [RFC3261]/14.1 on reception of this response is supported. | May be sent.<br>For re-INVITE request, the behaviour recommended in [RFC3261]/14.1 on reception of this response is supported. |
| | 493 Undecipherable | Supported.<br>The related call or transaction fails (note 1). | May be sent |

| SIP response | | Reception | Transmission |
|---|---|---|---|
| 5xx | | Supported.<br>The related call or transaction fails.<br>(note 1). | May be sent* |
| 6xx | 600 Busy Everywhere | Supported.<br>The related call or transaction fails.<br>(note 1). | May be sent |
| | 603 Decline | Supported.<br>The related call or transaction fails.<br>(note 1). | May be sent |
| | 604 Does Not Exist Anywhere | Supported.<br>The related call or transaction fails.<br>(note 1). | May be sent |
| | 606<br>Not Acceptable | Supported.<br>The related call or transaction fails.<br>(note 1). | May be sent |

***Table 3: 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".

** : no header containing the diverted number shall be present in 181 response sent at the SIP NNI. ~~If a Diversion header or an History-Info header is received from the downstream interconnected operator, this information shall be ignored.~~

Note 1: the reception of this response shall not lead to a retransmission of the request by the upstream operator when receiving this message.

#### *4.2.5.4 Supported headers in the responses*

Table 4 gives the header statuses 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 |
| Alert-Info | [RFC3261] and [RFC7462] | 180 | Supported<br>See section 18.4. | May be sent<br>See section 18.4. |
| Allow | [RFC3261] | All codes | Supported | May be sent |
| Call-ID | [RFC3261] | All codes | Mandatory | Mandatory |
| Call-Info | [RFC8147] | 200, 486, 600, 603 | Supported | May be sent. See section 23. |
| Contact | [RFC3261] | 1xx (except 100) | Supported | May be sent |
| Contact | [RFC3261] | 200 | Mandatory | Mandatory |
| 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 | Mandatory | Mandatory |
| P-Asserted-Identity | [RFC3325] | 200 | Supported. See section 18.1. | May be sent. See section 18.1. |

| Header name | Reference | Response code | Reception | Transmission |
|---|---|---|---|---|
| P-Early-Media | [RFC5009] | 18x | Supported with the restrictions described in section 13.1.3. | May be sent with the restrictions described in section 13.1.3. |
| Recv-Info | [RFC8147] | 200, 486, 600, 603 | Supported | May be sent. See section 23. |
| RSeq | [RFC3262] | 18x | Supported when the SIP preconditions are used (see criteria in section 12.1.4.1) and only in this case. Not applicable otherwise. | May be sent when the SIP preconditions are used (see criteria in section 12.1.4.1) and only in this case. Not applicable otherwise. |
| Reason | [RFC3326] and [RFC6432] | All relevant codes | Supported | May be sent |
| Record-Route | [RFC3261] | 18x<br>200 | Not applicable | Not sent |
| Require | [RFC3261] | 18x | Supported when the SIP preconditions are used (see criteria in section 12.1.4.1) and only in this case. Not applicable otherwise. | May be sent when the SIP preconditions are used (see criteria in section 12.1.4.1) and only in this case. Not applicable otherwise. |
| 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 |
| User-to-User | [RFC7433] | All codes (except 100) **if end-to-end responses** | Supported. See section 7 | May be sent. See section 7 |
| Via | [RFC3261] | All codes | Mandatory | Mandatory |

***Table 4: Supported SIP headers in the responses to the initial INVITE request***

### 4.2.6 Re-INVITE method

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

#### *4.2.6.1 SIP request handling*

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

#### *4.2.6.2 Supported headers in the request*

Table 5 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-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 |

| | | | |
|---|---|---|---|
| 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 5: Supported SIP headers in the re-INVITE request***

#### *4.2.6.3 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.

#### *4.2.6.4 Supported headers in the responses*

Table 6 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] | 415 | Mandatory | Mandatory |
| Allow | [RFC3261] | All codes | Supported | May be sent |
| Call-ID | [RFC3261] | All codes | Mandatory | Mandatory |
| Contact | [RFC3261] | 200 | Supported | May be sent |
| 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 |
| Min-SE | [RFC4028] | 422 | Mandatory | Mandatory |
| 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 6: Supported SIP headers in the responses to the re-INVITE request***

### 4.2.7 CANCEL method

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

#### *4.2.7.1 SIP request handling*

The handling of this request shall be compliant with [RFC3261].
When the calling party side wishes to terminate the session during the early-dialog phase it is recommended to use the Cancel method instead of the Bye method.

#### *4.2.7.2 Supported headers in the request*

Table 7 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 |

| Header name | Reference | Reception | Transmission |
|---|---|---|---|
| Max-Forwards | [RFC3261] | Mandatory | Mandatory |
| Reason | [RFC3326] | Supported | May be sent |
| Route | [RFC3261] | Supported | May be sent |
| To | [RFC3261] | Mandatory | Mandatory |
| Via | [RFC3261] | Mandatory | Mandatory |

***Table 7: 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].

#### *4.2.7.3 SIP response handling*

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

#### *4.2.7.4 Supported headers in the responses*

Table 8 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 8: Supported SIP headers in the SIP responses to the CANCEL request***

### 4.2.8 ACK method

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

#### *4.2.8.1 SIP request handling*

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

#### *4.2.8.2 Supported headers in the request*

Table 9 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 |
| Route | [RFC3261] | Supported | May be sent |
| To | [RFC3261] | Mandatory | Mandatory |
| Via | [RFC3261] | Mandatory | Mandatory |

***Table 9: Supported SIP headers in the ACK request***

### 4.2.9 BYE method

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

#### *4.2.9.1 SIP request handling*

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

#### *4.2.9.2 Supported headers in the request*

Table 10 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 |
| CSeq | [RFC3261] | Mandatory | Mandatory |
| From | [RFC3261] | Mandatory | Mandatory |
| Max-Forwards | [RFC3261] | Mandatory | Mandatory |
| P-Asserted-Identity | [RFC3325] | Supported | May be sent |
| Reason | [RFC3326] | Supported | May be sent |
| Route | [RFC3261] | Supported | May be sent |
| To | [RFC3261] | Mandatory | Mandatory |
| User-to-User | [RFC7433] | Supported. See section 7 | May be sent. See section 7 |
| Via | [RFC3261] | Mandatory | Mandatory |

***Table 10: 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].

#### *4.2.9.3 SIP response handling*

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

#### *4.2.9.4 Supported headers in the responses*

Table 11 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-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 |
| User-to-User | [RFC7433] | All codes (except 100) **if end-to-end responses** | Supported. See section 7 | May be sent. See section 7 |
| Via | [RFC3261] | All codes | Mandatory | Mandatory |

***Table 11: Supported SIP headers in the responses to the BYE request***

### 4.2.10 OPTIONS method

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

#### *4.2.10.1 SIP request handling*

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

#### *4.2.10.2 Supported headers in the request*

Table 12 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 |
| Allow | [RFC3261] | Supported | May be sent |
| 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 |
| P-Asserted-Identity | [RFC3325] | Supported | May be sent |
| Supported | [RFC3261] | Supported | May be sent |
| To | [RFC3261] | Mandatory | Mandatory |

| Header name | Reference | Reception | Transmission |
|---|---|---|---|
| Via | [RFC3261] | Mandatory | Mandatory |

***Table 12: Supported SIP headers in the OPTIONS request***

#### *4.2.10.3 SIP response handling*

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

#### *4.2.10.4 Supported headers in the responses*

Table 13 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] | 415 | Mandatory | Mandatory |
| 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 |
| 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 13: Supported SIP headers in the responses to the OPTIONS request***

### 4.2.11 PRACK method

When the SIP preconditions are used (see criteria in section 13.1.4.1) and only in this case, the PRACK method shall be supported as specified in [RFC3262].

#### *4.2.11.1 SIP request handling*

The handling of this request shall be compliant with [RFC3262].

#### *4.2.11.2 Supported headers in the request*

Table 14 gives the header status in the PRACK 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 |
| CSeq | [RFC3261] | Mandatory | Mandatory |
| From | [RFC3261] | Mandatory | Mandatory |
| Max-Forwards | [RFC3261] | Mandatory | Mandatory |
| P-Early-Media | [RFC5009] | Supported | May be sent |
| Route | [RFC3261] | Supported | May be sent |
| Require | [RFC3261] | Supported | May be sent |
| Supported | [RFC3261] | Supported | May be sent |
| Rack | [RFC3262] | Mandatory | Mandatory |
| To | [RFC3261] | Mandatory | Mandatory |
| Via | [RFC3261] | Mandatory | Mandatory |

***Table 14: Supported SIP headers in the PRACK request***

#### 4.2.11.3 SIP response handling

The handling of the responses shall be compliant with [RFC3262].

#### 4.2.11.4 Supported headers in the responses

Table 15 gives the header status in the SIP responses to the PRACK request for both reception and transmission directions.

| Header name | Reference | Response code | Reception | Transmission |
|---|---|---|---|---|
| Accept | [RFC3261] | 200 | Supported | May be sent |
| Accept | [RFC3261] | 415 | Mandatory | Mandatory |
| 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] | 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 |
| P-Early-Media | [RFC5009] | 200 | Supported | May be sent |
| Require | [RFC3261] | 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 15: Supported SIP headers in the responses to the PRACK request***

### 4.2.12 UPDATE method

The UPDATE method can only be used and is only supported, as specified in [RFC3311], in the following cases:

- When the SIP preconditions are used (see criteria in section 13.1.4.1).
- For keep-alive purpose if the use of [RFC4028] is agreed according to bilateral agreement (see §19). In such a case, UPDATE request contains no SDP.

#### 4.2.12.1 SIP request handling²

The handling of this request shall be compliant with [RFC3311].

#### 4.2.12.2 Supported headers in the request

Table 16 gives the header status in the UPDATE 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-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 |
| P-Early-Media | [RFC5009] | Supported | May be sent |
| Route | [RFC3261] | Supported | May be sent |
| Require | [RFC3261] | Supported | May be sent |
| Supported | [RFC3261] | Supported | May be sent |
| To | [RFC3261] | Mandatory | Mandatory |
| Via | [RFC3261] | Mandatory | Mandatory |

***Table 16: Supported SIP headers in the UPDATE request***

#### *4.2.12.3 SIP response handling*

The handling of the responses shall be compliant with [RFC3311].

#### *4.2.12.4 Supported headers in the responses*

Table 17 gives the header status in the SIP responses to the UPDATE request for both reception and transmission directions.

| Header name | Reference | Response code | Reception | Transmission |
|---|---|---|---|---|
| Accept | [RFC3261] | 200 | Supported | May be sent |
| Accept | [RFC3261] | 415 | Mandatory | Mandatory |
| Allow | [RFC3261] | All codes | Supported | May be sent |
| Call-ID | [RFC3261] | All codes | Mandatory | Mandatory |
| Contact | [RFC3261] | 200 | Mandatory | Mandatory |
| 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 |
| P-Early-Media | [RFC5009] | 200 | Supported | May be sent |
| Require | [RFC3261] | 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 17: Supported SIP headers in the responses to the UPDATE request***

### 4.2.13 INFO method

The INFO method [RFC6086] can be used at the SIP inter-operator NNI, only for the purpose of NG eCall MSD transfer as specified in [RFC8147].

#### *4.2.13.1 SIP request handling²*

The handling of this request shall be compliant with [RFC6086] and [RFC8147].

#### *4.2.13.2 Supported headers in the request*

Table 18 gives the header status in the INFO 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 |
| Call-Info | [RFC8147] | Mandatory | Mandatory |
| Content-Disposition | [RFC8147] | Mandatory | Mandatory |
| Content-Length | [RFC3261] | Mandatory as the body for MSD meta data is always present | Mandatory as the body for MSD meta data is always present |
| Content-Type | [RFC3261] | Mandatory as the body for MSD meta data is always present | Mandatory as the body for MSD meta data is always present |
| CSeq | [RFC3261] | Mandatory | Mandatory |
| From | [RFC3261] | Mandatory | Mandatory |
| Info-Package | [RFC8147] | Mandatory | Mandatory |
| Max-Forwards | [RFC3261] | Mandatory | Mandatory |
| ~~Recv-Info~~ | ~~[RFC6086]~~ | ~~Mandatory~~ | ~~Mandatory~~ |
| Route | [RFC3261] | Supported | May be sent |
| To | [RFC3261] | Mandatory | Mandatory |
| Via | [RFC3261] | Mandatory | Mandatory |

***Table 18: Supported SIP headers in the INFO request***

#### *4.2.13.3 SIP response handling*

The handling of the responses shall be compliant with [RFC6086].

#### *4.2.13.4 Supported headers in the responses*

Table 19 gives the header status in the SIP responses to the INFO request for both reception and transmission directions.

| Header name | Reference | Response code | Reception | Transmission |
|---|---|---|---|---|
| Accept | [RFC3261] | 200 | Supported | May be sent |
| Accept | [RFC3261] | 415 | Mandatory | Mandatory |
| Allow | [RFC3261] | All codes | Supported | May be sent |
| Call-ID | [RFC3261] | All codes | Mandatory | Mandatory |
| Contact | [RFC3261] | 200 | Mandatory | Mandatory |
| 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 |
| Recv-Info | [RFC6086] | 469 | Mandatory | Mandatory |
| To | [RFC3261] | All codes | Mandatory | Mandatory |
| Unsupported | [RFC3261] | 420 | Mandatory | Mandatory |
| Via | [RFC3261] | All codes | Mandatory | Mandatory |

***Table 19: Supported SIP headers in the responses to the INFO request***

## 4.3 SIP headers compact form

As stated in [RFC3261] it is optional to send SIP headers in compact forms, but implementations must support both the long and short forms of each header name in reception.

## 4.4 Maximum message size

Each network operator is responsible to check that the maximum size of SIP message and of SDP body it applies end to end does not prevent services to be delivered.

The maximum size of SIP message and of SDP body shall be **exchanged between the two interconnected operators in a bilateral agreement.**

If no agreement is found the following values shall be used by default:

- The size of SIP messages should not exceed 2048 bytes.
- The size of SDP bodies should not exceed 1024 bytes.

# 5 Calling party's location information for calls towards Value Added Services (VAS)

The calling party's location information can be optionally transmitted over the SIP interconnection interface according to bi-lateral agreement between interconnected network operators. The current specification takes into account the need to transmit location information of the calling party especially for interconnection calls towards national VAS when location information cannot easily be determined after analysis of first digits of calling line number contained in the P-Asserted-Identity header (for instance when calling line's number is a national ~~non~~ non-geographic number such as +336ABPQMCDU or +339ABPQMCDU).

Important: ARCEP decision n°2019 0954 of 2019, July the 11th comes to no more correlating the ZABPQ of a national fixed geographic calling line number +33ZABPQMCU with the actual location of the associated land line. As a conclusion, when the calling party is located in France, it is highly recommended to send calling party's location for interconnection calls towards national VAS, whatever the type of number contained in the P-Asserted-Identity header sent in initial INVITE request (national non-geographic number, national geographic number, international mobile number).

Note 1: new contexts may exist in the future, which require transmitting from now the location information into the initial INVITE request sent at the SIP interconnection interface. In these cases, the same solution for location information transmission applies.

The purpose of this chapter is to provide a SIP solution to transport the calling party's location information identical to the one of the SPIROU 'Location Number' parameter.

If transmitted, this location information shall be network provided. The location information provided by the network is identical to the one carried by the SPIROU Location Number parameter. It contains the originating network identifier (Operator Code) assigned by ARCEP to originating operator (as defined in Décision n°2019 0954, 11 juillet 2019 and in Table 18) and the location area code associated to calling party's geographic location. This information depends on the originating network nature:

- mobile originating network: BTS/nodeB post code.
- fixed originating network: INSEE code of the city, except in case of Paris, Lyon and Marseille where subdivisions are used.

– Note 2: if the calling user is located in France but no accurate information is available for providing required 'location area code', it is recommended to use C1…C5='00000' value.

| **Use of R1R2 operator code and associated C1…C5 coding (within PANI header) over the interconnection interface** | | | |
|---|---|---|---|
| R1R2 operator code value | Usage | R1R2 operator code signification | C1…C5 coding |
| 00 | Forbidden over the interconnection interface | | |
| 01 | Allowed | Identifier of the fixed originating network or the undefined originating network | INSEE code (note 2) |
| From 02 to 92 | Allowed | Identifier of the mobile originating network | Post code (note 2) |
| From 93 to 97 | Not used over the interconnection interface (reserved for potential future use cases) | | |
| 98 | Not used over the interconnection interface (no usage has been identified so far by the FFTelecoms) | Identifier of the fixed originating network or the undefined originating network | Post code |
| 99 | See section 6 for this operator code value, its usage and the related C1…C5 coding | | |

***Table 20: Use of R1R2 operator codes and associated C1…C5 coding (within PANI header) over the SIP interconnection interface***

The P-Access-Network-Info header field, as defined in [3GPP TS24.229] §7.2A.4, is used to carry this location information. The location information provided by the originating network operator shall be placed in the "operator-specific-GI" parameter and shall be equal to $R_1R_2C_1C_2C_3C_4C_5$, where $R_1R_2$ are the 2 digits of the Operator Code and $C_1C_2C_3C_4C_5$ are the 5 digits of the post code or INSEE code (as defined in Decision n°2019 0954, July the 11th of 2019 and in Table 18). Moreover the “np” (network provided) parameter shall be present.

If the location information sent at the interconnection interface is improperly formatted (e.g. wrong number of digits), service dysfunctions may occur for non-geographic caller numbers.

Therefore, the P-Access-Network-Info header carrying the calling party’s location information provided by the network shall be coded according to the following syntax:

**P-Access-Network-Info:(access-type / access-class);operator-specific-GI=**”value“**;network-provided**

The access-type or access-class parameters are by default not significant for the current specification. Nevertheless, according to the P-Access-Network-Info header field specification of the [3GPP TS24.229] §7.2A.4 it is mandatory to have one of them and their value always shall be compliant with this specification. Consideration of this field must be done according to a bilateral agreement.

The access-info parameters “operator-specific-GI” and “np” parameters shall always be present. The value of the operator-specific-GI parameter shall be compliant with the 3GPP TS 29.163 standard and the value of the SPIROU Location Number (described in SPIROU1998-005 /edition 1.0 §3.30 Location Number and in the Decision ARCEP n° 05-0521 of December 8th 2005 annex A) populates the operator-specific-GI parameter. The operator-specific-GI is set to the text string between quotes (double quotes) with the sequence of digits found in byte 3 to N (except the filler) starting with the 1st digit:

operator-specific-GI = $R_1R_2C_1C_2C_3C_4C_5XX$

where $R_1R_2$ are the 2 digits of the Operator Code and $C_1C_2C_3C_4C_5$ are the 5 digits of the Location Area Code as specified in table 18, and

where XX are 2 digits from 0 to 9 reserved for future use, for now set to 00.

Hereafter is given an example of P-Access-Network-Info header field for a user located in the Orange mobile access network (61) in Issy-les-Moulineaux (92130), with XX=00:
P-Access-Network-Info:GSTN;operator-specific-GI=“619213000”;network-provided

NOTE – This specification requires only “operator-specific-GI” and “np” values as “access-info” parameters. Additional access-info parameters are possible, but they are out of scope of the current specification. Therefore, they can be exchanged only on bilateral agreement and in this case, they always shall be compliant with the P-Access-Network-Info header field specification of the [3GPP TS24.229] §7.2A.4.

# 6 Indication of an incoming call with international origin

In this section, a call having an “international origin” means that the call is either emitted from the international network or that at least an international interconnection link/trunk has been used for establishing this call.

During or after call completion, the information that a call received at national SIP interconnection interface has an international origin (or not) is required. For example, this information is necessary for some real-time applications (e.g. barring of an international call when a national fixed number is contained in From header of INVITE request, services triggering, VAS…) or for some offline purposes such as monitoring, accounting or billing (e.g. wholesale billing, statistics).

Therefore, ~~It~~ it is mandatory~~recommended~~ that the information that an incoming call has an international origin is provided at the national SIP ~~national~~ interconnection interface for calls towards national destinations, especially by ~~the~~ upstream national operators that ~~is~~ are interconnected ~~to the~~with international operators delivering the calls towards ~~the~~ national called numbers (cf. figure in Annex 1 (§~~24~~29)).

When this indication is provided at SIP national interconnection interface:

- End to end transmission of this indication ~~is~~ shall be guaranteed for calls towards national VAS (Z=8) and ~~is~~ shall be guaranteed for all national destinations in full SIP case.

End to end transmission of this indication is (by default) not guaranteed for calls towards other destinations ~~other than national VAS (Z=8) in~~ (cf. case of interworking with circuit switched networks). ~~but may be guaranteed according to bilateral agreement.~~

-

When the calls that have an international origin are identified at SIP national voice interconnection interface, it shall be done as follows:
The P-Access-Network-Info header field, as defined in [3GPP TS 24.229] §7.2A.4, is used to carry this indication. This indication shall be placed in the "operator-specific-GI" parameter and shall be equal to $R_1R_2C_1C_2C_3C_4C_5X_1X_2$ where:

- $R_1R_2$ shall be set to “99” value (cf. Decision ARCEP n°2019-0954, 11 juillet 2019),
- $C_1C_2C_3C_4C_5$ shall be set to “99999” value (other values are reserved for future inter-operators use),
- $X_1X_2$ shall be set to “00” value.

The P-Access-Network-Info header carrying the indication that a call has an international origin shall be coded according to the following syntax:

**P-Access-Network-Info:(access-type / access-class);operator-specific-GI=**”value“**;network-provided**

The access-info parameters “operator-specific-GI” and “np” (network provided) shall always be present.
The operator-specific-GI in the access-info field is coded as a text string between double quotes (i.e. quoted-string).
The access-type or access-class parameters are not significant for the current specification. Nevertheless, according to [RFC 7315] and [RFC 7913], it is mandatory to have one of them and their value always shall be compliant with these specifications.
For the current specification, the access-type parameter is set to “GSTN” (not significant).

Hereafter is given an example of P-Access-Network-Info header field carrying the indication that a call has an international origin, with access-type set to “GSTN” and within operator-specific-GI, $R_1R_2$ set to “99” and $C_1C_2C_3C_4C_5$ set to “99999”:

P-Access-Network-Info:GSTN;operator-specific-GI=“999999900”;network-provided

If received, the P-Access-Network-Info header carrying the indication that a call has an international origin shall be transmitted over the SIP interconnection interface.

NOTE: Since there is no standardized solution to carry in SIP the indication that a call has an international origin, a national specific solution is defined here. As the interworking is thereby not described in standards, some precisions are given below:
The indication that a call has an international origin (cf. syntax above) in P-Access-Network-Info header in initial INVITE request is equivalent and should interwork to “1” value of ISUP “National/international call indicator” (bit A) of “Forward Call Indicators” parameter in IAM message (cf. ITU-T Q763, §3.23).
In case of interworking from SIP to ISUP (or SIP-I), upon reception of the SIP P-Access-Network-Info header carrying the indication that a call has an international origin (cf. syntax above), the ISUP “National/international call indicator” (bit A) of “Forward Call Indicators” parameter should be set to “1” value and no ISUP Location Number parameter should be generated in ISUP (or in SIP-I).

# 7 User to User Information

The SIP User-to-User header (UUI), defined in [RFC7433], has been created to convey transparently in SIP end-to-end user-to-user information, in conformance with the function requirements defined in [RFC6567].
The current FFT specification only considers “ISDN” user-to-user information exchange as specified in [RFC7434] for VAS services framework. This information is analog to and can interwork with the one of the ISDN UUS1 implicit supplementary service. Therefore, the UUI header field can be present only in INVITE requests and responses, and in BYE requests and responses. When the UUI header field is used in responses, it can only be utilized in end-to-end responses, for example in 1xx (excluding 100) and 2xx responses.

The syntax of UUI header [RFC7433] is the following:

```
UUI  = "User-to-User" HCOLON uui-value *(COMMA uui-value)
uui-value   = uui-data *(SEMI uui-param)
uui-data    = token / quoted-string
uui-param   = pkg-param / cont-param / enc-param / generic-param
pkg-param   = "purpose" EQUAL pkg-param-value
pkg-param-value = token
cont-param   = "content" EQUAL cont-param-value
cont-param-value = token
enc-param   = "encoding" EQUAL enc-param-value
enc-param-value = token / "hex"
```

The “ISDN” user-to-user information is included in the uui-data element. It is composed of two parts: firstly of a protocol discriminator and secondly of the user information.
The protocol discriminator describes the user information and is specified in table 4-26 of [ITU-T Recommendation Q.931]. It is one octet long.
The length of the user information is assumed to be at most equal to 128 octets.

The procedures for the “ISDN” user-to-user information exchange in SIP shall be compliant with the [RFC7434] with the following clarifications:

- UUI header field shall be present in the initial INVITE request if it is planned to use it in subsequent requests/responses, even when there is no data (except the protocol discriminator octet) to send at that point in time
- Only a single UUI header field can be included in each SIP message
- The “purpose” parameter should be included. Its value shall be equal to “isdn-uui”
- The “content” parameter is optional. If present, it shall be equal to “isdn-uui”
- The “encoding” parameter is optional. If present, it shall be equal to “hex”

An example of a UUI header sent over the SIP interconnection interface is given below:

User-to-User:”04353030303331”;purpose=isdn-uui

# 8 Service access number before translation

Some value-added services (ex: hotline, customer care, Freephone…) are reached dialing a service access number which is not a globally routable number and consequently needs to be translated into a routable SIP or tel URI to process the session establishment.
In order to permit the receiving entity to retrieve the service requested by the calling user, the service access number shall be stored during its translation in the SIP signalling message towards the final destination.

For that purpose, the service access number before translation shall be conveyed in the History-Info header and shall be identified thanks to a History-Info entry containing "cause" SIP URI parameter set to the value "380" as defined in [RFC 8119] which should also contain an "mp" or “rc” header field parameter as defined by [RFC 7044] (i.e. the History-Info entry containing the cause parameter value “380” conveys the service access number after translation and refers to the History-Info entry containing the service access number before translation thanks to “mp” or “rc” parameter if present; otherwise the service access number before translation is contained in the preceding History-Info entry).

The syntax of the History-Info header [RFC 7044] is the following:

```
History-Info   = "History-Info" HCOLON hi-entry *(COMMA hi-entry)
hi-entry                = hi-targeted-to-uri *(SEMI hi-param)
hi-targeted-to-uri      = name-addr
hi-param       = hi-index/hi-target-param/hi-extension
hi-index                = "index" EQUAL index-val
index-val      =  number *("." number)
number                  =  [ %x31-39 *DIGIT ] DIGIT
hi-target-param         = rc-param / mp-param / np-param
rc-param       = "rc" EQUAL index-val
mp-param       = "mp" EQUAL index-val
np-param       = "np" EQUAL index-val
hi-extension   = generic-param
```

The cause-param parameter is a SIP URI parameter and is defined in [RFC 4458].
The cause URI parameter shall be inserted and set to the value "380" in the History-Info entry (URI) of the service access number after translation, as defined in [RFC 8119].

An example of a History-Info header used for service access number before translation and sent over the SIP interconnection interface is given below:

History-Info:
<sip:*ServiceAccessNumber*;user=phone>;index=1,
<sip:*ServiceAccessNumberAfterTranslation*;user=phone;cause=380>;mp=1;index=1.1

# 9 Message bodies

In the context of this document, 2 cases can occur:

- Single body type: the only SIP message body type supported is SDP (application subtype "application/sdp").
- Multi-body type: applicable for NG eCall service related procedure. The "multipart" MIME type is used within the body of the message:
  - SDP (MIME type: "application/sdp")
  - MSD (MIME type: “application/ EmergencyCallData.eCall.MSD”)
  - MSD metadata/control block ((MIME type: “application/EmergencyCallData.Control+xml”)”

# 10 Supported option tags of SIP extensions

In the context of this document:
- the “timer” option tag is authorized if the optional keep-alive mechanism for active SIP sessions as defined in the [RFC4028] is used on bilateral agreement (see §19.1)
- the “histinfo” option tag is authorized for “Service access number before translation” (see §8) and for Call forwarding service when History-Info header is used (see criteria in §17.2).
- When the SIP preconditions are used (see criteria in section 13.1.4.1) and only in this case, the “precondition” and “100rel” option tags shall be supported.

No other option tag is supported in the context of this document.

# 11 Calling number Authentication

## 11.1 Identity header sending in initial INVITE request

When an initial INVITE request is sent at the SIP NNI between 2 national network operators, if one of the following subclauses is satisfied:

FROM header contains a E164 compliant calling TN

OR

FROM header contains the URI « sip:anonymous@anonymous.invalid » or the URI « sip:unavailable@unknown.invalid »
AND
P-Asserted-Id header is present and contains a valid E.164 compliant calling TN

then an Identity header coded in compliance with §11.3 shall be present in this INVITE request.

Note 1: According to the technical rules defined by APNF's "MAN program", calls delivered at the SIP interconnection interface with the absence of Identity header (or with an identity header with an invalid format in the initial INVITE request) may lead to call release, except in some use cases (e.g. voice calls towards French emergency numbers and other calls with authorized bypass of calling number verification procedure, cf. § 11.5) (technical rules are available at [FFTelecoms_MAN]).

Note 2: At the target, in some cases specified in MAN technical rules available at [FFTelecoms_MAN], the initial INVITE request sent at the SIP based interconnection interface may contain several Identity headers.

## 11.2 Identity header reception in initial INVITE request

When an Identity header is contained in initial INVITE request received at the SIP NNI between 2 national network operators, it must be processed according to the technical rules issued at the APNF' MAN WG (documents related to Calling Number Authentication Mechanism are available at the dedicated FFTelecoms' website [FFTelecoms_MAN])

## 11.3 Identity header format and coding

Identity Header contained in the initial INVITE requests sent at the SIP NNI between 2 national network operators MUST comply with the following format:

identity: <json web token>;info=<url certificat>;ppt=shaken;alg=< signing algorithm >

Example of Identity header content:

```
identity: eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwieDV1I \
   joiaHR0cHM6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJ \
   kZXN0Ijp7InVyaSI6WyJzaXA6YWxpY2VAZXhhbXBsZS5jb20iXX0sImlhdC \
   I6IjE0NDMyMDgzNDUiLCJvcmlnIjp7InRuIjoiMTIxNTU1NTEyMTIifX0.r \
   q3pjT1hoRwakEGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjpjlk-cpFYpFYs \
   ojNCpTzO3QfPOlckGaS6hEck7w;info=<https://biloxi.example.org \
   /biloxi.cert>;ppt=shaken;alg=ES256
```

Note 1: if one of the following requirements is not satisfied, then the incoming call is released (except if incoming call is an emergency call):

- Requirement 1: Presence of unencrypted parameters 'info', 'ppt' and 'alg'.
- Requirement 2: Presence of Identity header containing a JWT with 'ppt= shaken'

Note 2: alg=ES256 is an example. Other algorithms may be possible.

## 11.4 Interaction with call forwarding/diversion service

When an initial INVITE request contaning an Identity header coded as explained in §11.3 is forwarded (with insertion of Diversion or History-info header with relevant content) towards FFTélécoms' SIP inter-opertor interface, an additional Identity header resulting of Diversion PASSporT encryption should be sent in this initial INVITE request.
For more information, see the dedicated FFTelecoms' website [FFTelecoms_MAN].

This additional Identity Header MUST comply with the following format:
identity: <json web token>;info=<url certificat2>;ppt=div;alg=<signing algorithm2>

As a conclusion, the initial INVITE will contain 2 Identity headers as follows:
identity: <json web token>;info=<url certificat>;ppt=shaken;alg=< signing algorithm >
identity: <json web token>;info=<url certificat2>;ppt=div;alg=<signing algorithm2>

## 11.5 Disabling of calling number authentication on originating network operator incident

In some specific situations, the calling number authentication cannot be performed by the originating network operator due to an originating network outage.

> Note: analog problems could happen in a call redirecting network for performing redirecting number authentication.

As a result, in these use cases the initial INVITE request sent at the SIP interconnection interface towards downstream network operators shall contain a P-Identity-Bypass header whose content depends on a token provided by APNF (for more information, please refer to relevant APNF's MAN WG documents [FFTelecoms_MAN].

Note: if this SIP request contains an Identity header, this Identity header shall be ignored by downstream network operators.

# 12 Identities format, address parameters and signalling mode

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

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].

| **Supported formats in reception direction (NOTE 1)** | | **Sent formats in transmission direction (NOTE 2)** | |
|---|---|---|---|
| From<br>(for E.164 numbers) | 1. SIP URI like globalnumber@domainname with user=phone<br>2. SIP URI like globalnumber@IP_address with user=phone<br>3. Tel URI in global number format | From<br>(for E.164 numbers) | 1. SIP URI like globalnumber@domainname with user=phone<br>2. SIP URI like globalnumber@IP_address with user=phone<br>3. Tel URI in global number format |
| From<br>(for national short codes)<br>(NOTE 7) | 1.SIP URI in local number format @domainname with user=phone<br>2. SIP URI in local number format @IP_address with user=phone<br>3. Tel URI in local number format | From<br>(for national short codes)<br>(NOTE 7) | 1.SIP URI in local number format @domainname with user=phone<br>2. SIP URI in local number format @IP_address with user=phone<br>3. Tel URI in local number format |
| To<br>(for E.164 subscriber numbers) | 1. SIP URI like globalnumber@domainname with user=phone<br>2. SIP URI like globalnumber@IP_address with user=phone<br>3. Tel URI in global number format | To<br>(for E.164 subscriber numbers) | 1. SIP URI like globalnumber@domainname with user=phone<br>2. SIP URI like globalnumber@IP_address with user=phone<br>3. Tel URI in global number format |
| To<br>(for national short codes) | 1.SIP URI in local number format @domainname with user=phone<br>2. SIP URI in local number format @IP_address with user=phone<br>3. Tel URI in local number format | To<br>(for national short codes) | 1.SIP URI in local number format @domainname with user=phone<br>2. SIP URI in local number format @IP_address with user=phone<br>3. Tel URI in local number format |
| P-Asserted-Identity<br>(for E.164 subscriber numbers) | 1. SIP URI like globalnumber@domainname with user=phone<br>2. SIP URI like globalnumber@IP_address with user=phone<br>3. Tel URI in global number format | P-Asserted-Identity<br>(for E.164 subscriber numbers) | 1. SIP URI like globalnumber@domainname with user=phone<br>2. SIP URI like globalnumber@IP_address with user=phone<br>3. Tel URI in global number format |
| Request-URI<br>(for E.164 subscriber numbers) | 1. SIP URI like globalnumber@domainname with user=phone<br>2. SIP URI like globalnumber@IP_address with user=phone<br>3. Tel URI in global number format | Request-URI<br>(for E.164 subscriber numbers) | 1. SIP URI like globalnumber@domainname with user=phone<br>2. SIP URI like globalnumber@IP_address with user=phone<br>3. Tel URI in global number format |
| Request-URI<br>(for national short codes) | 1. SIP URI in local number format @domainname with user=phone<br>2. SIP URI in local number format @IP_address with user=phone<br>3. Tel URI in local number format | Request-URI<br>(for national short codes) | 1. SIP URI in local number format @domainname with user=phone<br>2. SIP URI in local number format @IP_address with user=phone<br>3. Tel URI in local number format |
| Diversion<br>(for E.164 subscriber numbers) | 1. SIP URI like globalnumber@domainname with user=phone<br>2. SIP URI like globalnumber@IP_address with user=phone<br>3. Tel URI in global number format | Diversion<br>(for E.164 subscriber numbers) | 1. SIP URI like globalnumber@domainname with user=phone<br>2. SIP URI like globalnumber@IP_address with user=phone<br>3. Tel URI in global number format |

| Supported formats in reception direction (NOTE 1) | | Sent formats in transmission direction (NOTE 2) | |
|---|---|---|---|
| History-Info (for E.164 subscriber numbers) | 1. SIP URI like globalnumber@domainname with user=phone<br>2. SIP URI like globalnumber@IP_address with user=phone<br>(NOTE 4) | History-Info (for E.164 subscriber numbers) | 1. SIP URI like globalnumber@domainname with user=phone<br>2. SIP URI like globalnumber@IP_address with user=phone<br>(NOTE 4) |
| Via | IP address / port | Via | IP address / port |
| Route | SIP URI (NOTE 3) | Route | SIP URI (NOTE 3) |
| Contact | SIP URI (NOTE 3) | Contact | SIP URI (NOTE 3) |
| NOTE 1 – In the receiving direction, when several formats are listed (e.g. 1. 2. 3…), this means that all formats must be supported.<br><br>NOTE 2 – In the sending direction, when several formats are listed, this means that at least one format of the list must be supported.<br><br>NOTE 3 – The use of a FQDN instead of an IP address must be agreed between both connecting parties beforehand.<br><br>NOTE 4 – Used URI scheme shall be SIP URI. The "cause" URI parameter cannot be added if hi-targeted-to-uri is a Tel URI. | | | |

***Table 21: Supported format identities***

Moreover, the following principles shall be taken into consideration:

- Global-number format shall be used for subscriber numbers (for E.164 subscriber numbers and M2M numbers) as described in [RFC3966]. In case of M2M services, the national significant number portion of the global number may belong to the French number range for M2M applications. In the French dialling plan, such numbers begin with 0700 and have an extended length: 13-digit NSNs for Metropolitan France and 12-digit NSNs for a DROM.
  In addition, global-number format can be used for transporting E164 value-added service numbers (contained in Req-URI or From header). However, this number shall not belong to forbidden national value-added-service number ranges such as +3389BPQ.
  In Global-number format, the "+" is mandatory in front of the number as described in [RFC3966]

- Local-number format, as described in [RFC3966], shall be used for national short codes (French specific non E.164 numbers: 1X, 1XY, 10YT, 118XYZ, 116XYZ, 3BPQ) whether for Metropolitan or DROM destination (or origin, see Note 7), the phone-context parameter is set to +33. For example, 3610 short code will be conveyed in Request-URI (or From header) as tel:3610;phone-context=+33 or sip:3610;phone-context=+33@domainname;user=phone.

- The telephone number must contain only digits.

- End-to-end delivery of a national short code contained in the From header received over the SIP interconnection interface is not guaranteed. For instance, this information could be modified due to protocol interworkings (e.g. SIP to ISUP interworkings) before presentation to called user.

- End-to-end delivery of a From header's display-name parameter received at the SIP interconnection interface is not guaranteed.

- Request-URI identity and To header contain information related to the called party number. From and P-Asserted-Identity headers contain information related to the calling party number, The Diversion / History info header contains information related to the diverting party number. Those identities are always in the form of a E.164 number, except for Request-URI, To and From headers in case of national short code transport (see the previous relevant bullet).

  - When they belong to the French numbering range, the E.164 numbers shall comply with one of the following formats:
    - +CCZABPQMCDU or,
    - +CC(number portability prefix)ZABPQMCDU (Request-URI identity and To header only (cf. Note 8)), with
      - CC is "33" or the country code allocated to a DROM depending on the value of the ZAB(P) except for VAS services (Z=8); In case of Z=8, CC=33 for Metropolitan and DROM destinations, and
      - (number portability prefix) is a number portability prefix as defined by the French regulation authority or,
    - o +CC("ZONE BLANCHE prefix")$N_1N_2…N_n$ (Request-URI identity and To header only), with
      - CC is "33", and
      - ("ZONE BLANCHE prefix") is a prefix in a 600xyz format as defined by the French regulation authority (e.g. 600794 for a national call from Bouygues Telecom network to SFR Network) with x = destination network, y = originating network, z = call type (MOC), and
      - $N_1N_2…N_n$ is a National Significant Number (as defined in ITU-T Recommendation E.164).

    or only for M2M applications:
    - +33700PQMCDUEFGH for Metropolitan France where 700PQMCDUEFGH is a National Significant Number (as defined in ITU-T Recommendation E.164), or
    - +CC700PQMCDUEFG, with CC is the country code allocated to a DROM (e.g. 262) where 700PQMCDUEFG is a National Significant Number (as defined in ITU-T Recommendation E.164), with
      - The value of P determines the value of CC as detailed in the Annex 2 ("Numéros mobiles de longueur étendue (ZAB = 700)") of the ARCEP decision n° 2012-085 17/07/12 "relative à la réorganisation des tranches de numéros commençant par 06 et 07".

  - When they do not belong to the French numbering range, i.e. correspond to international numbers ("foreign"), the E.164 numbers shall comply with the following format:
    - +CC$N_1N_2…N_n$ , with
      - CC is the country code allocated to the relevant country,
      - $N_1N_2$… Nn is a National Significant Number (as defined in ITU-T Recommendation E.164).

  - The Unavailable User Identity (« sip:unavailable@unknown.invalid »), as defined in the standard 3GPP TS 23.003 §13.7, shall be used (NOTE 5) in the From header exchanged over the SIP interconnection interface for the following use cases, and only for them:

- Unavailability of a valid telephone number identifying the calling party
- Calls crossing international boundaries without bilateral agreement on CLI information delivery
- 2G or 3G handset mobile access originating calls when the CLIR service is invoked
- Fixed analogic access originating calls when the CLIR service is invoked.

NOTE 5: For backward compatibility reasons, when using an interworking equipment implementing 3GPP release inferior to 12, the Anonymous User Identity (« sip:anonymous@anonymous.invalid »), as defined in the standard 3GPP TS 23.003 §13.6, may be used according to bilateral agreement in the From header exchanged over the SIP interconnection interface for the following use cases, and only for them:
- mobile access originating calls when the CLIR service is invoked
- Fixed analogic access originating calls when the CLIR service is invoked.

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.

NOTE 6: Identities sent over the national inter-operator interconnection interface may exceed 15 digits (max. length authorized by E.164). Nevertheless, they shall remain compliant with the ARCEP's national policies defining the structure of the French numbering plan.

NOTE 7: the national short codes that can be used in From header are defined in French numbering plan managed by ARCEP (examples: authorized 3BPQ (like 30PQ, 31PQ)).
Furthermore, if an initial INVITE request is sent at the SIP interconnection interface with a national short code in the From header, it shall contain:

- a P-Asserted-Id header coded with a valid French fixed E164 number associated to the calling line,
- a Request-URI coded with a valid French destination number belonging to national numbering plan (other destination numbers are unexpected).

NOTE 8: To header can contain a French E.164 prefixed number if and only if Request URI contains the same prefixed called number.

## 12.1 ISDN access

In case of a calling user behind an ISDN access where the "Special arrangement" applies (as defined in ETS 300−089) two calling party numbers must be conveyed by the network signalling. One is asserted by the network, originating from the network (NDI, Numéro de Désignation de l'Installation). The other one is provided by the user, originating from the user provided unscreened ISDN "Calling Party Number" information element (NDS, Numéro de Désignation Supplémentaire).

Therefore, at the downstream SIP interconnection interface, the value of the SIP "P-Asserted Identity" header field will have to equal to the value of the calling party identity asserted by the network. The value of the SIP "From" header field will have to equal to the calling party identity provided by the user.

# 13 Media session management

SDP offer/answer exchange shall be performed according to [RFC3261], [RFC3264] and [RFC4566], with the clarifications given in [RFC6337].
When the SIP preconditions are used (see criteria in section 13.1.4.1) and only in this case, SDP offer/answer exchange according to |RFC3312], [RFC4032], [RFC3262] and to [RFC3311] are supported.

When the SIP preconditions are used (see criteria in section 13.1.4.1) and only in this case, SDP information is also supported in the body of PRACK and UPDATE messages and their associated 200 OK responses.
Otherwise, 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 [RFC3264] shall be supported.

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

## 13.1 Media session establishment

### 13.1.1 Initial INVITE message

This section assumes offer/answer rules based on [RFC3261] and [RFC3264] are respected.

When the SIP preconditions are used (see criteria section 13.1.4.1) and only in this case, additional offer/answer rules defined in |RFC3312], [RFC4032], [RFC3262] and [RFC3311] are supported.

Initial INVITE messages shall contain an SDP offer with at least a media stream "m=audio" that at least contains G.711 codec.

NOTE:
- If several “m=” lines are present in the SDP offer sent at the SIP NNI, it is highly recommended that the “m=audio” line is ranked at the first place of this list.
  - Remark: some called SIP user equipment may reject incoming call if this principle is not respected.
- If an initial INVITE is received at the SIP NNI with only a media stream “m=text”, then this request shall be rejected.
- If an initial INVITE message does not contain an SDP offer, then backward early-media (towards the origin of the call) is not possible (cf. §13.1.3).

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

When the SIP preconditions are used (see criteria in section 13.1.4.1) and only in this case, the SDP offer/answer exchange is described in section 13.1.4.2. Otherwise:
- The initial INVITE contains an SDP offer and the SDP answer shall be present in the 200 OK response. The SDP direction attribute of these SDP offer and SDP answer shall be set to “sendrecv” or omitted (no direction attribute).

### 13.1.2 Codec negotiation rules

If several “m=” lines are present in a SDP body sent at the SIP NNI, it is highly recommended that the “m=audio” line is ranked at the first place of this list.
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 13.2).

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~~ packetization times for codecs are described in section 14.

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

- an initial INVITE or re-INVITE (or PRACK or UPDATE when the SIP preconditions are used (see criteria in section 13.1.4.1) and only in this case), it shall be rejected by a 488 "Not acceptable here" response;
- a 200 OK response to the INVITE message, the call shall be released.
  *Editor's note: when the SIP preconditions are used, initial INVITE requests shall contain an SDP offer, so the possibility to get the SDP offer in reliable 18x response is therefore not added here.*

### 13.1.3 Early media

The reception of a SDP answer in a 18x response is not a sufficient indication of an early media coming from a downstream domain. The P-Early-Media header must be included to guarantee an early media stream sent in the backward direction (towards the origin) or in the backward & forward directions will be taken into account in all cases. For early-media scenarios, the P-Early-Media header present in a 18x response must contain the direction parameter set to "sendrecv" or to "sendonly". The P-Early-Media header syntax is defined in [RFC5009] and [TS 24.628].

The supported direction parameters are: "sendrecv", "sendonly", "inactive". "recvonly" is not supported.
When "gated" is present (after all other direction parameters, in last position), it means that gating procedures have occurred downstream according to the direction parameter(s) and that it is consequently not useful to perform gating procedures upstream.

The P-Early-Media header with the "supported" parameter may be present in initial INVITE requests (cf. [RFC5009] section 6).

The P-Early-Media header should be present in the first provisional response containing SDP. If the P-Early-Media header is not present in a provisional response and no previous early media authorization has been received within the dialog, the associated early-media stream may be not taken into account in all cases.

If a P-Early-Media header has previously been received within a dialog and a subsequent provisional response does not contain any P-Early-Media, the previous early media authorisation is still valid (cf. [RFC5009] section 8).

Once the dialog is established (i.e. reception of the 200 OK), only the SDP direction attribute applies.

### 13.1.4 SIP preconditions

#### *13.1.4.1 Support of the SIP preconditions over the SIP interconnection interface*

For calls between 2 national mobile network operators, the use of the SIP preconditions is **mandatory** over the SIP interconnection interface and shall follow the following rules:

- The SIP preconditions shall be proposed in initial INVITE request over the SIP interconnection interface (i.e. the preconditions shall be indicated as supported in the initial INVITE request).
- And the SIP preconditions shall be present in response(s) to INVITE (with SDP) over the SIP interconnection interface (i.e. the preconditions shall be indicated as required in 183 Session Progress (SDP) response(s) to INVITE).

Their implementation shall comply with section 13.1.4.2.

For calls between 2 national fixed network operators and for calls between a national mobile network operator and a national fixed network operator, the SIP preconditions **are not authorized** (i.e. shall not be proposed in initial INVITE request) over the SIP interconnection interface.

| **Use of the SIP Preconditions over the SIP interconnection interface** | | |
|---|---|---|
| Calls from / to-: | To national **mobile** network operator | To national **fixed** network operator |
| From national **mobile** network operator | **mandatory** | **not authorized (*)** |
| From national **fixed** network operator | **not authorized (*)** | **not authorized (*)** |

***Table 22: Use of the SIP Preconditions over the SIP interconnection interface***

(*): means that the SIP preconditions shall not be proposed in initial INVITE request over the SIP interconnection interface.

Note 1: “mobile” encompasses mobile circuit-switched, VoLTE under 4G or 2G/3G coverage, VoWifi.

Note 2: in case of calls between a national mobile network operator and a national fixed network operator, the national mobile network operator should perform some procedures in its network operator to handle asymmetrically the preconditions. In particular for calls from mobile to fixed, the national mobile network operator should defer sending the initial INVITE request to fixed network until resources are reserved in mobile network, in order to guaranty service quality.

*Editor’s note: ISUP/SIP 29.163 §7.2.3.2.1.2 (MGCF should defer sending the INVITE request until receiving a COT message)*

#### *13.1.4.2 SIP preconditions mechanisms and SDP attributes*

All this section applies when the SIP preconditions are used (see criteria in section 13.1.4.1) and only in this case.

The handling of SIP preconditions shall follow [RFC3312] (updated by [RFC4032]) (only segmented status type is supported) and 3GPP [TS 24.229]. The following clarifications apply:

**The preconditions shall be proposed in the initial INVITE sent over the SIP interconnection interface as follows:**

- The ‘100rel’ and ‘precondition’ option tags shall be present in the Supported header (not in the Require header, cf. 3GPP [TS 24.229] section 5.1.3.1).
- An SDP offer shall be present in the initial INVITE (cf. 3GPP [TS 24.229] section 6.1.2).
- In this SDP offer,
    - the SDP direction attribute is recommended to be set to “sendrecv” or omitted (cf. Note).

      Note: although GSMA IR.92 v9 specification mandates the use of “a=sendrecv” in initial INVITE, some VoLTE UE from some suppliers are still not compliant with the standard on this topic and still send “a=inactive” (that was previously mandated). The default behaviour is to use “a=sendrecv” in initial INVITE. “a=inactive” is used only by exception at short term, only for mobile to mobile calls and in a transition phase. At the target, the use of “a=sendrecv” in initial INVITE is the required behavior for all types of calls, but if possible it should be used right now,
    - the SDP preconditions attributes shall be present and set as defined in [RFC3312] and 3GPP [TS 24.229] §6.1.2 (in particular, the local preconditions for QoS are indicated as met or not met, the remote preconditions for QoS are indicated as not met, the strength-tag value for the local segment is set to "mandatory", the strength-tag value for the remote segment is set to "optional", confirmation for the result of the resource reservation shall not be requested).

An example of SDP preconditions attributes in SDP offer of initial INVITE request sent over the SIP interconnection interface is given below:

*curr:qos local none*
*curr:qos remote none*
*des:qos mandatory local sendrecv*
*des:qos optional remote sendrecv*

**The preconditions shall be present in response(s) (with SDP) to INVITE over the SIP interconnection interface as follows:**

- The '100rel' and 'precondition' option tags shall be present in Require header in 183 Session Progress response(s) with SDP.
- In the SDP answer of 183 Session Progress response(s),
    - if the initial INVITE contains "a=sendrecv" or no direction attribute in the SDP offer, the SDP direction attribute is recommended to be set to "sendrecv" or omitted in the SDP answer, regardless of the resource reservation status.
    - the SDP precondition attributes shall be present and set as defined in [RFC3312] and 3GPP [TS 24.229] §6.1.3 (in particular, confirmation for the result of the resource reservation shall be requested if the remote preconditions were indicated as not met).

An example of SDP preconditions attributes in SDP answer of 183 Session Progress sent over the SIP interconnection interface is given below:

*curr:qos local none*
*curr:qos remote none*
*des:qos mandatory local sendrecv*
*des:qos mandatory remote sendrecv*
*conf:qos remote sendrecv*

**Then:**

- If confirmation for the result of the resource reservation was requested by the called side, the successful resource reservation shall be confirmed within the next SIP UPDATE (or PRACK) request.
- The 'precondition' option tag shall be present in Require header in subsequent in-dialog requests including SDP (e.g. UPDATE) and their related responses including SDP during call establishment.
- As defined in [RFC4032] §4, the reception of a 180 Ringing means implicitly that preconditions are fulfilled. The explicit confirmation of resource reservation by the called side (e.g. using UPDATE) is facultative.
- The 200 OK response to INVITE request shall not contain any SDP answer. If a SDP is contained, it must be ignored by the receiving party.
- After call establishment, the 'precondition' option tag may be present in re-INVITE in Supported header.

## 13.2 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].

## 13.3 Terminating a session

The procedures used to terminate a session are described in [RFC3261], with the following precision: When the calling party side wishes to terminate the session during the early-dialog phase it is recommended to use the CANCEL method instead of the BYE method (cf. §4.2.7).

## 13.4 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 MUST 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.

# 14 Voice codecs

The list of the supported codecs and their usage rules are described in [ArchitectureV3.1_FFT] section "Codecs à bande étroite" and section "Codecs à large bande".

# 15 DTMF transport

DTMF transport shall be used in accordance with the rules described in [ArchitectureV3.1_FFT]. More precisely:

**For Human to Machine**, the “telephone-event” [RFC 4733] must be used for DTMF transport. For this purpose, the support of "telephone-event" must be indicated during the SDP offer/answer exchange and used in accordance with rules described in [[ArchitectureV3.1_FFT] §4.2.2.4 “Telephone-event”. If received at interconnection interface, on reception of an SDP offer or answer containing “telephone-event” pseudo-codec, the “telephone-event” pseudo-codec in the m= line shall be transmitted over the interconnection interface. The SDP offer and the SDP answer must contain “telephone-event” over the interconnection interface.

**For Machine to Machine (M2M), and only in this case**, DTMF transport can be done either using “telephone-event” mode or in G.711 in-band when “telephone-event” mode is not suitable for some special usages (non-voice usages). In this last case, this enables to avoid transcoding from in-band DTMF tones to “telephone-event” and so fulfills the need of DTMF transport transparency for some critical M2M existing specific usages still performed by user equipment or central site servers such as Telealarm or Telemonitoring.
To transport DTMF in G.711 in-band for M2M communications between endpoints, the SDP offer must contain G.711 and may or may not contain “telephone-event”, and the SDP answer must contain G.711 over the interconnection interface and must not contain “telephone-event”.
In order to avoid dysfunctions, G.711 RTP flows shall be transparently transmitted end to end, from caller to called party, meaning without transcoding nor transrating. In particular, on reception of an SDP offer or answer containing G.711 codec at NNI, the G.711 codec in the m= line shall be transmitted over the interconnection interface without modification (it shall not be deleted neither moved in the codecs list). Moreover, the DTMF transport in G.711 in-band shall not be extracted/regenerated and shall not be interworked to “telephone-event” mode. It is also assumed that no interworking from G.711 in-band to “telephone-event” mode nor transcoding nor transrating is applied inside each operator’s network.
Attention should be paid that in-band DTMF is only applicable for sessions using the G.711 codecs. Moreover, when G.711 in-band DTMF is used, some telephony service features are not guaranteed.

**General recommendations:**
Only one technical solution for DTMF transport shall be used at the same time (either “telephone-event” or G.711 in-band). As a result, the DTMF signals shall not be sent encoded in audio packets using simultaneously “telephone-event” and G.711 in-band (in order to avoid interoperability issues on reception of DTMF signals duplicated in different formats).
Once the session is established, it is not possible to change of DTMF transport mode without re-negotiation.
By default the interconnection equipment shall be transparent to the SDP offer/answer negotiation, in particular for DTMF transport.
The transport of DTMF out-of-band (i.e. using SIP INFO) is forbidden in the context of this document.

*Editor’s note: this section may evolve according to the results of the inter-operator tests to be held on DTMF transport for M2M.*

# 16 FAX Modem

Fax modem calls are supported by default by using the G.711 codec (see [ [ArchitectureV3.0_FFT section “Codecs à bande étroite” for its usage rules) without media session modification.

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

In addition, T38 mode may be used when bilaterally agreed.
V.152 is optional.

However, there is no guaranty of end-to-end interoperability because it depends on customer devices, which is beyond the control of the operator.

# 17 Data Modem

Data modem calls are supported by using the G.711 codec (see [ArchitectureV3.1_FFT section “Codecs à bande étroite” for its usage rules) without media session modification.

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

V.152 is optional.

However, there is no guaranty of end-to-end interoperability because it depends on customer devices, which is beyond the control of the operator.

# 18 Supplementary services

## 18.1 CLIP/CLIR (OIP/OIR)

**Rule n°1:** At the SIP signalling interface between 2 network operators, the "P-Asserted-Identity" header must be present in the initial INVITE request (except in some cases, see Note 1) with a telephone number corresponding to the calling party, provided (or verified) by the originating network operator serving the calling party and expressed in a **valid global-number format** (see section 12, Table 19). For a call that is generated from a national network operator, the P-Asserted-Identity header must be present in the initial INVITE request over the SIP interconnection interface expect in case where relevant calling line number information is not available.

Note 1: In some cases (e.g. calls crossing some international boundaries, calls from some national PSTN accesses, emergency calls from an unregistered mobile calling user), it is accepted that P-Asserted-Identity is absent.

Note 2: If the P-AI header is present in the initial INVITE request sent at the SIP NNI and contains a French fixed E.164 number (e.g. +33ZABPQMCDU with Z=1, 2, 3, 4, 5 or 9), then this phone number must be assigned to a fixed telephony line of the originating French network operator.

**Rule n°2:** The "From" header must be sent with a telephone number identifying the calling party (except in some cases, according to section n°12 and Note 2 below) and expressed in **valid global-number (or local-number) format** (see section 12, Table 19) with a **valid content** (see Note 3). This rule applies even when the CLIR service is requested (see rule n°3). The upstream operator shall not remove a valid telephone number contained in the “From” header in messages sent over the interconnection interface.

Note 3: When the From header contains a French E164 telephone number, it can be:

- The same subscriber number as the one contained in P-Asserted-ID header,
- A subscriber number commercially associated to the calling line but different from the subscriber number contained in the P-Asserted-ID header,
- A subscriber number commercially associated to a different telephone line than the one which is used for the outgoing call (in this case, an agreement must have been established between involved customers on such calling line identifier use),
- A Value-Added Service number.

Note 4: When the From header contains

* a French telephone number whose display on called party handset is forbidden according to
  - national regulation (e.g. +3389BPMCDU, high price 3BPQ number, 118XYZ) or
  - calling telephone number assignee decision (cf. [FFTelecoms_MAN]), or
* a French +CCZABPQMCDU telephone number whose ZABPQ number block has not been allocated by ARCEP to a national operator
* a French E.164 telephone number that can only be used as a call routing number (e.g. +33Z0B’P’Q’ZABPQMCDU) or,
* an abnormal French calling identifier that is not compliant with normal global number format (e.g. +33, +33ZABPQMCDUEF), or not compliant with normal local number fomat (e.g. 000123)

the receiving network operator may reject the incoming call and send a 403 Forbidden SIP response towards the upstream network operator.

Important:

- If both rules n°1 and n°2 are respected, the content of the “From” header is presented to the CLIP subscriber.
- If one of the two rules detailed above is not respected, the provision of CLIP service to the called party is not guaranteed.
- The presentation of “Display-name” field of the “From” header is not guaranteed.

**Rule n°3**: The “Privacy” header is used for the CLIR service. The “Privacy” header is defined in [RFC3323] and shall contain at least the values “Id” and “user” for expressing the CLIR service invocation (except in some cases, see section 12, for which the Anonymous User Identity in the From header may be supported for CLIR service. In that case, a P-Asserted-Id header and a Privacy header shall be present, and the Privacy header shall contain “id” value for P-Asserted-Id’s privacy).

Note 5: The “P-Asserted-Identity” header is restricted with the value “id” defined in [RFC3325] in the “Privacy” header and the “From” header is restricted with the value “user” defined in [RFC3323] in the “Privacy” header.

## 18.2 Call forwarding services

### 18.2.1 Generalities

The expected behavior for the transport of call forwarding information over the SIP interconnection interface is the following:

- For forwarded calls between 2 national mobile network operators: the SIP History-Info header is used for Call forwarding services over the SIP interconnection interface.

- For forwarded calls from a national mobile network operator towards a national fixed network operator: by default, the SIP Diversion header is used for Call forwarding services over the SIP interconnection interface. According to bilateral agreement, the SIP History-Info header can be used instead.

- For forwarded calls between 2 national fixed network operators: by default, the SIP Diversion header is used for Call forwarding services over the SIP interconnection interface. According to bilateral agreement, the SIP History-Info header can be used instead.

- For forwarded calls from a national fixed network operator towards a national mobile network operator:
    - If the national fixed network operator supports to emit the SIP History-Info header for Call forwarding services, it is recommended that the SIP History-Info is emitted rather than the SIP Diversion header for Call forwarding services over the SIP interconnection interface.
    - Otherwise, the SIP Diversion header is used for Call forwarding services over the SIP interconnection interface.

  Therefore the national mobile network operator shall support to receive the SIP History-Info header, as well as the SIP Diversion header.
  The choice between both headers is done once, as written in the bilateral interconnection agreement signed with the national fixed network operator, and is not call by call.

The expected behavior for the transport of call forwarding information over the SIP interconnection interface is summarized below:

| **Header emitted to convey call forwarding information in the initial INVITE request over the SIP interconnection interface** | | |
|---|---|---|
| Forwarded calls from/to: | To national **mobile** network operator | To national **fixed** network operator |
| From national **mobile** network operator | **History-Info** (required) | **Diversion** by default (or History-Info on bilateral agreement) |
| From national **fixed** network operator | If supported by the fixed network operator, **History-Info** use is recommended;<br>Otherwise, **Diversion** is used | **Diversion** by default (or History-Info on bilateral agreement) |

***Table 23: Header emitted to convey call forwarding information over the SIP interconnection interface***

Moreover, the following principles shall be taken into consideration:

– At the target, History-Info header should be used for all types of forwarded calls over the SIP interconnection interface instead of Diversion header.

– In order to avoid any risk of inconsistency (cf. [RFC7544] §2), both Diversion and History-Info headers conveying call forwarding information shall not be present simultaneously in the initial INVITE request.

- If an interworking is performed between Diversion and History-Info headers in an operator's network, it should comply with [RFC7544].

### 18.2.2 Use of the Diversion header

When the Diversion header is used for a Call forwarding service (see §18.2.1), [RFC5806] shall be supported in order to represent call forwarding information.

*Additional information about parameters and values of the "Diversion" header:*

- *Diversion ="Diversion" ":" # (name-addr *( ";" diversion_params ))*
- *diversion-params =diversion-reason | diversion-counter | diversion-limit | diversion- privacy | diversion-screen | diversion-extension ;*
- *diversion-reason = "reason" "=" ( "unknown" | "user-busy" | "no-answer" | "unavailable" | "unconditional" | "time-of-day" | "do-not-disturb" | "deflection" | "follow-me" | "out-of-service" | "away" | token | quoted-string ) ;*

This field is mandatory. Values "unavailable", "time-of-day", "do-not-disturb", "follow-me", "out-of-service" and "away" may be sent over the interconnection interface but need not be taken into account by the recipient.

- *diversion-counter = "counter" "=" 1*2DIGIT ;*

This field is mandatory and its recommended value is '1' for each diversion that occurred as recommended in RFC 5806 (see Note). Otherwise, call delivery and on storage of the diversion data may fail.

*Note 1 – As a result of interworking with older control protocols (e.g. SSUTR2), the counter may be received with a value of "5".*

*Note 2 – The maximum value of the diversion-counter parameter shall be exchanged between the interconnected parties.*

- *diversion-limit = "limit" "=" 1*2DIGIT ;*

This field may be sent over the interconnection interface but needs not be taken into account by the recipient.

- *diversion-privacy = "privacy" "=" ( "full" | "name" | "uri" | "off" | token | quoted-string ) ;*

This field is recommended. The values "name" and "uri" are not supported. If received, they shall be mapped to "full". If the diverting user has a CLIR service activated, then privacy must be set to "full". If not, privacy must be set to "off".

- *diversion-screen = "screen" "=" ( "yes" | "no" | token | quoted-string ) ;*

This field may be sent over the interconnection interface but needs not be taken into account by the recipient.

- *diversion-extension = token ["="(token | quoted-string)] ;*

This field may be sent over the interconnection interface but needs not be taken into account by the recipient.

An example of a Diversion header used for Call forwarding and sent over the SIP interconnection interface is given below:

Diversion:
<sip:*office@example.com*;reason=user-busy;counter=1;privacy=full,
<sip:*bob@example.com*>;reason=unconditional;counter=1

### 18.2.3 Use of the History-Info header

When the History-Info header is used for a Call forwarding service (see §18.2.1), it shall contain a "cause" SIP URI parameter with cause values defined in [RFC4458] and should contain an "mp" header field parameter as defined by [RFC7044] (cf. Note).

Note: At short term, some implementations may not send any "mp" parameter due to the support of the previous version of History-Info header [RFC4244]. At the target, these implementations should evolve and implement History-Info header as specified in [RFC7044], thus it should contain a "mp" parameter. If possible, History-Info header used for a Call forwarding service should contain a "mp" parameter right now.

*Additional information about parameters and values of the History-Info header:*

The syntax of the History-Info header [RFC7044] is the following:

```
History-Info      = "History-Info" HCOLON hi-entry *(COMMA hi-entry)
hi-entry          = hi-targeted-to-uri *(SEMI hi-param)
hi-targeted-to-uri = name-addr
hi-param          = hi-index/hi-target-param/hi-extension
hi-index          = "index" EQUAL index-val
index-val         =  number *("." Number)
number            =  [ %x31-39 *DIGIT ] DIGIT
hi-target-param   = rc-param / mp-param / np-param
rc-param          = "rc" EQUAL index-val
mp-param          = "mp" EQUAL index-val
np-param          = "np" EQUAL index-val
hi-extension      = generic-param
```

For each call forwarding, a hi-entry shall contain a cause URI parameter expressing the diversion reason. This cause URI parameter is defined in [RFC4458].

When used for call forwarding, the following cause URI parameter values apply:

| **Redirecting Reason** | **Value** |
|---|---|
| Unknown/Not available | 404 |
| User busy | 486 |
| No reply | 408 |
| Unconditional | 302 |
| Deflection during alerting | 487 |
| Deflection immediate response | 480 |
| Mobile subscriber not reachable | 503 |

***Table 24: Cause URI values***

The cause-param parameter is a SIP URI parameter and shall be inserted in the History-Info entry (URI) of the diverted-to user in case of call forwarding.

Reason header field:
The Reason header field defined in [RFC3326] should be escaped in the hi-entry of the diverting user when the call diversion is due to a received SIP response. The Reason header field contains a cause parameter set to the true SIP response code received (Status-Code).

Privacy header field:
A Privacy header field as defined in [RFC3323] shall be embedded in hi-entries with the 'history' value defined in [RFC 7044] when the privacy is required for the redirecting identity.

An example of a History-Info header used for Call forwarding and sent over the SIP interconnection interface is given below:

```
History-Info:
    <sip:bob@example.com>;index=1,
    <sip:office@example.com;cause=302?Privacy=history>;index=1.1;mp=1,
    <sip:home@example.com;cause=486>;index=1.1.1;mp=1.1
```

### 18.2.4 Limitation of the number of diversions and loop issue

Based on bilateral agreement, each network operator shall mention for the interconnection interface the value of its internal limitation on the number of communication diversions allowed, as described in 3GPP [TS24.604] §4.5.2.6.1. If no agreement is found, the counter shall be set to 5 by default.

NOTE – The default value "5" is given provided that the resulting Post Dial Delay fulfills the QoS requirements.

An anti-loop mechanism shall be used to avoid loops between the two interconnected networks, e.g. having in each network a limitation procedure when the internal threshold is reached.

- When the Diversion header is used for call forwarding service, the Diversion-counter, enabling to count the number of communication diversions, shall be sent with reliable information."

- When the History-Info header is used for call forwarding service, the number of entries containing a “cause” SIP URI parameter with a cause value as listed in [RFC4458] enabling to count the number of communication diversions, shall be sent with reliable information.

Reminder, forwarding of an emergency call is forbidden (Decision ARCEP n° 2010-1233, 14 décembre 2010). Therefore, emergency calls delivered to the SIP interconnection interface cannot be marked as having already been diverted.

## 18.3 Call Hold

The Call Hold shall be provided according to the following principles:

- The service is possible only after the dialog is confirmed, i.e. after the 200 OK response to the initial INVITE;
- The mechanism described in [RFC 3264], section 8.4, using the direction attribute (“a=”) in an updated SDP to request the other party to stop sending media, may be used;
- The mechanism described in [RFC 2543], section B.5, using a connection address (“c=”) equal to 0.0.0.0. in an updated SDP to put on hold a call, may be used;

The mechanism described in [RFC 3264], section 8.4 is preferred.

## 18.4 Call Waiting (CW)

For CW service, a 180 ‘Ringing’ response is sent over the SIP interconnection interface. An Alert-Info header set to “urn:alert:service:call-waiting” may be sent in this 180 response.

## 18.5 Incoming Call Barring (ICB)

For ICB service, a 603 ‘Decline’ response is sent over the SIP interconnection interface (or optionally a 480 ‘Temporary Unavailable’ if interworking with TDM networks has occurred).
An early media announcement (as described in §13.1.3) may be provided prior to generating this SIP response.

## 18.6 Anonymous Call rejection (ACR)

When ACR service is invoked on called party side, a 433 ‘Anonymity Disallowed’ response is sent over the SIP interconnection interface.

An early media announcement (as described in §12.1.3) may be provided prior to generating this SIP response.

## 18.7 Conference (CONF)

For CONF service, INVITE and re-INVITE requests (as described in §4.3.4 and §4.3.5) are used over the SIP interconnection interface,
The Referred-By header (as defined in [RFC3892]) may be sent in the INVITE request inviting a user to join the conference bridge.
The “isfocus” feature parameter (as defined in the [RFC3840]) may be indicated in the Contact header of the (re-)INVITE requests. When “isfocus” is present then the Contact header shall remain unchanged so the TAS hosting the conference can be identified in the 200OK response.

# 19 Keep alive

## 19.1 Keep alive for active SIP sessions

A keep-alive mechanism shall be used to check that communications are still active. It can be performed either by sending periodic OPTIONS messages or as defined in [RFC4028]. 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 is 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 [RFC 3261].

## 19.2 Keep alive for interconnection signalling links

A keep-alive mechanism shall be used to monitor the general status of the signalling links between connecting equipments.
A similar keep alive mechanism to the sending of periodic OPTIONS messages, as previously described**,** 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.

# 20 Ring-back tone

It is up to the calling side to generate a local ring-back tone upon receipt of a 180 “Ringing” answer to an INVITE message. Nevertheless, the calling party side need to be prepared to receive ring-back tone delivered as early-media (i.e. using the voice codec and as described in §13.1.3) over the interconnection interface by the called party side.

# 21 Emergency calls towards national PSAP

To be completed.
National policy on resource reservation = to be accurately defined by CCED.

## 21.1 P-AI header in the INVITE request sent towards the network operator hosting called PSAP

### 21.1.1 Emergency calls from a fixed user

For an emergency call from a fixed user, the P-Asserted-Id header in the INVITE request sent towards the network operator hosing the called PSAP shall contain the national E.164 phone number identifying the calling user or calling user installation.

### 21.1.2 Emergency call from a mobile user

For an emergency call from a mobile user located in France, the P-Asserted-Id header in the INVITE request sent towards the network operator NO2 hosting the called PSAP shall contain the E.164 phone number identifying the calling mobile user.

When the From header of the INVITE request sent towards NO2 contains the URI “sip:anonymous@anonymous.invalid”, the P-AI header of this method should contain:
- an MSISDN when the calling user’s telephone number is known or
- another E.164 number when the calling user’s telephone number is unknown (see note below).

- Note: this is typically the case when the calling user's telephone number is unknown because the calling user is not registered to the mobile network handling the emergency call. The information contained in P-AI header could help the called PSAP to localize the mobile caller. The content of P-AI will be defined after the agreement with CCED (E.164 phone number identifying for example the access network handling the emergency call or an E.164 number based on IMEI information of calling handset)

# 22 PSAP callback setup

To be completed.
National policy on PSAP callback = to be defined accurately by CCED.

Note: CCED has decided in S2 2024 that a national emergency short number (e.g. 112) could be used as a calling user identifier (in From header of INVITE request) by an authorised PSAP when launching a 'PSAP callback'.

# 23 NG eCall (eCall over IMS)

February 2024 evolution of EU regulation on emergency calls requires the support of NG eCall by 01/01/2025 (at this date, upgraded IVS-embedded vehicles will have the legal possibility to send NG eCalls towards 112 number).

This policy impacts national SIP-based inter-operator voice interconnections for the need to convey eCalls initiated by IVS under 4G/5G radio coverage towards national PSAP supporting NG eCalls.

FFTelecoms' SIP interconnection profile is thus upgraded in this 3.3 version in order to support the transfer of the MSD information according to RFC 8147 and TS 24.229 (Rel. 14 or later).
The following messages are impacted: initial INVITE, 200 OK response to initial INVITE, SIP INFO methods and its responses.

A highlight of these messages for NG eCall service is given below. Please refer to the relevant standard specifications for more details.

## 23.1 Impacts on initial INIVITE

Pre-requisites: the originating mobile network operator shall translate any emergency service URN received from the IVS into a fixed national E.164 telephone number (cf. §12 Identities), and the initial INVITE request sent at the SIP NNI towards a NG eCall PSAP shall contain:
* a Request-URI identity coded with a national fixed E.164 number assigned to the called PSAP
* a To header coded with the same E.164 called number (in order to comply with the Identity header generation/verification conditions (see §12 Identities).

When a national mobile network operator sends an initial INVITE related to an NG eCall attempt towards a national fixed network operator hosting a NG eCall PSAP, this request shall contain:

- an emergency-related Minimum Set of Data (MSD), i.e. a multipart/mixed body containing an "application/EmergencyCallData.eCall.MSD" MIME body part.

To support the MSD body transfer,
- A call-info header is added to mark the message as containing the MSD.
- A Recv-Info header field per [RFC6086] is added to indicate the ability to receive potential INFO requests carrying required data by the called NG eCall PSAP.
- A new value "application/EmergencyCallData.Control+xml" is added to the "Accept" header to indicate the acceptability of the payload by the sender.

As a reminder, on legacy eCall, the MSD should not exceed 140 bytes and is encoded in binary ASN.1 PER.

## 23.2 Impacts on 200 OK response to INVITE

When an NG eCall PSAP acknowledges the MSD received in an initial INVITE request, the 200 OK response sent by the called fixed network operator to the calling mobile network operator contains an "application/EmergencyCallData.Control+xml" MIME body part with an "ack" element containing a "received" attribute set to "true" or "false", and a "ref" attribute set to the Content-ID of the MIME body part containing the MSD sent by the calling UE (cf. RFC 8147).

For this purpose,
- A call-info header is included to indicate that the message body contains a metadata/control block - acknowledging successful receipt of the eCall MSD.
- A Recv-Info header field per [RFC6086] is added to indicate the ability to receive INFO requests carrying required data.
- New values "application/EmergencyCallData.eCall.MSD" and "application/EmergencyCallData.Control+xml" are added to the "Accept" header to indicate the acceptability of the payload by the sender.

Note: when the transfer of the MSD is not acknowledged by the called PSAP, the IVS must fall back to the in-band transfer of the MSD, as in CS domain defined in 3GPP Release 14 TS 26.267.

## 23.3 Impacts on the other SIP responses to INVITE (486, 600 and 603)

According to RFC 8147, the called NG eCall PSAP may reject the initial INVITE containing MSD while indicating that it is aware of the situation by including a metadata/control object acknowledging the MSD and containing "received=true" within a final response such as 486 (Busy Here), 600 (Busy Everywhere) or 603(Decline).

If one of these responses is received by the fixed network operator hosting the called NG eCall PSAP, it shall be transmitted transparently (with the contained metadata/control object) towards the upstream interconnected network operator (e.g. national mobile network operator hosting the IVS, inter-operator transit network operator).

If the originating mobile network operator is interconnected with the called NG eCall PSAP, it can receive one of the above responses and must handle it according to relevant standards.

## 23.4 Impacts on SIP INFO (cf. transfer of an updated MSD procedure)

The NG eCall PSAP may require that the IVS provides an updated MSD because it suspects the state of the vehicle has changed. For this purpose, it sends a SIP INFO requesting MSD to the IVS (see §23.4.1).

The IVS shall then include an updated MSD within a SIP INFO request and send it within the dialog back to the called PSAP (see §23.4.2).

### 23.4.1 SIP INFO requesting MSD sent by NG eCall PSAP towards IVS through the SIP inter-operator NNI

During an established NG eCall, the downstream fixed network operator hosting the called NG eCall PSAP shall support the sending of an INFO request towards the originating mobile network operator containing:

1) an Info-Package header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147;

2) a multipart/mixed body including:
   a) an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147, containing a "request" element with an "action" attribute set to "send-data" and a "datatype" attribute set to "eCall.MSD"; and
   b) a Content-Disposition header field set to "By-Reference" associated with the "application/EmergencyCallData.Control+xml" MIME body part; and

3) a Content-Disposition header field set to "Info-Package" associated with the multipart/mixed body.

This SIP INFO request shall be responded with a relevant 200 OK message. Note that a 200 OK response to a SIP INFO request indicates only that the receiver has successfully received and accepted the SIP INFO request, it says nothing about the acceptability of the payload, which is served by the SIP INFO message in the reverse direction as described in the section below.

### 23.4.2 SIP INFO sent by IVS towards NG eCall PSAP through the SIP inter-operator NNI

To acknowledge the SIP INFO requesting MSD update sent by the NG eCall PSAP as described in the previous section, **2 cases** are possible:

**Case 1** - The IVS sends back a SIP INFO containing an updated MSD when it is able to provide this information. In this case the SIP INFO message contains:

a) an Info-Package header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147;
b) a multipart/mixed body including:
   i) an "application/EmergencyCallData.eCall.MSD" MIME body part as defined in RFC 8147 containing the MSD not exceeding 140 bytes and encoded in binary ASN.1 as specified in CEN EN 15722:2015; and
   ii) a Content-Disposition header field set to "By-Reference" associated with the "application/EmergencyCallData.eCall.MSD" MIME body part; and
c) a Content-Disposition header field set to "Info-Package" associated with the multipart/mixed body.

**Case 2** - If the IVS receives a request to send an MSD but it is unable to do so for any reason, the IVS instead sends a metadata/control object acknowledging the request, containing an element with a "success" parameter set to "false" and a "reason" parameter (and optionally a "details" parameter) indicating why the request could not be accomplished. Such SIP INFO contains:

a) an Info-Package header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147;
b) a multipart/mixed body including:
   i) an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 with an "ack" element containing: - a "ref" attribute set to the Content-ID of the "application/EmergencyCallData.Control+xml" MIME body part in the INFO request received by the UE; and - an "actionResult" child element containing:
      A) an "action" attribute set to "send-data";
      B) a "success" attribute set to "false"; and
      C) a "reason" attribute set to an appropriate value as defined in RFC 8147; and
   ii) a Content-Disposition header field set to "By-Reference" associated with the "application/EmergencyCallData.Control+xml" MIME body part; and
c) a Content-Disposition header field set to "Info-Package" associated with the multipart/mixed body.

In both cases, the SIP INFO shall be responded with a relevant 200 OK message.

# 24 RTT during voice calls between 2 national network operators

## 24.1 Introduction

### 24.1.1 General assumptions

According to EU's 2019/882 directive transposition in French telecommunications law in 2023 and massive use of SIP based interfaces for voice service interconnection between national network operators since T4 2024, "IP interconnection" WG of FFTelecoms decided in T1 2025 to enrich its SIP profile for voice interconnection between national operators.

The main goal is to make possible the use of Real-Time Text (RTT) media flows during voice calls between:
- a user A and a user B, where:
  - A and B are assigned with national telephone numbers, and are hosted by 2 different national network operators.
  - Both A and B are located in France from a geographic point of view.
  - Both A and B use RTT capable handsets.

  Context: user A has launched an enriched voice call with some text towards user B.
- a user A located in France (and using an RTT capable handset) and a national PSAP.
- Context: user A has launched an enriched voice call with some text towards a called PSAP.

### 24.1.2 Focus on redundant text transmission

Redundant text transmission through the inter-operator SIP NNI shall always be possible during voice call setup depending on SDP negotiation result between SIP end-points (cf. § 9.4 Text of TS 26.114 and §4 of RFC 4103).

For instance, if user A's terminal uses '200 % redundancy' for limiting impacts of potential text packets loss, SDP offer of the initial INVITE sent at the SIP NNI can contain:

- m=text 53490 RTP/AVP 100 98
- a=rtpmap:100 red/1000/1
- a=rtpmap:98 t140/1000/1
- a=fmtp:100 98/98/98

where:
- RTP payload type 100 is used for sending text with 200 % redundancy.
- RTP payload type 98 is used for sending text without redundancy.

Depending on user B's handset capabilities (or downstream network behaviour), SDP answer contained in the 200 OK response sent at the SIP NNI will:

- either indicate redundancy is possible (payload type 100 is selected)
- or indicate redundancy is not possible (payload type 98 is selected)

## 24.2 RTT for voice calls between 2 national NOs

### 24.2.1 Direct interconnection between 2 national NOs

When an INVITE request is sent at the SIP NNI by the originating NO O1 towards NO O2, a SDP body shall be present in this SIP request and contain at least the following codecs:

- G.711 audio codec
- T.140 text codec

### 24.2.2 Indirect interconnection between 2 national NOs

If an intermediate network operator O3 is used between 2 national NOs (for instance, in order to convey inter-operator transit voice calls), O3 should be transparent to:

- text codec present in SDP body of SIP messages received at the SIP NNI
- text media flows exchanged at RTP level between NOs.

## 24.3 RTT for voice calls from a national NO towards a national fixed NO hosting a national PSAP

When an INVITE request is sent at the SIP NNI by the originating NO towards the adjacent downstream fixed NO, a SDP body shall be present in this SIP request and contain at least the following codecs:

- G.711 audio codec
- T.140 text codec

# ~~24~~25 Differences with 3GPP/TISPAN standards (informative)

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

- According to 3GPP TS 24.604, IMS call forwarding services are implemented based on the History-Info header. However, in order to cope with currently available implementations in the market, the services can be rendered by other means in the context of this document (Cf. Diversion header). This impacts the headers transiting at the NNI. The use of either History-Info or Diversion header for Call forwarding service is detailed in section 18.2.

# ~~25~~26 Codecs and transcoding guidelines (informative)

Content of this section is moved to the annex of [ArchitectureV3.1_FFT] document.

# ~~26~~27 Work plan for the next versions (informative)

This section describes areas or candidate features considered for further study and that will be addressed in the next versions of this specification. This section is informative only.

The following work items have been identified:

- Additional impacts of Calling number verification using signature verification and attestation information (ppt=rph, …) in relation with studies driven by MAN workforce,
- Interaction of VoLTE roaming with the SIP information used at SIP NNI to indicate incoming call has an international origin (cf. §6).
- P-AI header content and semantic for an emergency call from a mobile user with unknown calling line identity (cf. §21)
- ECT service,
- Additional impacts of emergency calls handling
    - SIP header RP,
- PSAP Callback,
- ~~"C1…C5" coding in OSGI parameter of PANI header when the geographic location information related to calling party is not available,~~
- SIP format for SPIROU's "Calling Party Category" parameter information,
- QoS related subject,
- DTMF for M2M to be clarified.

# ~~27~~28 History

| History of the present document | | |
|---|---|---|
| V0.1 | 11/12/2009 | Document creation |
| V0.2 | 13/01/2010 | Modifications following the 11/01/2010 meeting |
| V0.3 | 10/03/2010 | Modifications proposed by France Télécom |
| V0.4 | 16/03/2010 | Modifications following the 15/03/2010 meeting |
| V0.5 | 22/03/2010 | Modifications following SFR comments and FT updates |
| V0.6 | 28/04/2010 | Modifications following the 12/04/2010 meeting |
| V0.7 | 04/06/2010 | Modifications following the 04/06/2010 meeting |
| **V1.0** | **06/2010** | **Approved public version** |
| V1.0.1 | 10/09/2012 | Document input to FFT meeting of 10/09/12 |
| V1.0.2 | 17/09/2012 | Modifications following the 10/09/2012 meeting and modifications proposed by France Télécom |
| V1.0.9 | 02/10/2012 | Modifications following the 01/10/2012 meeting. Version sent to consultation to the FFT member |
| V1.0.9 | 04/12/12 | Modification of §8.1.3 following ALU comments and the 03/12/2012 meeting |
| **V1.1** | **14/12/12** | **Approved public version** |
| V1.1.1 | 15/04/13 | Modifications following the 15/04/13 meeting: addition of international calls and short codes. |
| V1.1.2 | 10/06/13 | Modifications following the 10/06/13 meeting: addition of M2M calls, addition of explanations addition of a note on the banning of diverting emergency calls. |
| V1.1.3 | 15/07/13 | Modifications following the 15/07/13 meeting: modification of the Keep-alive mechanism §14 to cla status, modification of the requirement on the SIP header compact form §14, modification of §9, to take into account the new version of the Architecture document yet covering all codec aspect. |
| V1.1.4 | 16/09/13 | Modifications following the 3GPP CT3#74 (05-09/08/13) meeting and the FFT 16/09/13 meetir Unavailable User Identity in §13.1 (CLIP/CLIR) following the acceptance of the Orange Cha 131201. |
| V1.1.5 | 04/10/13 | Version sent to consultation to the FFT members and vendors. |
| V1.1.6 | 29/11/13 | Modification following the phone meeting of 29/11/13: §3 and §18 following ALU comments, comments. |
| **V1.2** | **16/12/13** | **Approved public version.** |
| V1.2.1 | 20/01/15 | Addition of §5 “Calling party’s location information for calls towards Value Added Services (VA header field and §6 “User To User Information” on the UUI header field. |
| **V2.0** | 02/02/15 | Rewording and modification of §9 for specification of the called party numbers in “Zone blanche **Approved public version.** |
| **V2.0.1** | 23/06/16 | §5 “Calling party’s location information for calls towards Value Added Services (VAS)“ correction read GSTN instead of GTSN as access-type in the P-Access-Network-Info header given as exar **Public version (minor update)**. |
| V2.0.1.1 | 23/06/16 | - In §9, new rule for VAS number, the code country (Global number with Z=8) and the phone number) shall be equal to (+)33 whatever the destination metropolitan or DOM.<br>- In §4.5, no more fixed value for the maximum size of the SIP messages and the SDP bodies l if no agreement can be found by bilateral agreement.<br>- In §5, a precision in case of improperly formatted or invalid location information.<br>- In §15.1, removal of Note 2 from CLIP/CLIR and inclusion into §9. |
| V2.0.1.2 | 01/09/16 | Remarks from FFT meeting of 28/07/2016 taken into account + clarifications in §3, §4.5, §5 and |
| V2.0.1.3 | 04/05/17 | Updates to take into account VAS needs in SIP:<br>- Use of History-Info for conveying in SIP the “service access number before translation” in § §7 (new section), §9, §10.<br>- Forward & backward early-media in §1.1 and §11.1.3 (already allowed in the document).<br>In addition, the following modifications are brought:<br>- In §10, addition of Note 5 allowing the use of “Anonymous” in From header in some specific c them on bilateral agreement.<br>- In §2 and in §4.3.4.4, addition of a reference to RFC 6432 for conveying Q.850 error codes in INVITE responses (already allowed in the document).<br>- Some editorial changes are also made in the document. |
| V2.0.1.4 | 29/05/17 | In §11.1.3, rewording to indicate that early-media is in backward or in the backward & forward di meeting of 29/05/2017. |
| V2.0.1.5 | 24/07/17 | In §7, addition of a precision concerning the transport of the service access number before transla but not in the entry containing the cause “380”). |
| V2.0.1.6 | 05/09/17 | - In order to take into account VAS needs in SIP, addition of a new section §6 to define in SIP a call has an international origin using specific coding of P-Access-Network-Info header, mer §4.3.4.2, addition of concerned RFC in §2, update of work plan in §22 and addition of a fig Indication of a call with international origin In §6 and §4.3.4.2, addition of the indicatio national/international to take into account VAS needs in SIP. |

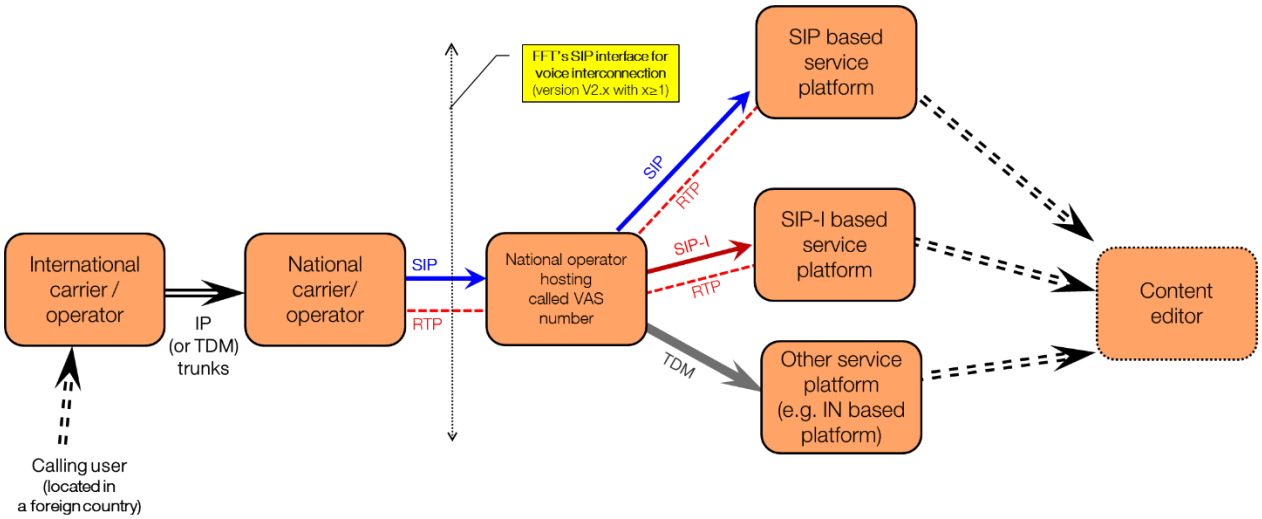
| | | |
|---|---|---|
| | | - In §7, rewording of a precision concerning the transport of the service access number b following FFT meeting of 24/07/2017.<br>- In §10, addition of ";user=phone" that was missing in an example of a call to 3610 short code |
| V2.0.1.7 | 15/09/17 | In §6, modifications on the indication that a call has an international origin, following FFT meetir and of 11/09/2017.<br>Version sent to consultation. |
| V2.0.1.8 | 17/10/17 | In §14 and in §1.1, modifications to take into account the request of the FFT GT4 "PSTN ext transport for M2M (possibility to use G.711 in-band for DTMF transport for M2M special usages th with telephone-event and only for them). |
| **V2.1** | **15/01/18** | In §6 (indication that a call has an international origin in SIP), replacement of the requirement by a following comments received during FFT meeting of 11/12/2017.<br>**Approved public version.** |
| **V2.1.1** | **17/06/19** | Update of the version of the document "Architecture for IP interconnection", FFT Doc 09.002, f 2014) to version V2.0 (May 2018) (in §2, §13, §14, §15, §16).<br>**Public version (minor update)**. |
| V2.1.1.1 (DRAFT V3.0) | 23/07/19 | Draft version taking into account the content of "VoLTE Lot 1" as defined by the FFT's 'IP interconn WG. This draft version introduces:<br>- the SIP Preconditions topic (in sections 2, 4.3.1, 4.3.4.4, 4.3.11 (new), 4.3.12 (new), 10, 12.1.2, 12.1.4 (new)).<br>- the possibility to use of the History-Info header for Call Forwarding services (in sections 17.2.1 (new), 17.2.2, 17.2.3 (new), 17.2.4, 20).<br>- the addition of missing supplementary services and impacts on existing ones (in section 17.1, 17.4 (new), 17.5 (new), 17.6 (new)).<br>- some minor modifications and updates (in sections 2, 4.3.1, 6, 16, 22).<br>- the indication that initial INVITE requests shall contain an SDP offer (in section 12.1.1), meeting of 15/07/19.<br>- The addition of ARCEP's Decision number (n°2019 0954) of July 2019 and of a table fo operator codes and associated C1…C5 coding over the interconnection interface (in se |
| V3.0 draft | 18/11/19 | Clean release for public consultation |
| **V3.0** | **23/03/20** | **Approved public version** |
| V3.1 draft | 13 /12/2021 | This version gathers the recommendations related to :<br>- Transparency for STIR procedure at the SIP/SIP interconnection interface (impacts regarding ST included in next profile version if any)<br>- support of 181 response<br>- ACR service (section 18.6)<br>- Clarifications on PANI (section 5)<br>- Clarification regarding identities rules management (section 6)<br>- Clarification CLIP/CLIR (section 18.1)<br>- Suppression of content regarding Codecs and transcoding guidelines (informative)~~Codecs and t guidelines (informative)~~ that have been moved to the FFTelecom voice architecture recommen |
| **V3.1** | **28/04/2022** | This version intends to answer the manufacturer feedbacks upon consultation. It incorporates:<br>- mainly clarifications on Verification and attestation of calling identity mechanism<br>- precisions on possible semantics of French E164 numbers contained in From header<br>**public version** |
| V3.1.1 | 13/02/2023 | Modifications of §12 allowing use of From header for conveying a national short code. |
| V3.1.2 | 13/03/2023 | Insertion of §11.4 (handling of interaction with call forwarding/diversion services), §28 (calls fro network operator towards OPTS) and §29 (calls from OPTV towards call terminating network op |
| V3.1.3 | 22/03/2023 | Insertion of §11.5 Disabling of calling number authentication on originating networkoperra associated modifications in § 4.3.4.2 and § 11.1 |
| V3.1.3a | 27/03/2023 | Modification of § 4.3.4.2 (APNF's reference document associated to P-Identity-Bypass header) |
| V3.1.4 | 04/04/2023 | Modification of §12 (Note 7) linked to P-Asserted-Id associated to From header containing a nati |
| V3.1.5 | 21/04/2023 | Modifications to § 11.4, §12 (Note 7) and §8 (title). |
| V3.2 draft | 28/04/2023 | Clean release for public consultation |
| **V3.2** | **25/07/2023** | **Approved public version** |
| V3.2.1 | 01/02/2024 | Modification of §12 (modification of Note 7, insetion of Note 8 related to French E.164 prefix contained in header To), modification of §18.1 (CLIP/CLIR) with From header contents that sh received. |
| V3.2.2 | 27/05/2024 | Modifications in § 4.1, creation of §23 (NG eCall) |
| V3.2.3 | 12/06/2024 | Modifications in §9 and §23 (NG eCall) |
| V3.2.4 | 19/06/2024 | Modifications in §23 (NG eCall) and §12. |

| | | |
|---|---|---|
| V3.2.5 | 25/06/2024 | Modifications in §4.3, §9 and §18.1 (CLIP/CLIR). |
| V3.3 draft | 26/07/2024 | Clean release for public consultation |
| **V3.3** | **14/10/2024** | **Approved public version** |
| V3.3.1 | 18/04/2025 | Modifications associated to:<br>- native RTT use during voice calls between national network operators.<br>- P-AI header always sent towards called PSAP when calling access to public telephony n identified and authenticated.<br>- No Diversion/History-Info header in 181 response sent at the SIP NNI |
| V3.3.2 | 23/06/2025 | Modifications associated to:<br>- media session establishment (§13.1): when RTT is invoked, 2 different “m=” lines are p “m=” line contains at least G.711 audio codec.<br>- native RTT use during voice calls between 2 national network operators (cf. §24.2)<br>- reject of incoming calls with international origin should be possible downstream when SIP NNI with a national fixed CLI (cf. 6) |
| V3.3.3 | 30/06/2025 | Modifications associated to:<br>- §4.2.5.3 SIP response handling: SIP request shall not be retried due to the impacts on S wholesale service.<br>- §13.1.1: initial INVITE request shall contain an SDP offer with at least “m=audio” media description shall contain at leasst G.711).<br>- Simplification of one sentence in§6. |
| V3.3.4 | 02/07/2025 | Modifications associated to:<br>- §4.2.5.3 SIP responses handling: insertion of ‘Note 1’.<br>- §5: use of C1…C5 = ‘00000’ value for calls originating in France (e.g. R1R2=63) without on accurate geographic location of calling user.<br>- §13.1.1: Note 1 evolution.<br>- § 24.1: context clarification and addition of mandatory support of redundant text trans 4103).<br>- §27: new study item for next SIP interconnection interface specification version (impac roaming (S8HR scenario) on SIPindication for incoming calls with international origin). |
| V3.3.5 | 10/07/2025 | Modifications associated to:<br>- §6: clarifications on the status of SIP indication for “incoming call with international ori<br>- § 24.1: clarifications on redundant text transmission (§24.1.2 creation). |
| V3.3.6 | 15/07/2025 | Modification of §13.1. |
| V3.4 draft | 20/07/2025 | Clean release for public consultation. |
| **V3.4** | **~~03~~/11/2025** | **Approved public version.** |

# ~~28~~29 Annex 1 – Calls with international origin towards national VAS numbers

This figure below gives an end-to-end macroscopic view of calls that have an international origin towards national VAS:



# ~~29~~30 Annex 2 (informative) – Additional specification part for SIP interconnection call from originating network operator towards (one of) its OPTS

Definition:
An OPTS (“OPérateur Technique de Signature”) is a network operator that proposes a wholesale service enabling attested originating calls signature and relevant Identity header generation in initial INVITE request in compliance with §11 of this specification (cf. APNF’s MAN WG).

Assumption:
an originating network operator N1 is interconnected in SIP with a downstream OPTS using the version 2.1 (or a more recent one like version 3.1) of FFTélécoms’ SIP profile for inter-operator interconnection.

When operator N1 sends an initial INVITE request towards (one of) its OPTS in order to perform attested calling party number’s signature, this request should contain Attestation-info and Origination-Id headers as described in § 4.4 Trust domain of 3GPP’s TS 24.229.

# ~~30~~31 Annex 3 (informative) – Additional specification part for SIP interconnection call from an OPTV towards the call terminating network operator

Definition
An OPTV (OPérateur Technique de Vérification) is a network operator that proposes a wholesale service enabling the verification of signed calls it collects before transmitting them to called party’s network operator (cf. APNF MAN WG).

Assumption: an OPTV is interconnected in SIP with the call terminating network operator using the version 2.1 (or a more recent one like version 3.1) of FFTélécoms’ SIP profile for inter-operator interconnection.

When an OPTV has performed calling party’s signature verification, it sends an initial INVITE request towards the called party’s network operator with From header (or P-Asserted-Id header if From header does not contains a telephone number) containing a verstat parameter coded according to verification procedure result:

- Option 1: “TN-Validation-Passed”
- Option 2: “TN-Validation-Failed”
- Option 3: “No-TN-Validation”

Note: when verstat parameter is coded according to Option 2 (or Option 3), the initial INVITE request may contain a Reason header as described in [RFC3326].

Important: the verstat parameter value should not be used by terminating network operator in order to be sent towards called party handset. (cf. MAN WG decisions).