DELTA Fiber Nederland B.V

Voice services Specification

Version: 1.0

27.1.2022

Disclaimer

When a new version of this specification is published it supersedes all previous versions of this specification. Users are advised to regularly check for updates on this specification.

DELTA Fiber Nederland reserves the right to deviate from this specification, in certain geographical areas for technical tests and network development purposes.

DELTA Fiber Nederland does not take any responsibility for the correctness of the reference values included in this specification.

This specification implements the following (in Dutch):

- Besluit van 12 december 2016, houdende regels inzake eindapparaten ter implementatie van richtlijn 2008/63/EG (Besluit eindapparaten).
- ACM Beleidsregel handhaving besluit randapparaten (bepaling van het netwerkaansluitpunt en de vrije keuze van eindapparaten) – Staatscourant nr. 26456, 27 juli 2021.
- Nota van bevindingen – Beleidsregel handhaving besluit eindapparaten (bepaling van het netwerkaansluitpunt en de vrije keuze van eindapparaten) – Zaaknr. ACM/19/036305/ Documentnr. ACM/UIT/558420.

and is intended for (fiber or cable) modem device manufacturers. The declaration of conformity with this specification is the sole responsibility of the manufacturer.

The specification does not apply under abnormal operating conditions such as:

- operating conditions arising as a result of operating services other than DOCSIS 3.x over the dedicated data RF interface.
- operating conditions arising as a result of a fault, maintenance and construction work or to minimize the extend of interruption of service.
- operating conditions arising as a result of force majeure or third-party interference.
- operating conditions arising as a result of test signal injection governed by regulation.
- In case of non-compliance of a network user’s installation or non-compliance of equipment with the relevant standards or non-compliance with the technical requirements for connection, established either by this interface specification or the public authorities including the relevant limits for electromagnetic compatibility.

The characteristics given in this specification are intended to be used to derive and specify requirements for equipment such as cable modems to connect them to the dedicated data RF interface, Fiber or Ethernet interface. The values in this specification take precedence over requirements in equipment product standards and installation standards. The given characteristics are not intended to be used as electromagnetic compatibility levels or user emission limits in the DELTA Fiber Nederland network.

This specification may be changed at any time and may break backward compatibility with previous versions. Manufacturers are therefore recommended to provide regular software updates to the end users to keep their devices in compliance with this specification. This specification may be superseded in total or in part by the terms of a contract between the individual network user and DELTA Fiber Nederland.

Contact Information

For all questions regarding this document please contact:

DELTA Fiber Nederland B.V.
attn. Afdeling Platforms – Vrije Modem Keuze
Overschieseweg 203
3112 NB Schiedam
Website: http://www.deltafiber.nl

Information for individual customers regarding the use of own modems on the DELTA Fiber networks is available at:

https://www.delta.nl/klantenservice/vrije-modemkeuze/

https://www.caiway.nl/klantenservice/vrije-modemkeuze/

Table of Contents

1. Conventions

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC 2119] [RFC 8174] when, and only when, they appear in all capitals, as shown here.

2. Scope of this document

The purpose of this document is to describe specifications and behavior of the Session Initiation Protocol (SIP) and related media aspects that enables direct connectivity between a SIP-enabled Service Provider Network (DELTA Fiber Netherland B.V.) and a SIP Endpoint (as used at the Customer premises for DELTA and Caiway (retail) consumers).

This document is about Telephony / VoIP and is supplementary to the network specification documents for each access technique (i.e. DOCSIS, FttH-P2P or FttH-XGS-PON) which are leading for the network related specifications.

It specifies the minimal set of IETF and ITU-T standards that must be supported, provides guidance in the areas where the standards leave multiple implementation options, and specifies a minimal set of capabilities that should be supported by the Service Provider and the SIP Endpoint (User-Agent / MTA).

Note: All relevant or mentioned IETF and ITU-T standards are collected in the tables at the end of this document, chapter 21.

3. Reference Architecture

The diagram in Figure 1 shows the functional elements required to support the interface described in this document. The diagram shows two reference points between the SIP UE and the Operator / SP Network (DELTA Fiber Nederland):

- [A] carries SIP signaling messages to support voice services between the SIP UE and the Operator network SIP Signaling Entity (SP-SSE).
- [B] carries the RTP and RTCP packets between the Operator and Media Endpoints.

Together, reference points A and B comprise the interconnection interface.

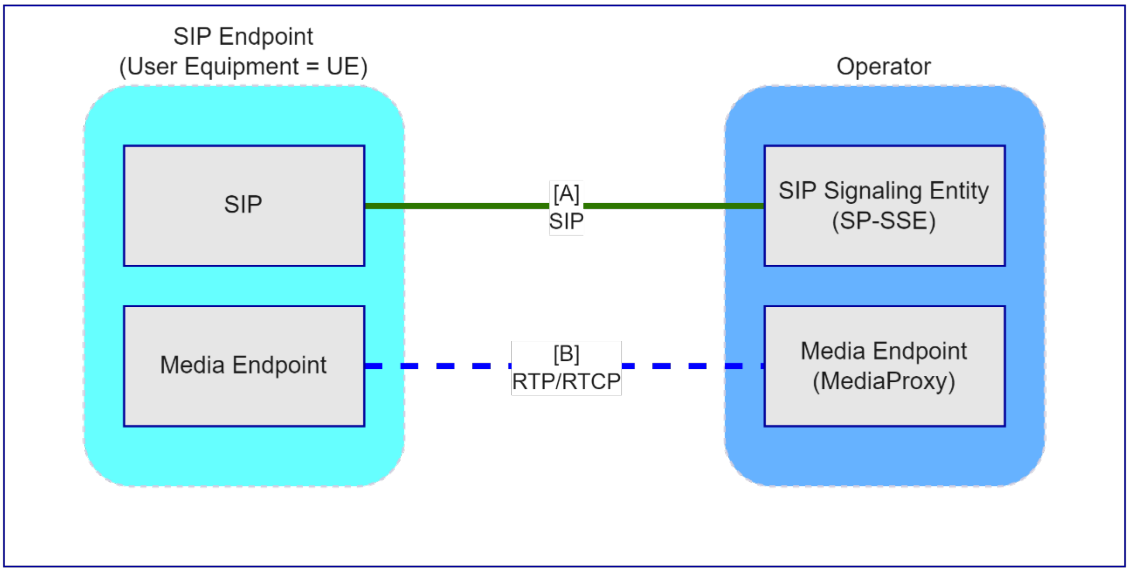

Figure 1

4. Definitions and Abbreviations

4.1. Definitions

Operator SIP-Signaling Entity (SP-SSE) - The Operator (or: Service Provider) point of SIP signaling interconnection with the SIP Endpoint (SIP UE).

SIP Endpoint (SIP UE) - The point of SIP signaling interconnection with the Operator.

Public Identity - An Address of Record (AOR) represented as a SIP URI

Registration AOR (Address of Record) - An AOR represented as a SIP URI, used solely to identify the SIP-UE during registration.

Media Endpoint - Any entity that terminates an RTP/RTCP stream.

Back-to-Back User Agent (B2BUA) - A logical entity that receives a request and processes it as a User Agent Server (UAS). In order to determine how the request should be answered, it acts as a User Agent Client (UAC) and generates a request to another SIP User Agent Server (UAS).

4.2. Abbreviations

Table containing the used abbreviations:

Abbreviation	Explanation
ATA	Analog Telephone Adaptor
CPE	Customer Premises Equipment
CPN	Service Provider Network
DFN	DELTA Fiber Nederland
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTMF	Dual-tone multi-frequency
FttH	Fiber to the Home
IETF	Internet Engineering Task Force
IP	Internet Protocol
MoH	Music-on-Hold
MTA	Multimedia Termination Adapter
NA(P)T	Network Address (and Port) Translation
NAPTR	Name Authority Pointer
PON	Passive Optical Fiber
PSTN	Public Switched Telephone Network
PtP	Point to Point
QoS	Quality of Service
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SC	Service Code (like *21)
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIP ALG	SIP Application Layer Gateway
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time To Live
UA	User Agent
UDP	User Datagram Protocol
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UE	User Equipment
URI	Uniform Resource Identifier

5. Key Assumptions and Limitations of Scope

The primary service to be delivered over this interface is audio-based call origination and/or termination between the SIP UE and the Operator Networks.

The following is not supported and therefore out of scope:

- The delivery of any other service (e.g. video-based services, instant messaging, etc.)
- Signaling considerations between the SP-SSE and other Operator devices (e.g. Trunking Gateway)
- Signaling considerations between the SIP UE and other devices (e.g. IP phones)

The following part of the third party implementation, independent of the DFN network/service and therefore out of scope:

- Layer 3 network design and QoS considerations
- Element management, network management, network security, and other operational considerations

6. IP Connectivity

IP Connectivity is necessary before an SIP device can be used for telephony. This depends on the access technique used, details can be found in DELTA Fiber Docsis, FTTH PtP and FTTH PON Interface Specification documents. These documents are leading over the listed bullets below:

6.1. DOCSIS / COAX

DELTA Fiber Docsis interface specification document

- The SIP UE **MUST** either use the same IP interface that is provisioned by Caiway/DELTA for data service (= Over-the-Top) for cable modems.
- The SIP UE **MUST NOT** announce itself as a PacketCable device by containing string like “pktc1.0”, “pktc1.5” or “pktc2.0” in DHCP option 60.
- The SIP UE **MUST NOT** be configured with a static IP address.
- The SIP UE **MUST** conform to the requirements in DNS standards as described in RFC 1034, RFC 1035, RFC 2782, RFC 2915.
- The SIP UE **MUST** honor the Time to Live (TTL) of DNS lookups.
- The SIP UE **MUST** follow standard industry best practice behavior with regards to usage of TTL.

6.2. FttH Point-to-Point (PtP)

DELTA Fiber PtP interface specification document

- The SIP UE **MUST** use VLAN ID 102 with a separate IP interface for the SIP/VoIP.
- The SIP UE **MUST** use this VLAN for all SIP / VoIP related traffic.
- The SIP UE **MUST NOT** be configured with a static IP address.
- The SIP UE **MUST** obtain an IP address using standard DHCP RFC 2131.
- The SIP UE **MUST** at least request following options (Parameter Request List) to the DHCP server: 1 = Subnet Mask, 3 = Router, 6 = Domain Name Server.
- The SIP UE **MUST** conform to the requirements in DNS standards as described in RFC 1034, RFC 1035, RFC 2782, RFC 2915.
- The SIP UE **MUST** honor the Time to Live (TTL) of DNS lookups.
- The SIP UE **MUST** follow standard industry best practice behavior with regards to usage of TTL.

6.3. FttH Point-to-Multipoint (XGS-PON)

DELTA Fiber PON interface specification document

- The SIP UE **MUST** use VLAN 102 with a separate IP interface for the SIP/VoIP.
- The SIP UE **MUST** use this VLAN for all SIP / VoIP related traffic.
- The SIP UE **MUST NOT** be configured with a static IP address.
- The SIP UE **MUST** obtain an IP address using standard DHCP RFC 2131.
- The SIP UE **MUST** at least request following options (Parameter Request List) to the DHCP server: 1 = Subnet Mask, 3 = Router, 6 = Domain Name Server.
- The SIP UE **MUST** conform to the requirements in DNS standards as described in RFC 1034, RFC 1035, RFC 2782, RFC 2915.
- The SIP UE **MUST** honor the Time to Live (TTL) of DNS lookups.
- The SIP UE **MUST** follow standard industry best practice behavior with regards to usage of TTL.

7. Basic SIP Support

SIP UE’s **MUST** support SIP in accordance with RFC 3261, RFC 3263 and offer-answer in accordance with RFC 3264, as qualified by statements in later sections of this document.

For the purpose of NAT traversal, a SIP UE **MUST** use the same port from sending and receiving SIP packets in accordance with RFC 3581.

Requirements for support of other IETF RFC’s and other standards are as stated in 20.3 at the end of this document.

8. Supported Signaling Transport Protocols

SIP UE’s **MUST** implement UDP.

SIP UE’s **MUST** learn the port where the SP-SSE listens to, from DNS query as per RFC 3263. By default this SIP port is 5060.

SIP UE’s **MUST NOT** use TCP, SCTP or TLS.

9. Modes of Operation

The only mode of operation supported in the context of this document is Registration mode. The other mode (Static mode) is not supported.

In the Registration mode, the SIP UE’s conveys its SIP signaling address to the Operator Network using the SIP registration procedure defined in RFC 3261.

The SP-SSE authenticates the SIP UE using SIP Digest.

SIP UE’s **MUST** support Registration mode.

9.1. Registration Mode

In Registration mode, the SIP UE conveys its SIP signaling address to the Operator Network using the SIP registration procedure. In effect, the SIP UE registers with the Operator Network.

9.1.1. Registration

In the REGISTER request, the SIP UE **MUST** include a Contact URI in accordance with RFC 3261 using a suitable domain part, e.g., the SIP UE's IP address. The SIP UE **MUST** insert the Registration AOR in the "From" and "To" header fields of the REGISTER request.

The REGISTER **MUST** include an expire header with a value of 300 seconds.

The SIP UE and SP-SSE **MUST** support the authentication mechanisms for digest authentication for the REGISTER requests, using a SIP Account and password agreed to by both parties. Using our SelfServiceportal, our Enduser is able to retrieve their SIP Account and set a SIP password.

9.1.2. Failure of SIP Endpoint to reach the SP-SSE

If the SIP UE fails to receive any response to a REGISTER request in Timer F time (typically 32 seconds) or encounters a transport error when sending a REGISTER request, the SIP UE **MUST** consider the SP-SSE unreachable and try to register with an alternate SP-SSE address if it has one.

If the SIP UE has an established connection-based transport (e.g., TCP) to the SP-SSE, and Timer F expires or a transport error is encountered as above, it **MUST** try to re-establish a connection to the same SP-SSE before considering it unreachable, by resetting Timer F and sending a new REGISTER request. The SIP UE **MUST NOT** attempt to re-establish the connection to the same SP-SSE more than once before considering the SP-SSE unreachable.

If no SP-SSE is reachable, or no alternates are available, the SIP UE **MUST** delay reattempting Registration for 30 seconds, and increasing this delay value by doubling it for each successive delivery failure until delivery succeeds, up to a maximum value of 960 seconds.

The RFC 3261 (from section 17.1.1.1) describes the usage of the mentioned timers and behavior.

9.1.3. Unknown SIP Endpoint Identity

Due to the nature of the provisioning a SP-SSE cannot know if the user does exist, as the account may exists but not have been present at the moment the request arrives. If the account does not exist, the SP-SSE **MUST** send a 401 Unauthorized to the SIP UE, which **MUST** retry a Registration attempt later. Any other code sent by the SP-SSE could cause a permanent failure, and the SIP UE will never retry again unless rebooted.

9.1.4. Incorrect SIP Endpoint Password

If the digest challenge response of the SIP UE in its REGISTER request is stale or invalid, the SP-SSE will issue one of the following response codes:

- 401 Unauthorized,
- 407 Authentication Required or
- 403 Forbidden

If a SIP UE receives more than three responses of 401, 407 or 403 in aggregate, without a different response other than one of those in between, then the SIP UE **MUST** consider the Registration attempt to have failed.

9.1.5. SP-SSE Administratively Disabled or Overloaded

An overloaded SP-SSE **MAY** generate a 503 Service Unavailable or 500 Internal Error response code to a REGISTER request, unless it is silently discarding requests due to overload, and **SHOULD** include a "Retry-After" header field value indicating how long the SIP UE should wait before re-attempting a REGISTER request to the same SP-SSE.

A SIP UE receiving such a response **MUST** support the "Retry-After" header field, and **MUST** honor the value as follows: if the value is 32 seconds or less, it **MUST** wait the requested time and retry the request to the same SP-SSE; if the value is larger, it **MUST** remember the value for that SP-SSE address instance, and try any alternate SP-SSE addresses it can. If an alternate SP-SSE can be successfully reached and Registration succeeds through the alternate, the SIP UE **MAY** discard the "Retry-After" value of the original. Otherwise, it **MUST** wait to reattempt registration to the original SP-SSE for the "Retry-After" interval.

9.1.6. Registration-related failures for other requests

If a SIP UE encounters a transport error when attempting to contact the SP-SSE, encounters Timer F expiry (non-INVITE requests) or Timer B expiry (INVITE requests), or receives a 403 response for any non-REGISTER request, the SIP UE **MUST**

- consider the request attempt to have failed and
- assume that the SIP UE's registration is no longer active at the SP-SSE.

The RFC 3261 (from section 17.1.1.1) describes the usage of the mentioned timers and behavior.

9.1.7. Maintaining Registration

It is important that registrations are maintained and, in the event of failure, are re-established quickly, since the SP-SSE depends on the SIP UE being registered in order to deliver inbound requests to the SIP UE. The SIP UE **MUST** honor the REGISTER expiry time provided by the SP-SSE, and **MAY** send REGISTER requests more frequently if NAT and firewall policies require this.

If failure is detected a SIP UE **MUST** attempt reconnection, and if that fails **MUST** try an alternative SP-SSE if available.

9.1.8. Authentication of the SIP Endpoint by the Operator

The SIP UE **MUST** support the digest authentication scheme as described in Section 22.4 of RFC 3261. The Operator assigns the SIP UE an username and associated password that are valid within the Operator SIP domain (realm).

The following rules apply:

The SP-SSE **MAY** challenge any SIP request. The SIP UE **MUST** support receiving 401 Unauthorized and 407 Authentication Required from the SP-SSE. When so challenged by the SP-SSE, the SIP UE **MUST** respond with authentication credentials that are valid within the Operator.

In order to avoid unnecessary challenges, the SIP UE **SHOULD** include its authentication credentials using the current nonce in each subsequent request that allows authentication credentials to be sent to the SP-SSE.

10. Public Identities

SIP UE’s **MUST** be able to support Public Identities in the form of a SIP URI containing a global E.164 [ITU-T E.164] number and the "user=phone" parameter.

For example:

sip: 0031101234567@SIP_DOMAIN;user=phone

The global E.164 number **MAY** begin with a leading "+", **MUST NOT** contain a phone-context parameter and **MUST NOT** include visual separators.

11. Establishing Basic 2-Way Calls

This section describes the procedures for establishing basic 2-way calls between the SIP UE and the Operator Network.

11.1. Outgoing Calls from the Operator to the SIP Endpoint

11.1.1. Request-URI

On receiving an INVITE request from the SP-SSE, the SIP UE **MUST** identify the called user based on the contents of the Request-URI.

11.1.2. "To" header field

The SIP UE **MUST NOT** rely on the contents of "To" header field for routing-decisions, but **MUST** use the info from Request-URI instead.

11.1.3. "From" header field

For IP-based originations, there are no special restrictions on the contents of the "From" header field URI, beyond the requirements specified in RFC 3261. In cases where the SP-SSE needs to generate an anonymous URI (e.g., for a call incoming to the Operator Network from the PSTN for which calling number privacy is requested), the SP-SSE will send a URI as shown here.

sip:anonymous@anonymous.invalid

Note: no semantic meaning is attributed to the display name.

The SP-SSE populates the "From" header field with a SIP URI containing the E.164 calling number, the Operator SIP domain name, and the "user=phone" parameter as shown below.

If any display name information is available and has not been restricted for delivery, it will also be provided by the SP-SSE.

sip:0031101234567@SIP_DOMAIN;user=phone

11.1.4. "Privacy" header field

If the caller requested privacy the SP-SSE **MAY** remove any P-headers when the server is sending the request to a SIP UE. The P-headers are only preserved when calls are routed to other Operators and PSTN Gateways (trusted peers).

In addition the SP-SSE **SHALL** provide an anonymous "From" header field URI as specified before sending the request to the SIP UE.

The SIP UE **MUST** support receiving a "Privacy" header field from the SP-SSE that contains a priv-value of either ‘id’ or ‘none’, as per RFC 3325, RFC 5876 and RFC 3323.

11.2. Outgoing Calls from the SIP Endpoint to the Operator

This section describes SIP UE and SP-SSE requirements for populating and receiving the Request-URI and "To" and "From" header fields for new dialog INVITE requests sent from the SIP UE to the SP-SSE. The SIP UE **MUST** ensure that all other header fields in the INVITE request comply with RFC 3261.

This section covers the case where the call is initiated by the SIP UE.

11.2.1. Request-URI

The SIP UE **MUST** populate the Request-URI of the INVITE request with a SIP URI of the following form, using the domain name of the Operator in the host part:

sip: 0031101234567@SIP_DOMAIN;user=phone

11.2.2. "To" header field

The "To" header field URI in a SIP request generated by the SIP UE is normally populated with the same URI as the Request-URI.

11.2.3. "From" header field

The SIP UE **MUST** populate the "From" header field URI with a URI that the SP-SSE wishes to be used for caller identification. In cases where the SIP UE needs to generate an anonymous URI on behalf of a caller (as opposed to passing on a received anonymous URI), the SP-SSE will check the validity of the From header, it must match the authentication credentials.

If anonymity is required, the SP-SSE will manipulate the headers accordingly.

11.2.4. "P-Asserted-Identity" header field

The SIP UE **MAY** include a "P-Asserted-Identity" header field in the INVITE request in accordance with the rules of RFC 3325 and RFC 5876, but the SP-SSE will remove any P-headers received from a SIP EU and will assert its own headers based on user profile in the database on the SP-SSE.

11.2.5. "Privacy" header field

If the SIP UE requires privacy for a call by suppressing delivery of caller identity to downstream entities, the SP-SSE **MUST** include a "Privacy" header field with value 'id' in the INVITE request, in addition to providing an anonymous "From" header field URI as specified.

11.2.6. User-Agent header field

The SIP UE **SHALL** contain a User-Agent header field containing a string with information about the UAC originating the request. It describes the source device that generated the SIP INVITE, with the contents/values of the following items: <VENDOR> <DEVICE MODEL/TYPE> <SOFTWARE VERSION>

12. Call Forwarding

Beside the SP-SSE based call forwarding where call forwarding’s can be configured by the user via service codes (SC) also known as Voice Features, like calling to *21, the SIP UE **MAY** also implement means to forward calls through the (web)interface. In order to forward a call, the SIP UE **MUST** send an INVITE request to the SP-SSE, with the Request-URI identifying the forwarded-to target destination.

The "To" header field URI can identify the originally targeted destination, in which case it will not match the Request-URI;

The "P-Asserted-Identity" header field can be absent or can assert an identity that is not a Public Identity;

The "From" header field URI **MUST** contain the Public Identity.

There **MUST** be a Diversion Header RFC 5806 that contain the Public Identity of the forwarding SIP UE.

13. Requirements for use of the re-INVITE method

The SIP UE **MUST** support both sending and receiving a re-INVITE request with an SDP offer, and sending and receiving a re-INVITE request without an SDP offer.

14. Media and Session Interactions

14.1. SDP Offer/Answer

A SIP UE acting on behalf of a Media Endpoint that originates and/or terminates RTP traffic **MUST** utilize the Session Description Protocol (SDP) as described in RFC 4566 in conjunction with the offer/answer model described in RFC 3264 to exchange media capabilities (IP address, port number, media type, send/receive mode, codec, DTMF mode, etc.).

SIP UE's **MUST** be capable of receiving INVITE requests without an SDP offer and supplying an SDP offer in an appropriate response, in accordance with RFC 3261.

A SIP UE that participates in SDP offer/answer negotiation **MUST** be prepared to accept additional offers containing SDP with a version that has not changed, and **MUST** generate a valid answer (which could be the same SDP sent previously, or could be different).

A SIP UE that sends additional SDP offers with the same version **MUST** be prepared to accept answers with SDP which may be the same as the previously received SDP, or may be different.

SIP UE implementations sending changes to negotiated media capabilities via SIP re-INVITE **MUST** support RFC 3261.

The SIP UE **MUST** use the same port for sending and receiving media and control packets (called symmetric RTP/RTCP), otherwise one cannot traverse the NAT if the port has not been used for outgoing packets first, in accordance with RFC 4961.

14.2. Codec Support and Media Transport

A Media Endpoint **MUST** transport and receive voice samples using the real-time transport protocol (RTP) as described in RFC 3550.

Any Media Endpoint **MUST** use the ITU-T G.711 a-Law (PCMA) voice codec.

Any Media Endpoint **MAY** use the ITU-T G.711 mu-Law (PCMU) or G.729 voice codec.

Any Media Endpoint **MUST NOT** use Silence suppression or Comfort Noise (CN) voice codec (as referenced in RFC 3389).

Any Media Endpoint that originates and/or terminates RTP traffic over UDP **MUST** use the same UDP port for sending and receiving session media (i.e. symmetric RTP, as referenced in RFC 4961).

Any Media Endpoint that originates and/or terminates RTP traffic **MUST** be capable of processing RTP packets with a different packetization rate than the rate used for sending.

Any Media Endpoint that originates and/or terminates voice traffic **MUST** support the ITU-T G.711 a-Law (PCMA) and mu-Law (PCMU) voice codec with a packetization rate of 20 ms.

14.3. Transport of DTMF Tones

A SIP UE **MUST** advertise support for telephone-events RFC 4733 in its SDP on behalf of any Media Endpoint that supports receiving DTMF digits using RFC 4733 procedures.

Any Media Endpoint that supports receiving DTMF **MUST** support RFC 4733 procedures.

Any Media Endpoint that supports sending DTMF **MUST** use the RFC 4733 procedures to transmit DTMF tones using the RTP telephone-event payload format, provided that the other side has advertised support for receiving RFC 4733 in the offer/answer exchange.

To provide backward compatibility with RFC 2833 implementations, any Media Endpoint **MUST** be prepared to receive telephone-event packets for all events in the range 0-15 and a SIP UE **MUST** be prepared to accept SDP with a payload type mapped to telephone-event.

14.4. FAX Calls

T.38 FAX relay **MUST NOT** be used.

Faxes and other modem transmissions **MUST** be supported over in-band ITU-T G.711 a-Law (PCMA) voice codec or **MAY** over ITU-T G.711 mu-Law (PCMA) voice codec, but we cannot guarantee the end-to-end interoperability.

14.5. Ringback Tone and Early Media

The delivery of in-band announcements and call progress tones from the Operator to a caller before a call is answered is achieved through early media. When acting as a call originator, the SIP UE, upon receipt of a 180 provisional response message (whether reliable RFC 3262 or unreliable) **MUST** instruct the Media Endpoint to play local Ringback tone to the user. Upon receipt of SDP in any 18x provisional response message (reliable RFC 3262 or unreliable), the SIP UE **MUST** forward this information to the Media Endpoint.

When acting as a call terminator and expecting the originating end to provide local Ringback tone, the Media Endpoint **MUST NOT** send RTP packets to the originator if a 180 provisional response message was sent. A Media Endpoint, on receipt of an instruction to play local Ringback tone, **MUST** do so until it receives valid RTP packets or is instructed by the SIP UE that the call has been answered. On receipt of valid RTP packets, a Media Endpoint **MUST** disable any local Ringback tone and play the received media. A Media Endpoint, on receipt of information concerning received SDP, **MAY** use the information to determine whether RTP packets received are valid and **MAY** discard RTP packets arriving before that time.

15. Supported Service Codes

The SP-SSE supports Service Codes, also known as Voice Features or Telephony services, which are handled by the platform used at our Service Provider Network.

In order to make use of these Service Codes, the SIP UE **MUST** send an INVITE request to the SP-SSE, with the Request-URI which are valid destinations.

Examples are:

URI	Description
***21*<destination>**	Enable Forward all incoming calls to <destination>
21	Disable Forward all incoming calls
***21*1**	Enable Forward all incoming calls to Voicemail
62	Enable/Disable Block incoming anonymous calls

More examples are listed in the following Enduser reference guides:

https://www.caiway.nl/klantenservice/telefonie/doorschakelen/sterretjesdiensten

https://www.delta.nl/bellen/mogelijkheden

16. References

16.1. ITU-T

International Telecommunications Union (ITU-T) References overview:

URL	Author(s)	Subject	Ref	Date
ITU-T E.164	International Telecommunications Union	"Recommendation E.164: The international public telecommunication numbering plan"	E.164	May 1997
ITU-T G.168	International Telecommunications Union	"Recommendation G.168:Digital network echo cancellers"	G.168	January 2007
ITU-T G.711	International Telecommunications Union	"Recommendation G.711: Pulse code modulation (PCM) of voice frequencies "	G.711	November 1988
ITU-T G.729	International Telecommunications Union	"Recommendation ITU-T G.729: Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)"	G.729	January 2007

16.2. IETF RFC

RFC References overview from the Internet Engineering Task Force (IETF):

RFC URL	Author(s)	Subject	Ref	Date
RFC1034	P. Mockapetris	"DOMAIN NAMES - CONCEPTS AND FACILITIES"	RFC 1034	November 1987
RFC1035	P. Mockapetris	"DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION"	RFC 1035	November 1987
RFC1918	Y. Rekhter, R. G Moskowitz, D. Karrenberg, G.J. de Groot, E. Lear	"Address Allocation for Private Internets"	RFC 1918	February 1996
RFC2119	S. Bradner	"Key words for use in RFCs to Indicate Requirement Levels"	BCP 14 RFC 2119	March 1997
RFC2131	R. Droms	"Dynamic Host Configuration Protocol"	RFC 2131	March 1997
RFC2246	T. Dierks, C. Allen	"The TLS Protocol Version 1.0"	RFC 2246	January 1999
RFC2560	M. Myers et. al.	"X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP"	RFC 2560	June 1999
RFC2782	A. Gulbrandsen, P. Vixie, L. Esibov	"A DNS RR for specifying the location of services (DNS SRV)"	RFC 2782	February 2000
RFC2833	H. Schulzrinne, S. Petrack	"RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals"	RFC 2833	May 2000
RFC2915	M. Mealling, R. Daniel	"The Naming Authority Pointer (NAPTR) DNS Resource Record"	RFC 2915	September 2000
RFC3261	J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler	"SIP: Session Initiation Protocol"	RFC 3261	June 2002
RFC3262	J. Rosenberg, H. Schulzrinne	"Reliability of Provisional Responses in Session Initiation Protocol (SIP) "	RFC 3262	June 2002
RFC3263	J. Rosenberg, H. Schulzrinne	"Session Initiation Protocol (SIP): Locating SIP Servers"	RFC 3263	June 2002
RFC3264	J. Rosenberg, H. Schulzrinne	"An Offer/Answer Model with Session Description Protocol (SDP)"	RFC 3264	June 2002
RFC3265	A. B. Roach	"Session Initiation Protocol (SIP)-Specific Event Notification."	RFC 3265	June 2002
RFC3311	J. Rosenberg	"The Session Initiation Protocol (SIP) UPDATE Method"	RFC 3311	September 2002
RFC3323	J. Peterson	"A Privacy Mechanism for the Session Initiation Protocol (SIP)"	RFC 3323	November 2002

RFC URL	Author(s)	Subject	Ref	Date
RFC3325	C. Jennings, J. Peterson, M. Watson	"Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks"	RFC 3325	November 2002
RFC3327	D. Willis, and B. Hoeneisen	"Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts"	RFC 3327	December 2002
RFC3389	R. Zopf	"Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN) "	RFC 3389	September 2002
RFC3515	R. Sparks	"The Session Initiation Protocol (SIP) Refer Method"	RFC 3515	April 2003
RFC3550	H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson	"RTP: A Transport Protocol for Real-Time Applications"	RFC 3550	July 2003
RFC3581	J. Rosenberg, H. Schulzrinne	"An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing"	RFC 3581	August 2003
RFC3665	A. Johnston, S. Donovan, R. Sparks, C. Cunningham, K. Summers	"Session Initiation Protocol (SIP) Basic Call Flow Examples"	RFC 3665 BCP 75	December 2003
RFC4538	J. Rosenberg	"Request Authorization through Dialog Identification in the Session Initiation Protocol (SIP) "	RFC 4538	June 2006
RFC4566	M. Handley, V. Jacobson, C. Perkins	"SDP: Session Description Protocol"	RFC 4566	July 2006
RFC4733	H. Schulzrinne, T. Taylor	"RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals"	RFC 4733 (Obsoletes RFC 2833)	December 2006
RFC4856	S. Casner	"Media Type Registration of Payload Formats in the RTP Profile for Audio and Video Conferences"	RFC 4856	March 2007
RFC4961	D. Wing	"Symmetric RTP / RTP Control Protocol (RTCP)"	RFC 4961	July 2007
RFC4967	B. Rosen	"Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier"	RFC 4967	July 2007
RFC5031	H. Schulzrinne	"A Uniform Resource Name (URN) for Emergency and Other Well-Known Services"	RFC 5031	January 2008
RFC5280	D. Cooper et. al.	"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"	RFC 5280	May 2009
RFC5589	R, Sparks, A. Johnston, D. Petrie	"Session Initiation Protocol Call Control – Transfer"	RFC 5589	March 2009

RFC URL	Author(s)	Subject	Ref	Date
RFC5806	S. Levy, M. Mohali	"Diversion Indication in SIP"	RFC 5806	March 2010
RFC5876	J. Elwell	"Updates to Asserted Identity in the Session Initiation Protocol (SIP)"	RFC 5876	April 2010
RFC8174	B. Leiba	"Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words"	RFC 8174	May 2017

16.3. SIP Forum

SIP Forum Document references:

URL	Author(s)	Subject	Ref	Date
SIP Forum Document Number: TWG-2	S. Dawkins	SIP Endpoint / Service Provider Interoperability "SIPconnect 1.1 Technical Recommendation"	TWG-2	2011
SIP Forum Document Number: TWG-11	A Hutton, G. Salgueiro	SIP-PBX / Service Provider Interoperability "SIPconnect 2.0 Technical Recommendation"	TWG-11	2016