Interface Specification

for the
Telephony Service
in the Cable Network of
PŸUR – Tele Columbus Group

Version: 2.0
Date: Mai 25, 2020
Status: Issued
Author: PŸUR – Tele Columbus Group

Tele Columbus AG
Vorstand: Dr. Daniel Ritz (Vorsitzender),
Eike Walters

Sitz der Gesellschaft
Kaiserin-Augusta-Allee 108
10553 Berlin

Weitere Informationen erhalten Sie unter
www.pyur.com

1 Disclaimer

This document is furnished on an "AS IS" basis. Tele Columbus Group and its affiliates and/or subsidiaries as defined under 4. below (together “Operator”) are not liable regarding claims arising from or in context with the application of this document.

Operator reserves the right to apply at any time implementations deviating from this document for reasons of technical trials that are limited in time and geographic area.

This document is subject to amendments without any notice. From publication of a new version of this document all prior versions shall become obsolete.

3 Contents

4 Conventions

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in [RFC 2119]

5 Applicability and Contact

This document applies to Tele Columbus Group. Affiliates and/or subsidiaries as listed below:

- Martens Deutsche Telekabel GmbH
- PrimaCom Berlin GmbH
- KSP-Kabelservice Prenzlau GmbH
- Tele Columbus Multimedia GmbH
- Tele Columbus Hessen GmbH
- Tele Columbus Kabel Service GmbH
- Tele Columbus Netze Berlin GmbH
- BIG Medienversorgung GmbH
- Tele Columbus Cottbus GmbH
- Tele Columbus Berlin-Brandenburg GmbH & Co.KG
- Tele Columbus Sachsen-Anhalt GmbH
- Tele Columbus Sachsen-Thüringen GmbH
- BBcom Berlin-Brandenburgische Communikationsges. mbH
- Teleco GmbH Cottbus Telekommunikation
- Cable Plus GmbH
- Wwcon Wärme-Wohnen-Contracting GmbH
- pepcom GmbH
- KKG Kabelkommunikation Güstrow GmbH
- TKN Telekabel-Nord GmbH
- FAKS, Frankfurer Antenne- und Kommunikationsservice GmbH
- REKA Regionalservice Kabelfernsehen GmbH
- Tele-System Harz GmbH
- Kabelcom Rheinhessen GmbH
- NEFtv GmbH
- Kabelfernsehen München Servicecenter GmbH
- WTC Wohnen & TeleCommunication Verwaltung GmbH & Co.KG
- Cabletech Kabel- und Antennentechnik GmbH
- MEDIACOM Kabelservice GmbH
- Hlkomm Telekommunikations GmbH

For all questions regarding this document please contact:
Tele Columbus AG
Kaiserin-Augusta-Allee 108
10553 Berlin
Website: http://www.pyur.com

6 Reference Architecture

The reference architecture 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 Endpoint and the Operator Network; reference point (1) and reference point (2).

Reference point (1) carries SIP signaling messages to support voice services between the SIP Endpoint and the Operator network SIP Signaling Entity (SP-SSE).

Reference point (2) carries the RTP and RTCP packets between the Operator and Media Endpoints.

Reference points (1) and (2) together comprise the interconnection interface.

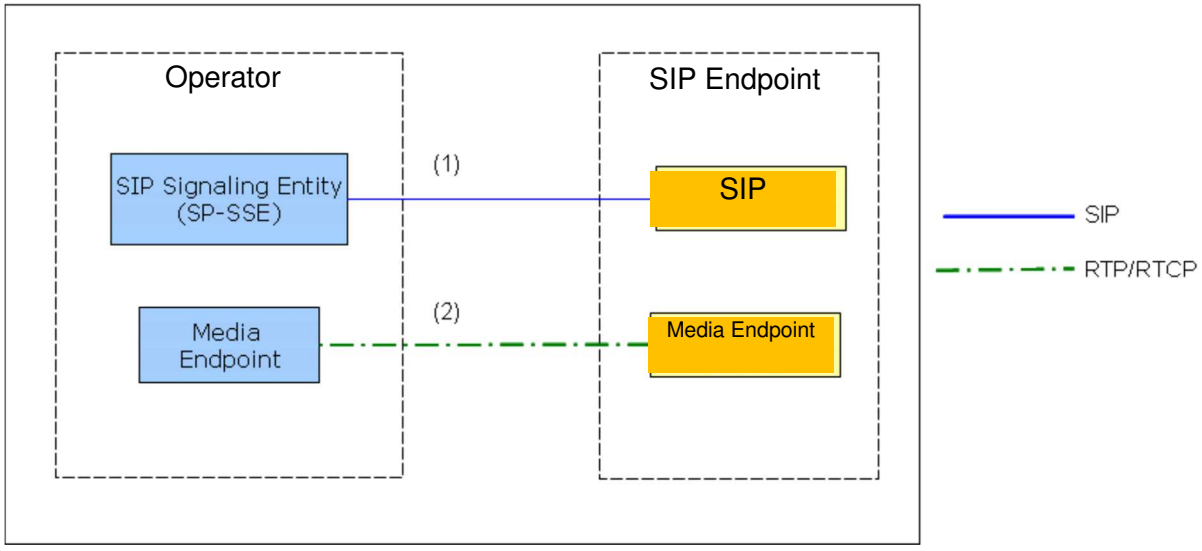

Figure 1: Reference Architecture

7 Definitions

Operator SIP-Signaling Entity (SP-SSE)

– the Operator (or: Service Provider) point of SIP signaling interconnection with the SIP Endpoint.

SIP-Endpoint

– the point of SIP signaling interconnection with the Operator.

Public Identity

– an Address of Record (AOR) represented as a SIP URI

Registration AOR

– an AOR represented as a SIP URI.

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).

8 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 Endpoint and the Operator Networks, including emergency services. The delivery of any other service (e.g. video-based services, instant messaging, etc.) is out of scope.

Signaling considerations between the SP-SSE and other Operator devices (e.g. Trunking Gateway) are outside the scope of this document.

Signaling considerations between the SIP Endpoint and other devices (e.g. IP phones) are outside the scope of this document.

Layer 3 network design and QoS considerations are outside of the scope of this document

Element management, network management, network security, and other operational considerations are outside the scope of this document.

9 Basic SIP Support

SIP Endpoint **MUST** support SIP in accordance with [RFC 3261] and offer-answer in accordance with [RFC 3264], as qualified by statements in later sections of this document. Requirements for support of other IETF RFCs and other standards are as stated in later sections of this document.

10 Modes of Operation

The only mode of operation supported in the context of this document is registration mode.

In the Registration mode, the SIP Endpoint conveys its SIP signaling address to the Operator Network using the SIP registration procedure defined in [RFC 3261]

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

SIP Endpoints **MUST** support registration mode.

11 Supported Signaling Transport Protocols

SIP Endpoints **MUST** implement UDP. TCP support is **OPTIONAL**.

12 Public Identities

SIP Endpoints **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:004934186970@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.

13 Establishing Basic 2-Way Calls

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

13.1 Outgoing Calls from the Operator to the SIP Endpoint

13.1.1 Request-URI

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

13.1.2 "To" header field

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

13.1.3 "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:004934186970@SIP_DOMAIN;user=phone

13.1.4 "P-Asserted-Identity" and "Privacy" header fields

If the caller requested privacy the SP-SSE **MAY** include a "Privacy" header field with value 'id' in the INVITE request, in addition to providing an anonymous "From" header field URI as specified before sending the request to the SIP Endpoint.

The SIP Endpoint **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].

13.2 Outgoing Calls from the SIP Endpoint to the Operator

This section describes SIP Endpoint 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 Endpoint to the SP-SSE. The SIP Endpoint **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 Endpoint.

13.2.1 Request-URI

The SIP Endpoint **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:004934186970@SIP_DOMAIN;user=phone

13.2.2 "To" header field

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

13.2.3 "P-Asserted-Identity" header field

The SIP Endpoint **MAY** include a "P-Asserted-Identity" header field in the INVITE request in accordance with the rules of [RFC 3325] and [RFC 5876].

13.2.4 "From" header field

The SIP Endpoint **MUST** populate the "From" header field URI with a URI that the SIP PBX wishes to be used for caller identification. In cases where the SIP Endpoint needs to generate an

anonymous URI on behalf of a caller (as opposed to passing on a received anonymous URI), the SIP Endpoint **MUST** send a URI of the form

"sip:anonymous@anonymous.invalid"**sip:anonymous@anonymous.invalid**

13.2.5 "Privacy" header field

If the SIP Endpoint requires privacy for a call by suppressing delivery of caller identity to downstream entities, it **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.

14 Call Forwarding

Beside the SP-SSE based call forwarding where call forwardings can be configured by the user via vertical service codes (VSC) the SIP Endpoint **MAY** also implement means to forward calls through the interface. In order to forward a call, the SIP Endpoint **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 an Public Identity;

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

There **MUST** be a Diversion Header [RFC5806] that contain the Public Identity of the forwarding SIP endpoint.

15 Requirements for use of the re-INVITE method

The SIP Endpoint **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.

16 Emergency Services

The SIP Endpoint **MUST** have a dial plan that recognizes emergency calls. When a SIP Endpoint routes a call recognized as an emergency call to the SP-SSE, it **MUST** populate the Request-URI using a dial string URI that contains the national emergency services number.

The SIP Endpoint **MUST** include the identity of the caller in the "From" header. The SIP Endpoint **MUST NOT** anonymize the "From" header field.

17 Media and Session Interactions

17.1 SDP Offer/Answer

A SIP Endpoint 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 Endpoints **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 Endpoint 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 Endpoint 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 Endpoint implementations sending changes to negotiated media capabilities via SIP reINVITE **MUST** support [RFC 3261].

17.2 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 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).

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] µ-Law and A-Law PCM codecs with a packetization rate of 20 ms.

17.3 Transport of DTMF Tones

A SIP Endpoint **MUST** advertize 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 advertized 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 Endpoint **MUST** be prepared to accept SDP with a payload type mapped to telephone-event.

If the other side does not advertize any [RFC4733] procedures DTMF MUST be transported in-band as normal audio tones with on special coding or markers.

17.4 Echo Cancellation

Any Media Endpoint that can introduce echo **MUST** provide [ITU-T G.168]-compliant echo cancellation.

17.5 FAX Calls

Media Endpoints that support fax (e.g., a SIP media server that can originate/terminate faxes) and Media Endpoints that can act as a T.30 gateway (e.g., a Media Endpoint that supports an RJ11 analog telephone interface) **MUST** support the [ITU-T G.711] µ-Law and A-Law PCM codecs.

17.6 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 Endpoint, 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 Endpoint **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 Endpoint 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.

17.7 Putting a Session on Hold

A 2-way session can be put on hold by using an offer-answer exchange and the directionality attributes as described below.

The hold initiator **MUST** set the SDP directionality attribute to "a=sendonly".

If the hold initiator does not provide Music on hold (MOH), it **MUST** set the SDP directionality attribute to "a=inactive" or "a=sendonly". The attribute "a=inactive" is **RECOMMENDED** because it provides an indication to the held entity that MOH is not being provided by the hold initiator.

A SIP Endpoint **MUST** support the ability to receive SDP session descriptions that have the ‘c=’ field set to all zeros (0.0.0.0), when the addrtype field is IPv4.

18 Registration Mode

In Registration mode, the SIP Endpoint conveys its SIP signaling address to the Operator Network using the SIP registration procedure. In effect, the SIP Endpoint registers with the Operator Network, just as a directly hosted SIP Endpoint would register. However, because a SIP Endpoint has multiple Public Identities, it needs to register a contact address on behalf of each of these.

18.1 Firewall and NAT Traversal

The Operator Network is providing an implicit NAT traversal function.

18.2 Registration

In the REGISTER request, the SIP Endpoint **MUST** include a Contact URI in accordance with [RFC 3261] using a suitable domain part, e.g., the SIP Endpoint's IP address. The SIP Endpoint **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 from 600 to 3600 seconds.

The SIP Endpoint and SP-SSE **MUST** support the authentication mechanisms for digest authentication for the REGISTER requests, using a user name and password agreed to by both parties.

18.3 Failure of SIP Endpoint to reach the SP-SSE

If the SIP Endpoint 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 Endpoint **MUST** consider the SP-SSE unreachable and try to register with an alternate SP-SSE address if it has one. If the SIP Endpoint 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 Endpoint **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 Endpoint **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.

18.4 Unknown SIP Endpoint Identity

The SP-SSE **MUST** issue a 404 Not Found response to a REGISTER request, if the Registration AOR of the SIP Endpoint is not found in its database. An SIP Endpoint receiving such a response to a REGISTER request **MUST** consider the Registration attempt to have failed.

18.5 Incorrect SIP Endpoint Password

If the digest challenge response of the SIP Endpoint 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 Endpoint 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 Endpoint **MUST** consider the Registration attempt to have failed.

18.6 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 Endpoint should wait before re-attempting a REGISTER request to the same SP-SSE.

A SIP Endpoint 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 Endpoint **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.

18.7 Registration-related failures for other requests

If a SIP Endpoint 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 Endpoint **MUST**

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

18.8 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 Endpoint being registered in order to deliver inbound requests to the SIP Endpoint. The SIP Endpoint **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 Endpoint **MUST** attempt reconnection, and if that fails **MUST** try an alternative SP-SSE if available.

18.9 Authentication of the SIP Endpoint by the Operator

The SIP Endpoint **MUST** support the digest authentication scheme as described in Section 22.4 of [RFC 3261]. The Operator assigns the SIP Endpoint a 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 Endpoint **MUST** support receiving 401 Unauthorized and 407 Authentication Required from the SP-SSE. When so challenged by the SP-SSE, the SIP Endpoint **MUST** respond with authentication credentials that are valid within the Operator.

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

19 References

SIP Endpoint / Service Provider Interoperability, „ *SIPconnect 1.1 Technical Recommendation“;* SIP Forum Document Number: TWG-2

[ITU-T E.164] International Telecommunications Union, "Recommendation E.164: The international public telecommunication numbering plan", May 1997, <http://www.itu.int>.

[ITU-T G.168] International Telecommunications Union, "Recommendation G.168:Digital network echo cancellers", January 2007, <http://www.itu.int>.

[ITU-T G.711] International Telecommunications Union, "Recommendation G.711: Pulse code modulation (PCM) of voice frequencies ", November 1988, <http://www.itu.int>.

[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)", January 2007, <http://www.itu.int>.

[ITU-T T.38] International Telecommunications Union, "Recommendation T.38: Procedures for real-time Group 3 facsimile communication over IP networks ", April 2007, <http://www.itu.int/rec/T-REC-T.38/e>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, 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.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., 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.

[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.

[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.

[RFC3389] R. Zopf, "Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)", RFC 3389, September 2002.

[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.

[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.

[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.

20 Document History

Version	Date	Status
1.0	July 29, 2016	Initial public version
2.0	Mai 25, 2020	Updated PŸUR version