

Telefónica O2 Czech Republic, a.s.	Příloha 1 verze: 1.0	Kód_dokumentu B400.TE000002-1			
Bezpečnostní klasifikace:	VEŘEJNÝ	Strana	1	z

ROZHRANÍ PRO SLUŽBY VOIP CONNECT PŘÍLOHA 1

Účel:

Příloha podrobněji popisuje technické specifikace rozhraní v koncových bodech sítě pro poskytování telefonní služby Voice over IP connect a služeb IP Centrex společnosti Telefónica O2 Czech Republic, a.s. nabízených mimo standardní PSTN/ISDN rozhraní přes IP prostředí.

Působnost:

Tento dokument je částí platné technické specifikace B400.TE000002 společnosti Telefónica O2 Czech Republic, a.s.; nesmí se používat samostatně. Specifikace je určena pro informaci technické veřejnosti, zejména pro dodavatele a výrobce koncových zařízení.

Obsah:

- 1 Technická specifikace VoIP účastnického rozhraní SIP UNI – s registrací k SIP serveru 3
- 2 Technická specifikace VoIP účastnického rozhraní SIP NNI – bez registrace k SIP serveru 8
- 3 Technická specifikace VoIP účastnického rozhraní IP-BX - H.323..... 13

1 TECHNICKÁ SPECIFIKACE VOIP ÚČASTNICKÉHO ROZHRANÍ SIP UNI – S REGISTRACÍ K SIP SERVERU

Specifikace VoIP protokolů pro jednotlivé účastníky, kteří jsou registrováni na SIP serveru jako účastnické telefonní číslo.

Specifikace je platná i pro zákaznické brány (Voice- CPG) s účastnickým Z- rozhraním a ISDN BRI rozhraním, dále je platná pro SIP telefony.

Přehled technických předpisů:

- **RFC 3261:** SIP: Session Initiation Protocol, June 2002

The optional Alert-info header described in: RFC 3261 should be supported for the distinctive ringing and priority alert services

Flash based services support

IP phone shall support Flash-based Service Support via INFO Method with a proprietary extension to the INFO method to support flash-based user services such as call waiting, call transfer, three-way calling, and so on. The extension includes the definition of a new value for the *Content-Type* header. The new value is: application/broadsoft.

The application/broadsoft Content-Type allows an endpoint to notify VoIP platform that a flash hook has occurred or to direct an endpoint to play a tone, as specified by the VoIP solution.

The Content-Type of application/broadsoft indicates that a proprietary body is in the message. The body must be in one of the following formats in order for VoIP solution or the endpoint to interpret the intention: (These fields are not case sensitive.)

- event <event name>
- play tone <tone name>
- stop <tone name>

Optionally, the play tone body may contain the following body parts to communicate call waiting calling party identification information. Note that the INFO body is case insensitive.

- Calling-Name:"<calling-name>" where <calling-name> is a string representing the calling party's name
- Calling-Number:<calling-number> where <calling-number> is a string representing the calling party's number The Calling-Name and Calling-Number are always included in the INFO for call waiting as long as the calling party information is available. When the information is not available, the device must populate the calling line identification signal to the analog line with the appropriate unavailable signal. When the calling party information is not available, the Calling-Name and/or Calling-Number fields are not included in the INFO method body. It is possible that the calling number may be available without the calling name and vice versa. When these conditions occur, only the information that is available is included in the INFO method body (that is, it is possible to have a Calling-Number field in the INFO method body without a Calling-Name field and vice-versa).
- When any portion of the calling party information is restricted, the Calling-Name and Calling-Number fields are included in the INFO method body header and are

populated with Private. Note that restricted calling party information overrides unavailable calling party information. When the calling number is restricted and the calling name is unavailable or vice versa, both the Calling-Name and Calling-Number fields are included in the INFO method body and are populated with Private.

The Calling-Number field is sent in the INFO method body with the national format when the calling number and called number are within the same country code.

When the calling number and called number are in different country codes, the Calling-Number field is populated with the E.164 number of the calling party.

The only event currently defined is flashhook (this is not case sensitive).

The only tones currently defined are:

CallWaitingTone1

- CallWaitingTone2
- CallWaitingTone3
- CallWaitingTone4

The only parameter allowed for the stop body is: CallWaitingTone.

- A body with stop CallWaitingTone indicates that the access device should cease applying the call waiting tone regardless of which type of call waiting tone is applied.

The access device should send INFO when a flash is detected on the device.

VoIP platform sends type of INFO with play tone body when a VoIP subscriber has the Flash Call Waiting service assigned and a second call arrives for the VoIP platform subscriber while the subscriber is in an active call. The access device should never send this type of INFO.

Following is an example of INFO with stop body. Note that BroadWorks sends this type of INFO under the following conditions:

- BroadWorks subscriber has Flash Call Waiting service assigned.
- Second call arrives for the VoIP subscriber while the subscriber is in an active call.
- INFO with a play tone body has been sent to the device to apply the appropriate call waiting tone.
- Calling party hangs up prior to the VoIP subscriber answering the waiting call.

The INFO with stop body is not sent when the device answers the call via a flashhook. VoIP platform is expecting the device to implicitly stop the tone upon flashing, to answer the unanswered call. The only time VoIP platform will send the stop tone is when the call waiting caller hangs up before the call waiting party flashes to answer the call. Note that the access device should never send this type of INFO.

- **RFC 3262:** Reliability of Provisional Responses in SIP, June 2002 (PRACK support)

In case located behind a NAT router, the client/terminal should start sending "dummy RTP" data when receiving an "Early Media" answer from SDP, i.e. SDP in provisional response. The dummy data should be sent from the UDP-port where the client expects to receive "early data"

- **RFC 3263:** Session Initiation Protocol (SIP): Locating SIP Servers, June 2002 (DNS SRV redundant server support)
- **RFC 3264:** An Offer/Answer Model with the Session Description Protocol, June 2002

When receiving 180 Ringing, 183 Session Progress or 200 with SDP, the terminal shall open the RTP flows

When receiving 180 Ringing/SDP and then receiving 183 Session Progress/SDP with different/updated SDP the terminal shall use the latest SDP, i.e. that of the 183 Session Progress

When receiving 180 without SDP, the terminal shall provide local ringing tone

- **RFC 3265:** Session Initiation Protocol (SIP)-Specific Event Notification, June 2002
- **RFC 3515:** The Session Initiation Protocol (SIP) Refer Method, April, 2003
- **RFC 3325:** Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, November 2002
- **RFC 3966:** The tel URI for Telephone Numbers, December 2004
- **RFC 2806:** URLs for Telephone Calls, April, 2000
- **RFC 3323:** A Privacy Mechanism for the Session Initiation Protocol (SIP), November 2002
- draft-levy-sip-diversion-08.txt: Diversion Indication in SIP, August 25, 2004
- **RFC 3311:** The Session Initiation Protocol (SIP) UPDATE Method, September 2002
- **RFC 4028:** Session Timers in the Session Initiation Protocol (SIP), April 2005
- draft-ietf-sip-connect-reuse-04.txt: Connection Reuse in the Session Initiation Protocol (SIP), July 14, 2005
- **RFC 3725:** Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP), April, 2004
- **RFC 2976:** The SIP INFO Method, October 2000
VoIP uses a proprietary extension to the INFO method to support flash-based user services. (for details see note *1) in chapter 4)

- draft-levin-mmusic-xml-media-control-03.txt: XML Schema for Media Control, February 15, 2004
- draft-ietf-avt-rfc2429-bis-04.txt: RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+), December 30, 2004
- **RFC 3842:** A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP), August 2004
The client should support Message waiting indication according to RFC 3842
- **RFC 3891:** The Session Initiation Protocol (SIP) "Replaces" Header, September 2004
- **RFC 3892:** The Session Initiation Protocol (SIP) Referred-By Mechanism, September 2004
- draft-ietf-sipping-dialog-package-06.txt: An INVITE Initiated Dialog Event Package for the Session Initiation Protocol (SIP), April 12, 2005
- draft-ietf-sipping-cc-conferencing-07.txt: Session Initiation Protocol Call Control – Conferencing for User Agents, June 3, 2005
- draft-ietf-sipping-conference-package-12.txt: A Session Initiation Protocol (SIP) Event Package for Conference State, July 1, 2005
- draft-ietf-sipping-conferencing-framework-05.txt: A Framework for Conferencing with the Session Initiation Protocol, May 27, 2005
- **RFC 3428:** Session Initiation Protocol (SIP) Extension for Instant Messaging, December 2002
The client should support the MESSAGE Method described in RFC 3428
- RFC 2833: RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, May 2000
- **RFC 2327:** SDP: Session Description Protocol, April, 1998
- **RFC 3266:** Support for IPv6 in Session Description Protocol (SDP), June 2002
- **RFC 3959:** The Early Session Disposition Type for the Session Initiation Protocol (SIP), December 2004
- **RFC 3960:** Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP), December 2004
- **RFC 1890:** RTP Profile for Audio and Video Conferences with Minimal Control, January 1996
- **RFC 3550:** RTP: A Transport Protocol for Real-Time Applications, July 2003

- **RFC 3551:** RTP Profile for Audio and Video Conferences with Minimal Control, July 2003
- **RFC 2617:** HTTP Authentication; Basic and Digest Access Authentication. Note, however that it is only required to support the Digest Access Authentication Scheme.
- **3GPP TS 23.003** The client/terminal **MUST** have the user name in authentication headers in the form of "user@domain" where both the user portion and the host portion is present.
- **RFC 3856** A Presence Event Package for the Session Initiation Protocol (SIP)
- **RFC 3903** Session Initiation Protocol (SIP) Extension for Event State Publication

2 TECHNICKÁ SPECIFIKACE VOIP ÚČASTNICKÉHO ROZHRANÍ SIP NNI – BEZ REGISTRACE K SIP SERVERU

Specifikace VoIP protokolů pro připojení IP PBX a CPG s rozhraním pobočkových ústředěn (PBX) bez registrace IP PBX/CPG k SIP serveru.

Přehled technických předpisů:

RFC 3261 “SIP: Session Initiation protocol”

IP-PBX or CPG must behave as an User Agent but no registration (SIP REGISTER request) must be performed for any of the user behind these nodes.

The solution supports both UDP and TCP transports, but UDP is preferable.

Only SIP INVITE request is supported to establish a session. Other SIP message as MESSAGE, OPTION, SUBSCRIBE and NOTIFY are rejected.

SIP INFO only used to send DTMF numbers

All INVITE's responses are supported (1XX, 2XX, 3XX, 4XX, 5XX and 6XX).

RFC 2806 URLs for Telephone Calls

and RFC 3966 the tel URI for Telephone Numbers

IP-PBX or CPG must support receiving SIP-URIs and TEL-URIs in the concerning fields (REQ URI, TO, FROM, etc). When SIP URI format is used, IP-PBX or CPG must manage any “host name” (domain) used at Operator (VoIP network) level, for instance: +34913392874@operator.com.

IP-PBX or CPG must extract the destination from the “user info” part without forcing to use a specific IP-PBX or CPG “domain”.

Any information sent by the IP-PBX in relation to any user or identity involved in the call (Calling Party Number, Called Party Number, Diversion Information, Transfer Information, etc) must contain a National Significant Number or a number which makes sense inside the VoIP network. Therefore no Alias neither identities with characters other than numbers, will be accepted by VoIP solution.

RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)

RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks.

IP-PBX or IDA must support the standards track RFC 3323, A Privacy Mechanism for the Session Initiation Protocol (SIP), and RFC 3325, Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, to protect the identity of PBX users when inter-working in the VoIP solution.

The IP-PBX or CPG access Interface is treated as untrusted therefore any Calling Party Identity information sent in the FROM or P-Asserted-ID header will be validated by VoIP for any originating call.

RFC 3323 A Privacy Mechanism for the Session Initiation Protocol

Privacy Mechanism could be invoked by means a Prefix dialing in from of Called party, by Business Trunking service configuration at user level and by means of SIP signaling information according to RFC 3323/RFC 2235.

VoIP behavior for Business Trunking is the following according to the SIP signaling:

Originating: Privacy header other than .None, Header or Session.

The initial INVITE contains a Privacy header with a value other than .None, Header, or .Session..

The behavior of VPN BT depends on the called party. The called party may belong to a defined company (destination PBX) or not.

In the INVITE to the terminating PBX User the following header fields are impacted:

- From header: .anonymous<sip:anonymous@anonymous.invalid>
- P-Asserted_Identity header: removed if present
- Privacy header: ignored and removed

In the INVITE to the terminating no PBX User the following header fields are impacted:

The Privacy header is kept as is and no other action is required regarding privacy.

Originating: Privacy Header .None.

The initial INVITE contains a Privacy header with a value .None..

No action is required regarding privacy.

Originating: Privacy header .Header or Session.

The initial INVITE contains a Privacy header with a value .Header or Session.

The behavior of VPN BT depends on the presence of the Privacy header field value .Critical:

1 Privacy Includes .Critical.

VPN BT cannot grant the requested privacy and the call setup is aborted.

2 Privacy does not include .Critical.

VPN BT cannot grant the requested privacy and the call setup continues without the requested privacy.

Terminating call to IP-PBX: Privacy Header .None.

No action is required regarding privacy.

Terminating call to IP-PBX: Privacy Header .User. and/or .Id.

The following header fields are impacted:

- From header: .anonymous.<sip:anonymous@anonymous.invalid>
- P-Asserted_Identity header: removed if present
- Privacy header: removed

Terminating call to Ip-PBX: Privacy Header .Header or Session.

The behavior of VPN BT depends on the presence of the Privacy header field value .Critical.

1 Privacy Includes. Critical.

VPN BT cannot grant the requested privacy and the call setup is aborted.

2 Privacy does not include .Critical.

VPN BT cannot grant the requested privacy and the call setup continues without the requested privacy.

RFC 3311 The Session Initiation Protocol (SIP) UPDATE Method

UPDATE method is not supported.

RFC 3262 Reliability of Provisional Responses in SIP

IP-PBX or CPG must support this RFC

RFC 2833 RTP Payload for DTMF Digits

Access devices should support RFC 2833 as it guarantees reliable delivery of DTMF digits from the access device to the entity collecting the digits.

Otherwise, the VoIP platform collects digits via the RTP stream of packets.

RFC 2976 SIP INFO Method)

could be used to send DTFM digits

T.38 SIP Support for Real-Time Fax

VoIP platform supports T.38. T38 attributes included in the SDP are transparently passed to the associated device.

When interworking with the PSTN using the MGW which supports facsimile/modem bypass (G.711) and Fax Relay (T.38).The MGC 4.2 T.38 fax support requires that the call is first setup as a normal voice connection (e.g. with G.711) before a switchover from voice to T.38 fax is done with SIP Re-INVITE practices.

RFC 3263 Locating SIP Servers

IP-PBX or CPG must support this RFC

RFC 3515 The Session Initiation Protocol (SIP) Refer Method

Not applicable for IP-PBX or CPG.

RFC 3891 The Session Initiation Protocol (SIP) "Replaces" Header**RFC 3892 The Session Initiation Protocol (SIP)**

Referred-BY Mechanism BroadWorks supports this functionality.

RFC 3515/ RFC 3891 /RFC3892

Business Trunking solution does not support call transfer services based on those RFC. When a call transfer is invoked by the PBX user, IP-PBX or PBC connected to an CPG must generated a new complete new call from VoIP platform point of view. Referrer and Refer Targeted (as defined in RFC 3892) must be connected via PBX or CPG capabilities.

Any SIP message associated to this call transfer (NOTIFY, etc) must be sent to the network (VoIP platform)

draft-levy-sip-diversion-08 Call diversion treatment and Diversion Indication in SIP

A Business Trunking IMT user, which is connected to a PBX, receives a call from user A, which is forwarded by the PBX to an off-net destination (user C). Several flavors exist for the PBX to forward the call:

- 1) A new call is set up from the PBX to the off-net user C, where the Request URI and To header field contains the forwarded-to destination and the From header field contains information representing the original called party. This means that the PBX generates complete new call for the diverted call.
- 2) A new call is set up from the PBX to the off-net user C, where the Request URI and the To header field contain the forwarded-to destination, the Diversion header field contains the original called party, and the From header field contains the original calling party. This means that the PBX generates complete new call for the diverted call with Diversion information which is analyzed by the BT service to apply the concerning logic.
- 3) The PBX can respond to the call attempt to user B with SIP Response 302 Moved Temporarily.

RFC-2327 SDP: Session Description Protocol**RFC 3264 An Offer/Answer Model with Session Description Protocol**

An access device (IP-PBX or CPG) must support the following actions:

- An access device must support receiving a subsequent INVITE (Re-INVITE) with a new session description. The device should swap media streams transparently.
- An access device must support receiving an initial INVITE with a session description where the "c" destination addresses for the media streams are set to zero (0.0.0.0). Note that this method of putting a device on hold is deprecated, but must be supported for backwards compatibility. An access device should support receiving an initial INVITE with a session description where the a=inactive attribute is present to indicate a particular media stream is inactive (that is, on hold). The access device should make use of the a=sendonly, a=recvonly, a=inactive, a=sendrecv (default) attribute in the session description it provides, to indicate the disposition of the media it is providing.
- An access device must support receiving a subsequent INVITE (Re-INVITE) with a modified session description where the "c" destination addresses for the media streams are set to zero (0.0.0.0). Note that this method of putting a device on hold is deprecated, but must be supported for backwards compatibility. An access device should support receiving a subsequent INVITE (Re-INVITE) with a modified session description where the a=inactive attribute is present to indicate a particular media stream is inactive (that is, on hold). The access device should make use of the a=sendonly, a=recvonly, a=inactive, a=sendrecv (default) attribute in the session description it provides, to indicate the disposition of the media it is providing.
- An access device must support receiving an initial INVITE with no session description (Null SDP). In this scenario, the device should be able to handle setting up a media connection when it receives an ACK with media. Additionally, the access device should respond with an SDP in the 200 OK response to the INVITE, which contains all of the supported CODECs of the device in the order of preference. An access device should also support receiving an initial INVITE with a session description with SDP but no media lines. An access device should respond with an SDP in the 200 OK response to the INVITE with an SDP with no media lines.
- An access device must support receiving a subsequent INVITE (Re-INVITE) with no session description (Null SDP). In this scenario, the device should be able to handle setting up a media connection when it receives an ACK with media. Additionally, the access device should respond with an SDP in the 200 OK response to the INVITE, which contains all of the supported CODECs of the device in the order of preference.
- An access device must support receiving an ACK to an INVITE, which did not have a session description, with a session description where the "c" destination addresses for the media streams are set to zero (0.0.0.0). Note that this method of putting a device on hold is deprecated, but must be supported for backwards compatibility. An access device should support receiving an ACK to an INVITE, which did not have a session description, with a session description where the a=inactive attribute is present, to indicate a particular media stream is inactive (that is, on hold). The access

device should make use of the a=sendonly, a=recvonly, a=inactive, a=sendrecv (default) attribute in the session description it provides, to indicate the disposition of the media it is providing.

- Upon receiving a subsequent INVITE (Re-INVITE) with no session description, an access device should return a session description that results in connecting the media streams. A device should not return a 200 OK response with a session description where the “c” destination addresses for the media streams are set to (0.0.0.0) or containing an a=inactive attribute, unless it intends to place the call “on-hold”. Note this method of putting a device on hold (c=0.0.0.0) is deprecated, but must be supported for backwards compatibility.

This scenario can happen when the device is placed “on-hold” via an session description where the “c” destination addresses for the media streams are set to zero (0.0.0.0) or contain an a=inactive attribute, and receives a subsequent INVITE (Re-INVITE) with no session description (Null SDP).

- The intention of the subsequent INVITE (Re-INVITE) is to re-establish the media path(s). Therefore, a device should not return a 200 OK response with a session description where the “c” destination addresses for the media streams are set to zero (0.0.0.0) or contain an a=inactive attribute, unless it intends to keep the call “on-hold”.

- An access device must support changing media streams in 18x responses and subsequent 200 OK responses. For calls from an access device to a BroadWorks user, it is noted that the SDP information sent in a 180 Ringing, 183 Session Progress, 200 OK response, and subsequent INVITEs (Re-INVITEs) can all contain different media descriptions. BroadWorks may forward a call from a user to voice mail or transfer from the Auto Attendant to a user, which in both cases alters the media stream.

- Upon receipt of an 18x response with media, the access device should stop providing local ringback and rely on the remote side for its “progress announcements”. This could occur in a no-answer forward scenario or transfer before answer scenario. The access device does not have to support switching from remote ring back to local ring back as BroadWorks will not initiate this transition. However, it is desirable for the access device to support switch from remote to local ring back.

- IP-PBX must be able to packet time negotiation according to “ptime” SDP parameter.

RFC 4028 Session Timers in the Session Initiation Protocol (SIP)

IP-PBX or CPG must support this RFC. Re-INVITE method is used to refresh the session.

RFC-3389. Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)

IP-PBX or CPG must support this RFC

RFC 3265 Session Initiation Protocol (SIP)-Specific Event Notification

Not applicable for IP-PBX or CPG.

RFC 3960 Early Media and Ringing Tone Generation in the Session Initiation Protocol

Not applicable for IP-PBX or CPG.

RFC 3959 The Early Session Disposition Type for the Session Initiation Protocol (SIP)

IP-PBX or CPG must support this RFC

draft-ietf-sip-connect-reuse-04.txt: Connection Reuse in the Session Initiation Protocol

Not applicable for IP-PBX or CPG.

3 TECHNICKÁ SPECIFIKACE VOIP ÚČASTNICKÉHO ROZHRANÍ IP-BX - H.323

Specifikace VoIP protokolů pro připojení IP-PBX s rozhraním H.323

Přehled technických předpisů:

H.323 V4 Packet-based multimedia communications systems

Fast start and fast start with parallel H.245

H.323 Annex E Support for UDP signaling

H.245 Control Protocol for Multimedia Communication

H.225.0/Q.931 RAS, Call Signaling and setup (Call signaling with RAS)

H.245 Tunneling – Encapsulates H.245 messages within H.225/Q.931 messages.

Přenos DTMF – **RFC 2833 nebo H.245** UII (User input indication)

Komunikační módy:

Back-to-back gateway signalling

Interworking gatekeeper/gateway

-----konec přílohy-----