# Vodafone Anlagen-Anschluss Plus (S0/S2M)

# Interface Specification

Version: 1.2
20.04.2020

# Contents

# 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 IETF RFC 2119.

# Contact

Vodafone GmbH
Ferdinand-Braun-Platz 1
40549 Düsseldorf
Germany
Telefon: +49 (0)800 172 1212
Website: www.vodafone.de

# 1 Scope

In the context of Vodafone Anlagen-Anschluss Plus a local gateway also known as Integrated Access Device (IAD) is introduced to offer classical ISDN BRA/PRA access towards end-user while connecting to an IMS core including application server on the network side by using a SIP trunk.

This document describes the basic functionality and the service specific functionality required from the local gateway to support Vodafone's Anlagen-Anschluss Plus service.

This interface specification may be changed at any time. The user of this interface specification has to check for the newest version available from Vodafone GmbH. This interface specification may be superseded in total or in part by the terms of a contract between the individual network user and Vodafone GmbH.

# 2 References

In the case of a conflict between specific requirements in this document with requirements in any of the directly or indirectly referenced documents, the specific requirements of this document are applicable.

## 2.1 Normative References

| | |
|---|---|
| 3GPP TS 24.229 | IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 |
| 3GPP TS 24.407 Rel.7 | PSTN/ISDN simulation services; Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) |
| 3GPP TS 24.504 Rel.8 | PSTN/ISDN simulation services ; Communication diversion (CDIV) |
| 3GPP TS 24.508 Rel.8 | PSTN/ISDN simulation services; Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) |
| RFC 791 | Internet Protocol |
| RFC 2617 | HTTP Authentication: Basic and Digest Access Authentication |
| RFC 2833 | RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals |
| RFC 3261 | SIP: Session Initiation Protocol |
| RFC 3262 | Reliability of Provisional Responses in the Session Initiation Protocol (SIP) |
| RFC 3263 | Session Initiation Protocol (SIP): Locating SIP Servers |
| RFC 3264 | An Offer/Answer Model with the Session Description Protocol (SDP) |
| RFC 3311 | The Session Initiation Protocol (SIP) UPDATE Method |
| 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 |
| RFC 3398 | Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping |
| RFC 3455 | Private Header (P-Header) Extensions to SIP for 3GPP |
| RFC 3550 | RTP: A Transport Protocol for Real-Time Applications |
| RFC 3551 | RTP Profile for Audio and Video Conferences with Minimal Control |
| RFC 4028 | Session Timers in the Session Initiation Protocol (SIP) |
| RFC 4040 | RTP Payload Format for a 64 kbit/s Transparent Call |
| RFC 4566 | SDP: Session Description Protocol |
| SIPConnect 1.1 | Technical Recommendation |

## 2.2 Informative References

| | |
|---|---|
| SIP Trunking Empfehlung 2011 | Bitkom Position Paper "SIP Trunking - Detailempfehlungen zur harmonisierten Implementierung in Deutschland“, 2011. |
| 3GPP ETSI TS 29.163 | Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks (Release 8) or at least ITU-T Q.1912.5 - Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part |
| RFC 2460 | Internet Protocol, Version 6 (IPv6) |

## 2.3 Reference Acquisition

- 3GPP: http://www.3gpp.org
- bitkom: https://www.bitkom.org/Bitkom/Organisation/Gremien/Business-Communications.html
- European Telecommunications Standards Institute: http://www.etsi.org

- Internet Engineering Task Force (IETF) RFCs: http://www.ietf.org
- SIP Forum: http://www.sipforum.org/sipconnect

# 3 Definitions and Abbreviations

## 3.1 Definitions

The definitions in the referenced standards apply.

For the topics covered in this specification the following terminology will be used:

**A-Number:** this is the caller, also named the originator of the call. Where referred to in this document the A-number is understood to be in unknown (national) format.

**B-Number:** represents the dialed destination or the called party number. Where referred to in this document the B-number is understood to be in unknown (national) format.

**C-Number** can have to meanings:

1). In originating call cases represents the end receiver in case of call forwarding call, i.e. the party to which the B-number has forwarded the call;

2). In terminating call cases represents PBX user answering a call coming to another PBX user (from the same PBX!).

Where further referred to in this document, the B-number is understood to be in unknown (national) format.

**A-Side:** this is the side of the originating user from where the A-number initiates the call.

**B-Side:** in case of normal call case scenarios this is the side of the terminating user and where the call ends (the location of B-number) - in case of call forwarding scenarios this is the side where the call will be forwarded to a third party (C-side).

**C-Side:** in Call Forwarding scenarios this is the side where the call will be terminated after forwarding is initiated at B-side.

**HN:** PBX Header Number. It represents given PBX trunk and is not dialable number. It does not contain LAC, neither national access code nor extension number - e.g. from number 069 2169 0, HN is ‘2169’

**Public HN:** this is the HN preceded by LAC - e.g. from number 069 2169 0, Public HN is ’69 2169’

**PN:** PBX Pilot number, also known as ‘Default extension’, “Operator 0” or “Operator Seat”. It is a dialable number composed as follows: <LAC><HN><X>, where ‘X’ is the default extension number (usually 0, but may be also another number - e.g. from number 069 2169 0, PN is 69 2169 0

**PBX Full number** has the following two cases:

1). Dialing the PBX HN and consecutively dialing the extension

<LAC><HN> + <PBX-Extension> - e.g. 69 2169 + 1234

2). **DDI** - Direct-Dial-In number. Also referred to as GN (Geographical number). This is the full number to be dialed in order to reach the end point (PBX user). It has the following format:

<LAC><HN><PBX-Extension> - e.g. 69 2169 5678

**SN:** Subscriber number.

SN = <HN> + <PBX-Extension> - e.g. 69 2169 5678

**Dialable Numbers:** These are numbers in all formats according to table in subclause 6.3.2.1

## 3.2 Abbreviations

The definitions in the referenced standards apply.

| | |
|---|---|
| AES | Advanced Encryption Standard |
| ALG | Application Layer gateway |
| BRA | Basic Rate Access |
| CC | Country Code |
| CLIP | Calling Line Identification Presentation |
| CLIR | Calling Line Identification Restriction |
| COLP | Connected Line Identification Presentation |
| COLR | Connected Line Identification Restriction |
| DDI | Direct Dial-In (also known as Direct Inward Dialing) |
| DES | Data Encryption Standard |
| DTMF | Dual Tone Multi Frequency |
| FQDN | Fully Qualified Domain Name |
| GW | Gateway |
| IAD | Internet Access Device (also referred to as 'Local GW' in this specification. |
| LAC | Local Area Code |
| MPLS | Multiprotocol Label Switching |
| NAT | Network Address Translation |
| OIP | Originating Identification Presentation |
| OIR | Originating Identification Restriction |
| PBX | Private Branch Exchange |
| PN | Pilot Number |
| RSA | Public-key cryptosystem (named after Rivest, Shamir and Adleman) |
| SBC | Session Border Controller |
| SDES | Session Description Protocol Security Description |
| SDP | Session Description Protocol |
| SIP | Session Initiation Protocol |
| SN | Subscriber Number |
| SRTP | Secure Real-time Transport Protocol |
| SRV | Services Resource Record |
| TCP | Transport Control Protocol |

| | |
|---|---|
| TIP | Terminating Identification Presentation |
| TIR | Terminating Identification Restriction |
| UDP | User Datagram Protocol |
| VF | Vodafone GmbH |
| VPN | Virtual Private Network |

# 4 General overview

The following diagram (Figure 1) depicts several possible deployment scenarios for the local gateway in the Anlagen-Anschluss Plus product.

From access architecture point of view three main deployments are foreseen:

- Local Gateway used for interconnection of PBX with BRA (n x S0).
- Local Gateway used for interconnection of PBX with single S2M PRA interface.
- Local Gateway used for interconnection of PBX with multiple S2M PRA interfaces.

***Note:*** for Phase 1 of the project only Scenario 2 will be considered and implemented. Scenario 3 is planned for Phase 2 or later.

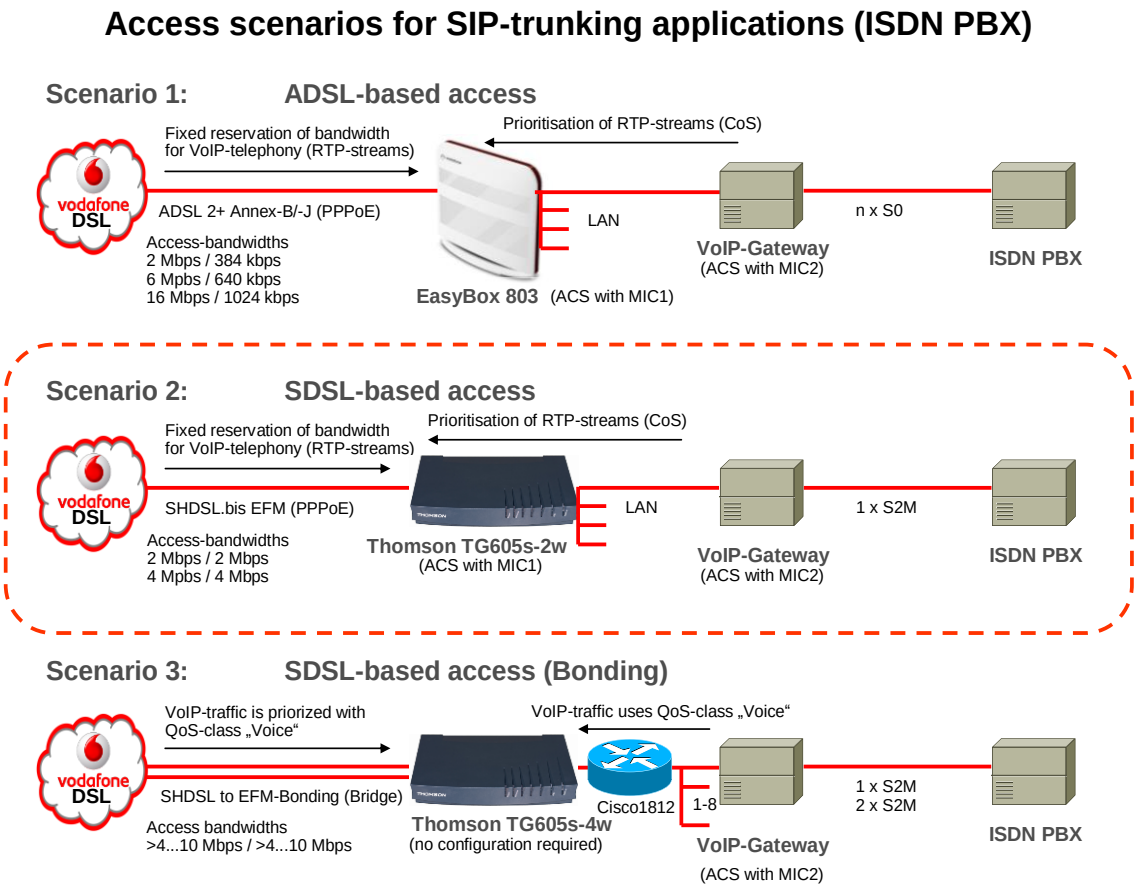



Figure 1 Anlagen-Anschluss Plus access scenarios

# 5 Support

## 5.1 Supported standards

The local GW SHALL comply with the standards in subclause 2.1 and SHOULD comply with the standards in subclause 2.2.

## 5.2 Supported protocol stack

The Local GW SHALL support the SIP Protocol over UDP and SHOULD support the SIP Protocol over TCP.

For the first phase of Anlagen-Anschluss Plus only UDP support is mandatory.

## 5.3 Supported codecs

Following codecs SHALL be supported and requested according the priority order below (topmost with highest priority):

1. G.711 (a-law)

2. G.729A

3. G.726

4. clearmode (64kbit/s transparent call)

64kbit/s transparent call according RFC4040 is supported but also depends on the capabilities of the remote party.

To provide FAX support the gateway SHALL as well support T.38 fax relay.

## 5.4 Supported end user feature list

### 5.4.1 CLIP (OIP, B-side)

CLIP is a service offered to B-side (the terminating user). It provides B-side with possibility to receive calling line identity information containing the identity of A-side (the originating user).

Local gateway SHALL derive the value of 'Privacy' header field from the incoming INVITE, analyze it and set the corresponding value into DSS.1 'Presentation indicator' field according to 3GPP TS 24.407 Rel.7 specification.

For Anlagen-Anschluss Plus, in case of PBX Terminating calls, the network will provide CLI to the local gateway in the 'From' header field. Therefore the local gateway SHALL retrieve the CLI information from the 'From' field.

Incoming INVITE (to B-side local GW) with CLI (A-side without CLIR) will have syntactically correct 'From' header field which may contain any type of number (e.g. national unknown, international, etc…). The local gateway should be able to receive and process these different types of number formats.

Example of incoming INVITE where from Header is in national number format:

```
INVITE sip:+4971193309821@ims_sip_domain.de;user=phone SIP/2.0
From: <sip:0511124554820@ims_sip_domain.de;user=phone>;tag=abc
To: <sip:071193309821@ims_sip_domain.de;user=phone>
Accept: application/sdp,application/dtmf-relay
Contact: <sip:SBC_session_id@sbc_ip_address:udp_port;user=phone>
```

```
Privacy: none
CSeq: 1 INVITE
```

Example of incoming INVITE where from Header is in international number format:

```
INVITE sip:+4971193309821@ims_sip_domain.de;user=phone SIP/2.0
From: <sip:+49511124554820@ims_sip_domain.de;user=phone>;tag=abc…
To: <sip:071193309821@ims_sip_domain.de;user=phone>
Accept: application/sdp,application/dtmf-relay
Contact: <sip:SBC_session_id@sbc_ip_address:udp_port;user=phone>
Privacy: none
CSeq: 1 INVITE
```

Further information about the content of 'From' field is specified in subclause 6.3.1.2

### 5.4.2 CLIR (OIR, A-side)

CLIR is a service offered to A-side (the originating user). It gives A-side possibility to restrict its own calling line identity information and not present it to the B-side (the terminating user).

Same as for CLIP service, the local gateway SHALL map the DSS.1 'Presentation indicator' field of 'Calling party number' information element into corresponding 'Privacy' header according to 3GPP TS 24.407 Rel.7 specification. For CLIR service that will mean interworking of "presentation restricted" parameter on DSS.1 side into 'Privacy' header set to 'id' or 'user;id'. Thus, network-provided privacy as described in RFC3323 (Section 3.3) and RFC3325 (Section 7) will be achieved. The 'From' header SHALL be left unmodified and SHALL be populated with the CLI of the A-side as described in subclause 5.4.1.

Further information about the format of 'From' field is specified in subclause 6.3.1.2.

Outgoing INVITE (direction local gateway to network) from PBX user requesting CLIR SHALL have the following format:

```
INVITE sip:071193309821@ims_sip_domain.de;user=phone SIP/2.0
From: <sip:051112455480@ims_sip_domain.de;user=phone>;tag=abc…
To: <sip:071193309821@ims_sip_domain.de;user=phone>
Accept: application/sdp,application/dtmf-relay
Contact: <sip:0511124554820@gw_ip_address:5060;user=phone>
P-Preferred-Identity: <sip:051112455480@ims_sip_domain.de;user=phone>
Privacy: id(;user)
Content-Type: application/sdp
CSeq: 22 INVITE
Max-Forwards: 70
```

***Note:*** *usage of 'user' privacy value is optional.*

*Incoming INVITE (direction network to local gateway) towards called party will have the following format:*

```
INVITE sip:071193309821@ims_sip_domain.de  SIP/2.0
From: Anonymous <sip:anonymous@anonymous.invalid>;tag=abc…
To: <sip:071193309821@ims_sip_domain.de;user=phone>
Accept: application/sdp,application/dtmf-relay
Contact: <sip:sbc_ip_address:5060;user=phone>
Content-Type: application/sdp
CSeq: 22 INVITE
```

```
Max-Forwards: 70
```

***Note:*** *Alternatively R-URI may contain 'user=phone' parameter. Local GW SHALL support both options in order to assure future proof interworking.*

### 5.4.3 COLP (TIP)

From functional point of view, COLP is a feature applied to the PBX user when acting as call initiator (calling party). In order for this functionality to be implemented in Anlagen-Anschluss Plus product, certain header and parameter mappings (SIP to ISDN/DSS1 and vice versa) should take place in local gateway.

The following rules SHALL apply in case of PBX Originating call:

- On B-side (terminating user) in order for COLP to be provided, the information received in 'Connected number' information element from the PBX SHALL be inserted into 'P-Preferred-Identity' header in '200 OK' message. The 'Presentation indicator' field of the 'Connected number' information element shall be mapped into 'Privacy' header according to 3GPP TS 24.508 Rel.8.

'200 OK' Message providing COLP information sent from local gateway on B-Side (Called party gateway) to network:

```
Status-Line: SIP/2.0 200 OK
Content-Type: application/sdp
CSeq: 1 INVITE
From: <sip: 0511124554820@ims_sip_domain.de;user=phone>;tag=SDd1q1801
To: <sip:071193309821@ims_sip_domain.de;user=phone>;tag=436B
P-Preferred-Identity: <sip: 071193309827@ims_sip_domain.de;user=phone>
Privacy: none
```

The following rules SHALL apply in case of PBX Originating call:

- On A-side (calling party gateway) in order for COLP to be derived and following the recommendations from 3GPP TS 24.508 Rel.8, the local GW SHALL fetch the information from 'P-Asserted-Identity' header field in the '200 OK' messages on SIP side and properly map it to 'Connected number' information element on ISDN/DSS1 side

'200 OK' Message coming to local GW (calling party gateway) containing COLP information:

```
Status-Line: SIP/2.0 200 OK
Content-Type: application/sdp
CSeq: 1 INVITE
From: <sip: 0511124554820@ims_sip_domain.de;user=phone>;tag=SDd1q1801
To: <sip:071193309821@ims_sip_domain.de;user=phone>;tag=436B
P-Asserted-Identity: <sip: 071193309827@ims_sip_domain.de;user=phone>
Privacy: none
```

Where:

A-number (Calling line): 0511124554820

B-number (Called line): 071193309821

C-number (Connected line): 071193309827

### 5.4.4 COLR (TIR)

From functional point of view, COLR is a feature used by the PBX end user when being in the role of call receiver (called party). It is applied if the PBX wishes to override the default network settings and prevent the presentation of the connected number (the terminating identity).

- On B-side (terminating user) in case of PBX Terminating call, the local gateway shall interwork the DSS.1 “Connected number’ information element in ISDN/DSS1 connect message into ‘P-Preferred-Id’ parameter in ‘SIP 200 OK’ message and set ‘Privacy’ header to ’Id’ in case ‘Presentation indicator’ is set to ‘Restricted’ according to 3GPP TS 24.508 Rel.8.

B-side: ‘200 OK’ Message sent from local GW (the gateway of the B-number) according to COLR rules:

```
Status-Line: SIP/2.0 200 OK
Content-Type: application/sdp
CSeq: 1 INVITE
From: <sip: 0511124554820@ims_sip_domain.de;user=phone>;tag=SDd1q1801
To: <sip:071193309821@ims_sip_domain.de;user=phone>;tag=436B
P-Preferred-Identity: <sip: 071193309827@ims_sip_domain.de;user=phone>
Privacy: Id
```

Where:

A-number (Calling line): 0511124554820

B-number (Called line): 071193309821

C-number (Connected line): 071193309827

- On A-side (originating user) the local gateway will receive the ‘200 OK’ message without “P-Asserted-Identity” header, because A-SBC will strip it out based on the policy implied in case of existing privacy header.

A-side: the corresponding ‘200 OK’ Message arriving at local GW (calling party gateway) according to COLR rules:

```
Status-Line: SIP/2.0 200 OK
Contact: <sip:+49211123456@pbx-ip-address;user=phone>
Content-Type: application/sdp
CSeq: 1 INVITE
From: <sip: +49511124554820@ims_sip_domain.de;user=phone>;tag=SDd1q1801
To: <sip:+4971193309821@ims_sip_domain.de;user=phone>;tag=436B
```

### 5.4.5 CALL FORWARDING

The gateway shall interwork DSS.1 ‘Redirecting number’ information element into SIP ‘Diversion’ header to indicate a forwarding call initiated by the ISDN PBX. The gateway should follow the rules described in 3GPP TS 24.504 Rel.8.

```
INVITE sip:02115349900@ims_sip_domain.de;user=phone SIP/2.0
From: <sip:+49511124554820@ims_sip_domain.de;user=phone>;tag=abc
To: <sip: +492115349900@ims_sip_domain.de;user=phone>
Accept: application/sdp,application/dtmf-relay
Contact: <sip:+4971193309821@gw_ip_address:5060;user=phone>
Diversion:
<sip:+4971193309821@ims_sip_domain.de;user=phone>;reason=”…”
P-Preferred-Identity: <sip: +497119330980@ims_sip_domain.de;user=phone>
Privacy: none
```

```
CSeq: 22 INVITE
Max-Forwards: 70
```

| | |
|---|---|
| A-number (Calling line): | 0511124554820 |
| B-number (Called line/forwarding party): | 071193309821 |
| C-number (Forwarded to number): | 02115349900 |
| Pilot Number: | 07119330980 |

In case that the PBX is not capable of providing redirecting number, the local gateway should treat this call as an ordinary originating PBX call. The 'Diversion' header should not be present and 'R-UR'I and 'To' headers should contain the forwarded to number (C-number). The 'From' filed should contain either the forwarding party (B-number) or the originator of the call (A-number):

```
INVITE sip: 02115349900@ims_sip_domain.de;user=phone SIP/2.0
From: <sip: 071193309821@ims_sip_domain.de;user=phone>;tag=abc
To: <sip: 02115349900@ims_sip_domain.de;user=phone>
Accept: application/sdp,application/dtmf-relay
P-Preferred-Identity: <sip: 07119330980@ims_sip_domain.de;user=phone>
Privacy: none
CSeq: 22 INVITE
Max-Forwards: 70
```

Or

```
INVITE sip: 02115349900@ims_sip_domain.de;user=phone SIP/2.0
From: <sip: +49511124554820@ims_sip_domain.de;user=phone>;tag=abc
To: <sip: 02115349900@ims_sip_domain.de;user=phone>
Accept: application/sdp,application/dtmf-relay
P-Preferred-Identity: <sip: 07119330980@ims_sip_domain.de;user=phone>
Privacy: none
CSeq: 22 INVITE
Max-Forwards: 70
```

The local gateway should map the reason for the diversion according to RFC 5806, chapter 9.1.

### 5.4.6 Dialling options

Features like emergency call, local dialing, special number routing (free-call, shared-cost or premium rate services) require transparent mapping of dialed digits from DSS.1 called party number parameter into Request-URI. No number normalization shall be applied by the local gateway.

### 5.4.7 Trunk/gateway identification

To support PBX identification on network side the gateway shall be able to use a static source IP address in case of Vodafone corporate access or IP- VPN and a 'P-Preferred Identity' header containing the pilot number assigned to the PBX from where calls are initiated.

# 6 Adressing/Routing and formats

## 6.1 NAT traversal

A Network Address Translation (NAT) device may be located between the local gateway and the IMS Core. NAT devices are primarily used in combination with fixed broadband access. Only NAT devices outside the borders of IMS Core are considered, i.e. NAT devices are assumed to be located at the subscriber's site or in the access network. If there are multiple NAT devices in either of these locations, it is assumed that their effect sums up in such a way that they can be treated as a single NAT.

The general handling of NAT traversal for signaling messages is specified in 3GPP TS 23.228 and 3GPP TS 24.229.

For the first phase of Anlagen-Anschluss Plus, the local GW does not have to provide SIP NAT ALG functionality. The SBC will handle this function instead.

However, the local gateway SHOULD support procedures for NAT traversal and procedures for protected signaling messages as specified in 3GPP TS 33.203 when applicable.

Also, the local gateway MAY use STUN Binding Requests as a keep-alive mechanism to maintain NAT bindings for signaling flows over UDP, or CRLF as a keep-alive mechanism to maintain NAT bindings for signaling flows over TCP as specified in RFC 5626.

Local gateway SHOULD support configurable ports for SIP signaling and RTP.

For detail procedures to keep the NAT binding and firewall pinholes open for signaling traffic and media, see ETSI TR 187 008.

## 6.2 SBC detection

SBC node is for local gateway the access point to IMS Core network for SIP signaling procedures. The local gateway sends and receives SIP signaling to and from SBC only.

For Anlagen-Anschluss Plus couple of SBC node pairs working in HA (High Availability) mode will be deployed in two different locations across Germany to achieve geo-redundancy and load sharing.

### 6.2.1 SBC detection method

Each local gateway will have a serving (home) SBC Cluster. The local gateway SHALL resolve the serving SBC Cluster IP address via external DNS query. This SHALL be done via DNS SRV records according to RFC 3263. For that purpose in the local gateway an alias will be provisioned. This alias will be resolved by external DNS (via SRV records with different priority) and will always return two IP addresses – the first will be the primary IP address of home SBC Cluster. The second will be the redundant SBC Cluster IP address.

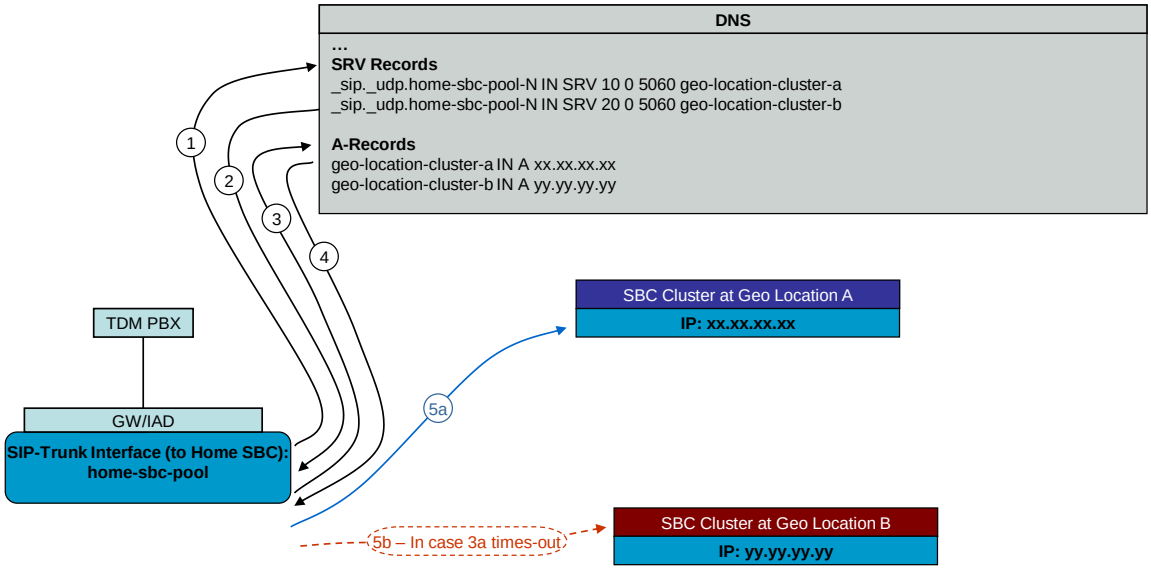
In normal conditions the local gateway SHALL always use the ‘learned’ primary IP address for SIP signalling. The Secondary should be used according to the rules specified in the next subclause 6.2.2.

### 6.2.2 Actions in local gateway at loss of contact with SBC

As already written in the previous subclause, local gateway SHALL always send the SIP request messages to the primary IP address of home SBC Cluster. Only in case of timeout (the timer SHALL be configurable) the request messages should be sent to the secondary IP address.

For phase 1 of Anlagen-Anschluss Plus this should be a stateless mechanism, i.e. for calls coming after timeout expiry of a previous call the SIP requests SHALL still be sent to the primary address and only on timer expiry – to the secondary IP address. Direct requests to the Secondary IP address SHALL NOT be sent.

***Note:*** *Possible implementation of stateful mechanism can be re-considered during the next phases of the project.*




1. **DNS SRV Query** – Name: **_sip._udp.home-sbc-pool-N**?
2. **DNS Response** – name of Serving SBC Clusters is ***geo-location-cluster-a*** (the Primary with lower priority) and name of standby SBC Cluster is ***geo-location-cluster-b***
3. **DNS A Record Query –** Host address?
4. **DNS Response** - IP Addresses of the SBC Clusters (**xx.xx.xx.xx** as serving/home SBC address and **yy.yy.yy.yy** as secondary/redundant SBC IP Address

5a. **SIP INVITE** Message to Serving SBC Cluster (sent to Primary IP address).

5b. **SIP INVITE** Message to Redundant SBC Cluster (sent to Secondary IP address) in case of no answer from Primary IP and time-out.
Secondary IP address is of the redundant SBC Cluster in the other geo location.

Figure 2: SBC Detection via SRV Record query.

# 6.3 Addressing formats

### 6.3.1 Numbering formats for incoming (terminating) calls (from network to local gateway)

*The default format for Public Identities is a SIP URI with the user part in E.164 format:*

*sip: +49<subscriber-number>@ims_sip_domain.de*

*For PBX terminating calls, this format is used in all headers which carry Public Identity.*

#### *6.3.1.1 'Request-URI' format*

*The user part of the 'R-URI' will be populated with number address information corresponding to the public identity of the called PBX entity. It will*

*be always in E.164 number format and can contain either DDI number or PN (Pilot Number):*

*e.g.* *sip: +49691234567@<ims_sip_domain.de>*

*e.g.* *sip: +496912340@<ims_sip_domain.de>*

*The host part of 'R-URI' will contain the PBX Service domain.*

#### *6.3.1.2 'From' header field format*

- If privacy is not required or the calling user is not using CLIP No screening feature, the 'From' field SHALL contain telephone numbers in either unknown (national, with leading '0') or international (E.164) formats:

e.g. sip: +49691234567@<ims_sip_domain.de>

or sip: 0691234567@<ims_sip_domain.de>

- In case Privacy is required (either CLIR Permanent or CLIR temporary at A-side), the 'From' field in an INVITE message arriving at B-side local GW (terminating PBX call) may contain anonymous information. The format provided from the network will follow the recommendations in RFC 3323 and RFC 3325:

From: "Anonymous" sip:anonymous@anonymous.invalid;user=phone

or

From: "Anonymous" <sip:anonymous@anonymous.invalid;>

*To avoid interworking problems, the network SHALL be able to provide and the local GW SHALL support anonymous 'From' header field in both formats: with 'user=phone' parameter and without it.*

*For Anlagen-Anschluss Plus service, the preferred option is anonymous 'From' header without 'user=phone' parameter.*

- In case calling party is using CLIP No Screening number, the 'From' filed can contain any number combination.

#### *6.3.1.3 'To' header field format*

'To' field SHALL contain the dialed number and could be either in unknown (national) or international (E.164) format:

e.g. sip: +49691234567@<ims_sip_domain.de>

or sip: 0691234567@<ims_sip_domain.de>

#### *6.3.1.4 'P-Asserted-Identity' header field format*

In standard scenarios 'P-Asserted-Id' is not sent from network to local gateway. It is a Vodafone requirement that 'P-Asserted-Identity' shall not presented to the terminating client side and therefore it will be stripped out by the SBC.

However, certain product or services still demand the presence of 'P-Asserted-Id'. Therefore the following rules SHALL apply:

- For SIP Methods there will be no ‘P-Asserted-Identity’ sent from the network towards the local gateway.
- For SIP Responses ‘P-Asserted-Identity’ will be allowed in order to facilitate certain functionality (e.g. COLP/COLR).

### 6.3.2 Numbering formats for outgoing calls

The following rules should apply for PBX originating calls:

#### *6.3.2.1 ‘R-URI’ format*

The user part of the R-URI should be populated with number address information according to the table below:

| | |
|---|---|
| 1 | Short Number (Private Numbering Plan) |
| 2 | Special Number (Service Number) |
| 4 | NATIONAL_ACCESS_CODE + Special Number (Service Number) |
| 5 | INTERNATIONAL_ACCESS_CODE + CC + Special Number (Service Number) |
| 6 | "+"CC + Special Number (Service Number) |
| 8 | Emergency Number |
| 9 | NATIONAL_ACCESS_CODE + LAC + SN (fixed national) |
| 10 | NATIONAL_ACCESS_CODE + NDC + SN (mob national) |
| 11 | SN (PSTN Local Dialling) |
| 12 | INTERNATIONAL_ACCESS_CODE + CC + LAC + SN (fixed national) |
| 13 | INTERNATIONAL_ACCESS_CODE + CC + NDC + SN (mob national) |
| 14 | INTERNATIONAL_ACCESS_CODE + CC + other country number |
| 15 | "+"CC + LAC + SN (fixed national) |
| 16 | "+"CC + NDC + SN (mob national) |
| 17 | "+"CC + other country number |

The host part of ‘R-URI’ should be predefined in the local gateway and will be equal to the Anlagen-Anschluss Plus service domain.

Additionally, SIP-URI parameter “user=phone” SHALL be added.

Example for R-URI in unknown (national) format:

Request-Line: INVITE sip:0691234567@ims_sip_domain.de;user=phone

#### *6.3.2.2 ‘From’ header field format*

The ‘From’ field is usually used to provide caller identification. However, if Privacy is required from the calling user or the PBX has active CLIP No Screening feature, the content of the ‘From’ header is not a relevant information any more.

- If privacy is not required or the calling user is not using CLIP No screening feature, the ‘From’ field should contain telephone numbers in either unknown (national) or international (E.164) formats:

e.g. sip: +49691234567@<ims_sip_domain.de>

or sip: 0691234567@<ims_sip_domain.de>

From billing point of view the content of 'From' header field will also be used as served party.

The following requirements SHALL apply for a correct reproduction in the detail bill:

- The number in national unknown format SHALL be presented with 0 in front of the NDC

or

- The number in International format SHALL be presented with either '00' or '+' in front of the Country code.

If the number format is different, the detail bill might be erroneous. The same applies to the diversion header for the forwarding scenario.

- In case Privacy is required, the 'From' field SHALL still contain A-side CLI information as described in the bullet above and explained in clause 5.4.2.

- In case the calling party is using CLIP No Screening service, the 'From' field can contain any syntactically valid information. Nevertheless, the information carried in the 'From' header will still be used for generating CDRs, which will be used later on to generate detail bill information.

#### *6.3.2.3 'To' header field format*

'To' field should contain the dialed number and should be either in unknown (national) or international (E.164) format:

e.g. sip: +49691234567@<ims_sip_domain.de>

or sip: 0691234567@<ims_sip_domain.de>

#### *6.3.2.4 'P-Asserted-Identity' header field format*

For Anlagen-Anschluss Plus no 'P-Asserted-Identity' should be provided in the initial INVITE setting up originating call.

Even if provided, it will be treated as not trustable.

#### *6.3.2.5 'P-Preferred-Identity' header field format*

In Anlagen-Anschluss Plus each PBX will have one unique Pilot number assigned. This pilot number will be provisioned in PBX and in SBC and will be used for PBX validation (along with other methods, not mentioned in this specification).

'P-Preferred-Identity' will be used to convey the above mentioned Pilot number. Therefore in case of originating call the local gateway (A-side) SHALL generate 'P-Preferred-Id' containing the Pilot number and it SHALL be present in each 'INVITE' establishing or modifying a call session.

'P-Preferred-Id' SHALL be also present in SIP Responses sent from B-side local gateway to core network. This is necessary in order to facilitate the implementation of COLP feature. In SIP Responses 'P-Preferred-Id' SHALL contain the connected line information. For further details see subclause **Error! Reference source not found.** COLP.

The 'P-Preferred-Id' in SIP responses will be latter used as 'P-Asserted-Id' within the core network and in the call leg to A-side.

P-Preferred-Id should be always in international E.164 format during session setup (initial 'INVITE') and in the '200 OK' messages. SIP URI parameter "user=phone" SHALL always be included.

#### *6.3.2.6 'Diversion' header field format*

TDM PBXs might have different behavior with regards to Call Forwarding scenarios. In some cases they can provide Redirecting Number and thus indicate the PBX extension from where the call forwarding is initiated. In such cases, when local gateway detects 'Redirecting Number' information element on DSS1/ISN side it SHALL be properly mapped to 'Diversion' header and included in the forwarding INVITE send to network.

The format of INVITE with 'Diversion' header and further details are presented in subclause 5.4.5.

'Diversion' header will be handled transparently and will be presented in the detailed bill together with P-A-Id (PN and Ext. number). In case present, 'Diversion' will replace 'From' header in the detailed bill.

# 7 'Regulatory requirements, e.g. emergency call

## 7.1 Emergency calls

The gateway shall be able to detect emergency call request, e.g. by Request-URI used (110,112). In case of emergency call the gateway shall not apply any called party number manipulation, but transparently use the received called number.

## 7.2 Special Numbers

Special numbers (e.g. 115, 116) are routed to predefined interconnection points of Dt. Telekom and are always delivered in the defined standard format. In order to be routed properly, the local gateway SHALL always pass the special number unchanged (as dialed).

# 8 Special arrangements on SIP methods

## 8.1 IMS Registration

The gateway shall be capable to support IMS registration using digest authentication. However this functionality is not required in the first deployment of the Anlagen-Anschluss Plus service. Therefor IMS registration shall be a configurable parameter to be switched on/off.

# 9 Timer configuration

The local GW should support the SIP timers according to RFC 3261 and RFC 4028

# 10 Capabilities

## 10.1 Basic call scenario description for originating and terminating voice calls

### 10.1.1 Originating call

The local GW should initiate the call with the following mandatory parameters:

- SIP Header “P-Preferred-Id” present and with content according to subclause 6.3.2.5
- The offered codec list should be as specified in subclause 5.3

PBX Originating with G.711 codec

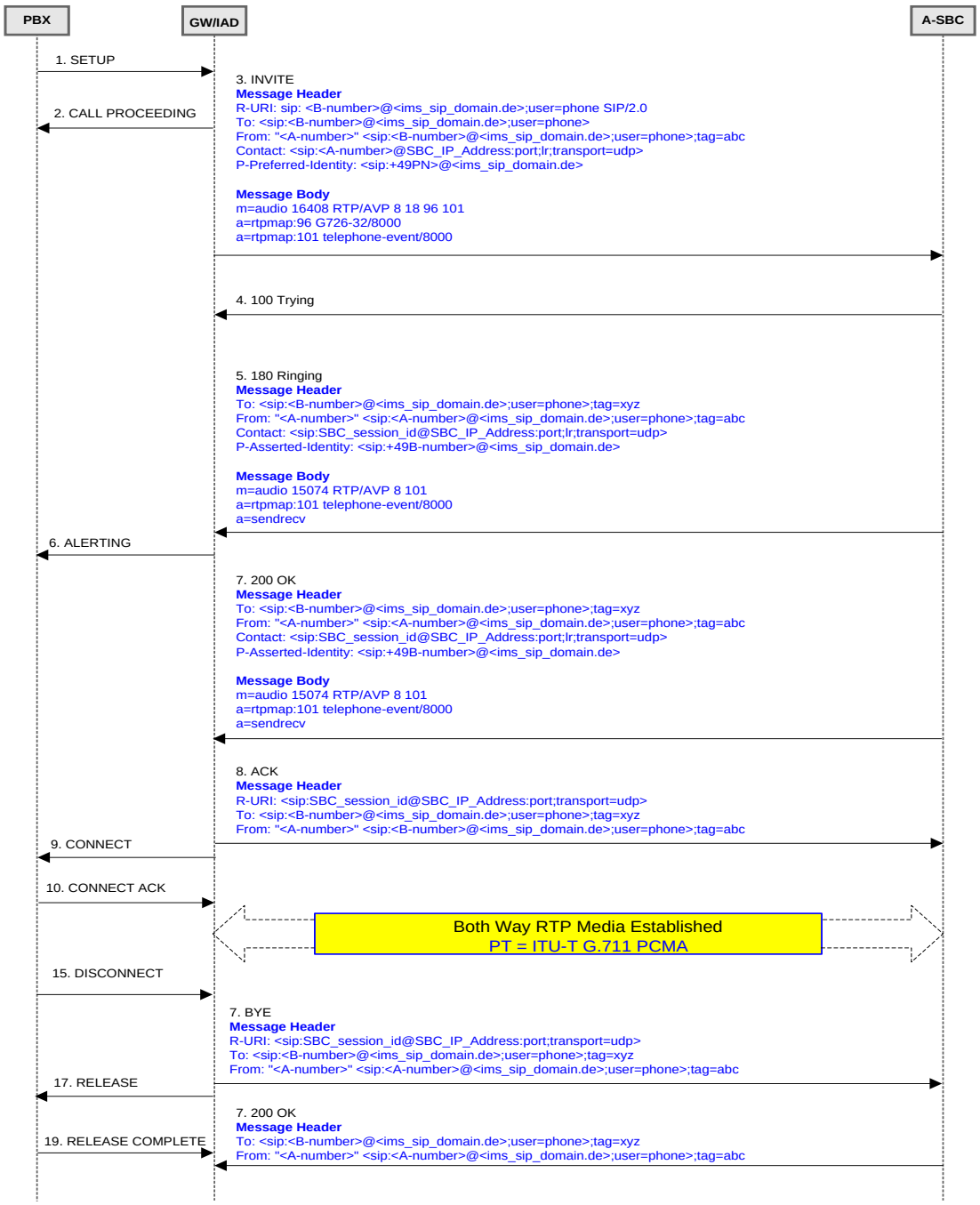



Figure 3 PBX Originating call with G.711 codec

### 10.1.2 Terminating call

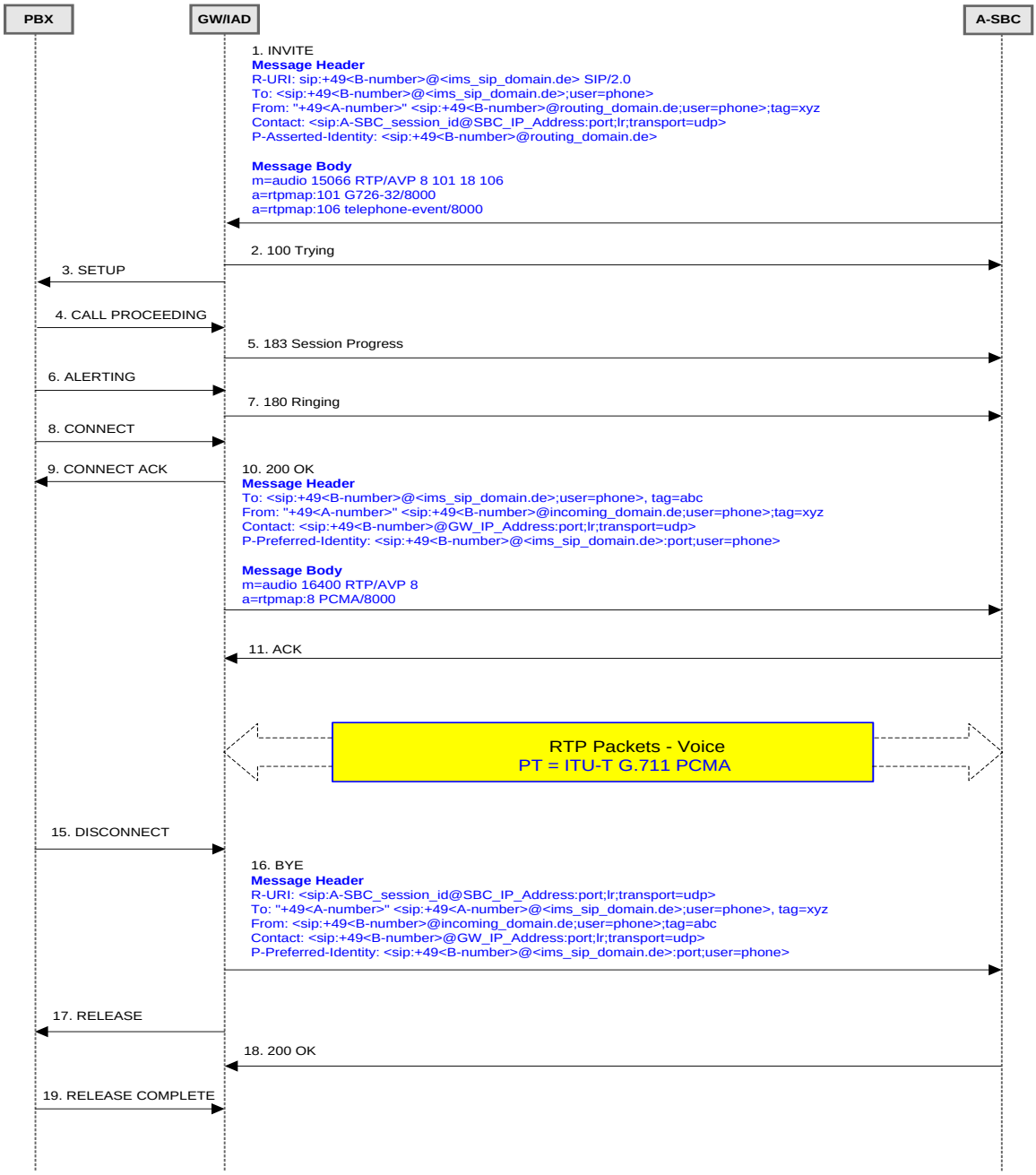



Figure 4 PBX Terminating call

## 10.2 FAX Calls

The local GW should support fax using G.711 and T.38. Fallback from T.38 to G.711 should be supported as well.

The transmission of Fax SHALL be supported according to the ITU-T T.30 method (also called “pass-through” and using G.711 as voice codec).
On request ITU-T T.38 method MAY also be provided as option in the session negotiation. There, the following guidelines apply:

- The SIP/SDP call establishment procedures of ITU-T T.38 Annex D for facsimile and voice over IP environment apply for all connection scenarios. According to those, first a voice connection, e.g. with the G.711 codec for T.30 passthrough facsimilie, has to be established successfully prior to T.38 session negotiation and upon negotiation failure for T.38 communication a fallback to T.30 takes place.

- The SIP/SDP call establishment procedures of ITU-T T.38 Annex D for facsimile-only environments are not supported for connection scenarios which involve the media gateway, i.e. connections crossing the border to the ISDN.

### 10.2.1 Originating Fax call with G.711 Codec

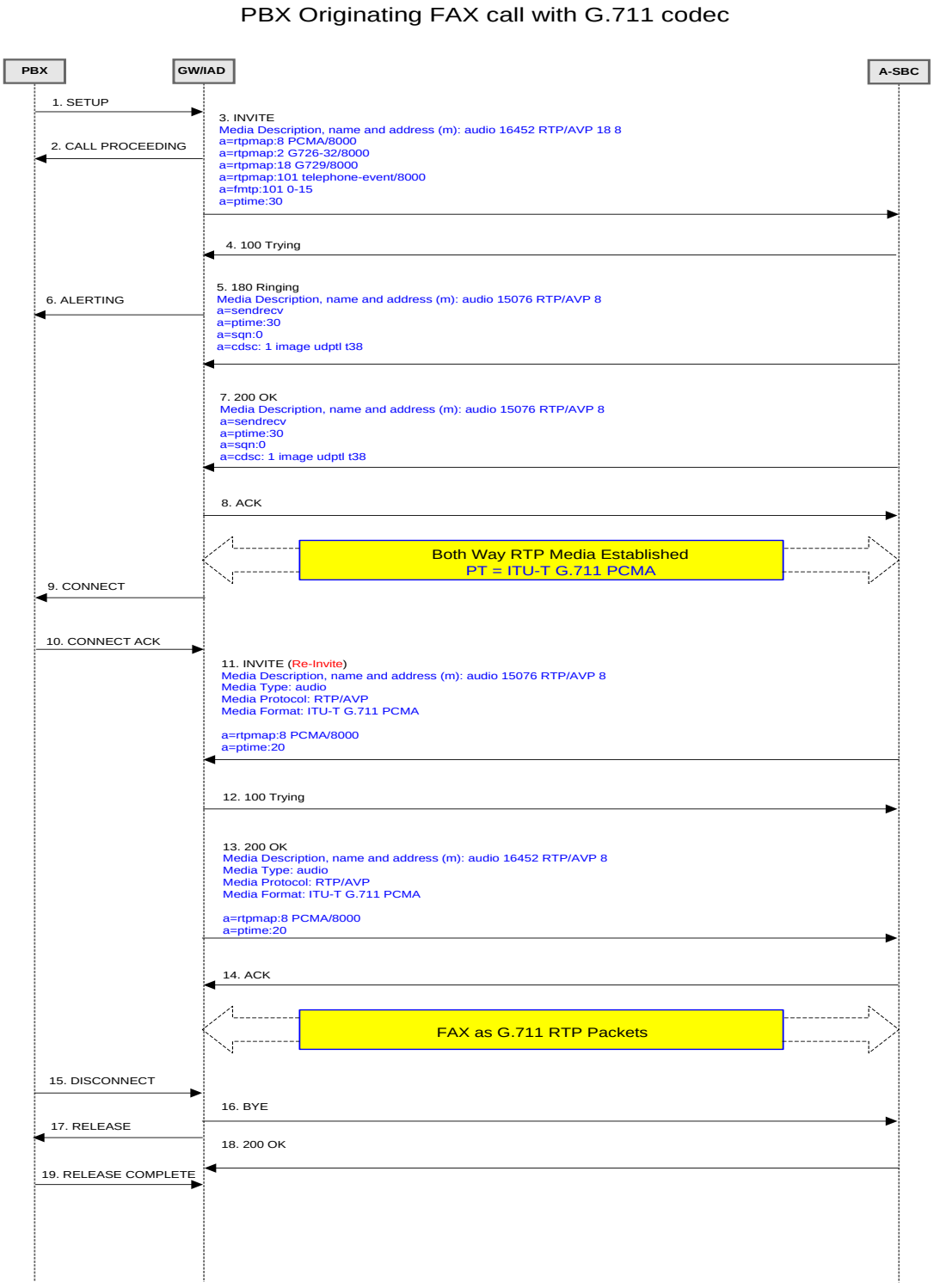



Figure 5 Originating FAX call with G.711 codec

### 10.2.2 Originating Fax call with T.38

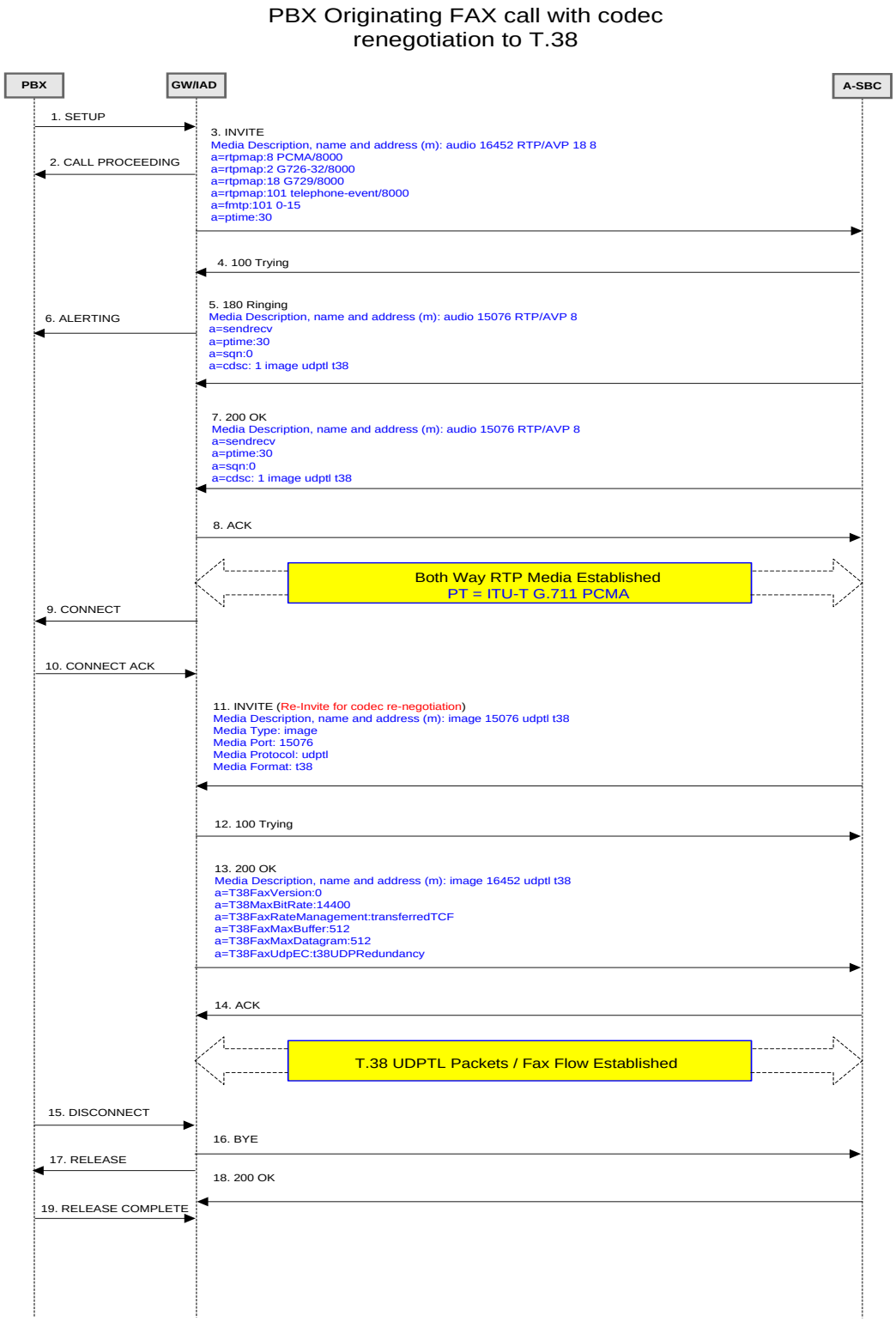



Figure 6 PBX Originating FAX call with T.38

### 10.2.3 Originating Fax call with T.38 and fallback to G.711

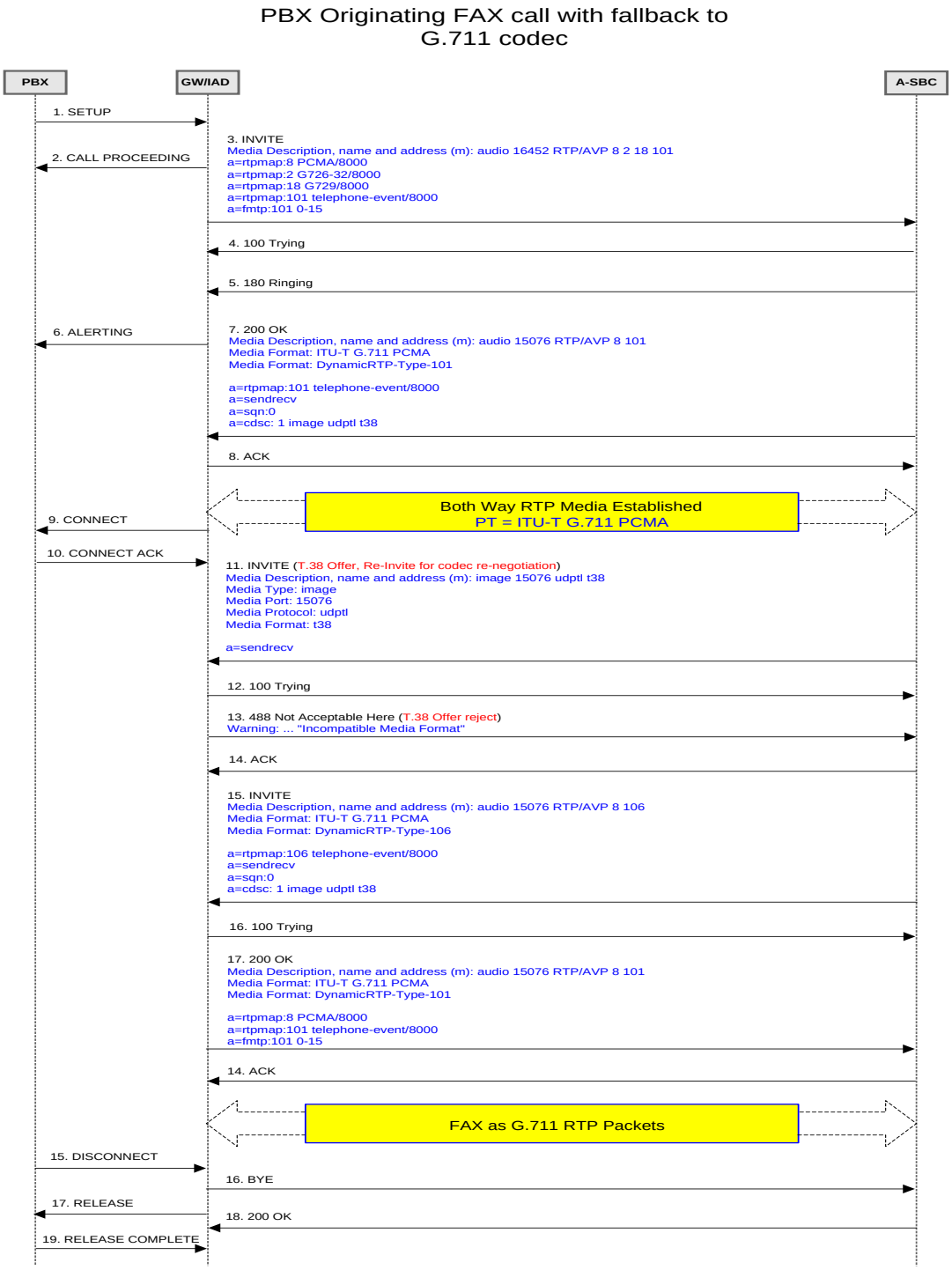



Figure 7 PBX Originating FAX call with fallback to G.711

### 10.2.4 Terminating Fax call with T.38

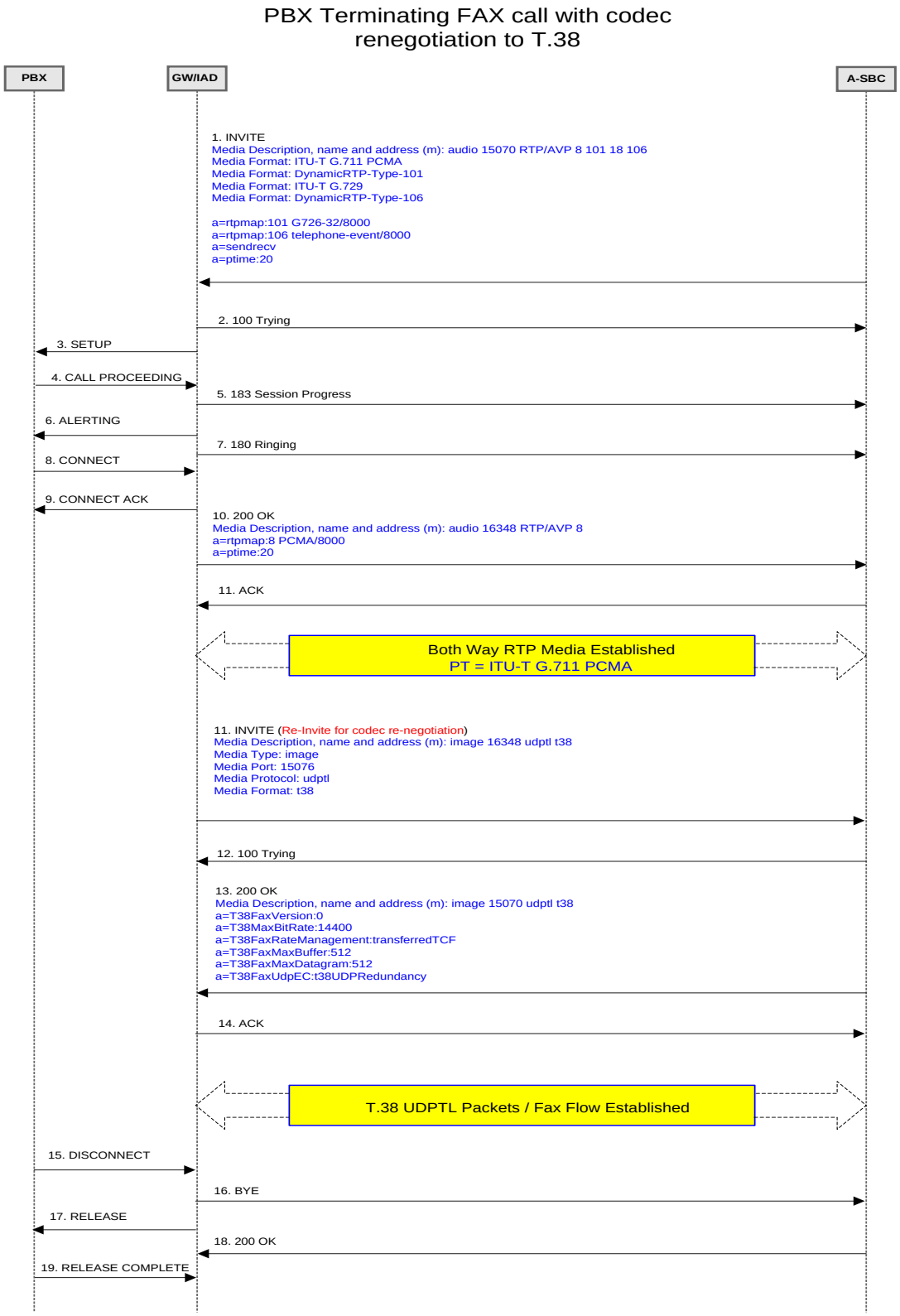



Figure 8 PBX Terminating FAX call with T.38

### 10.2.5 Terminating Fax call with G.711 codec

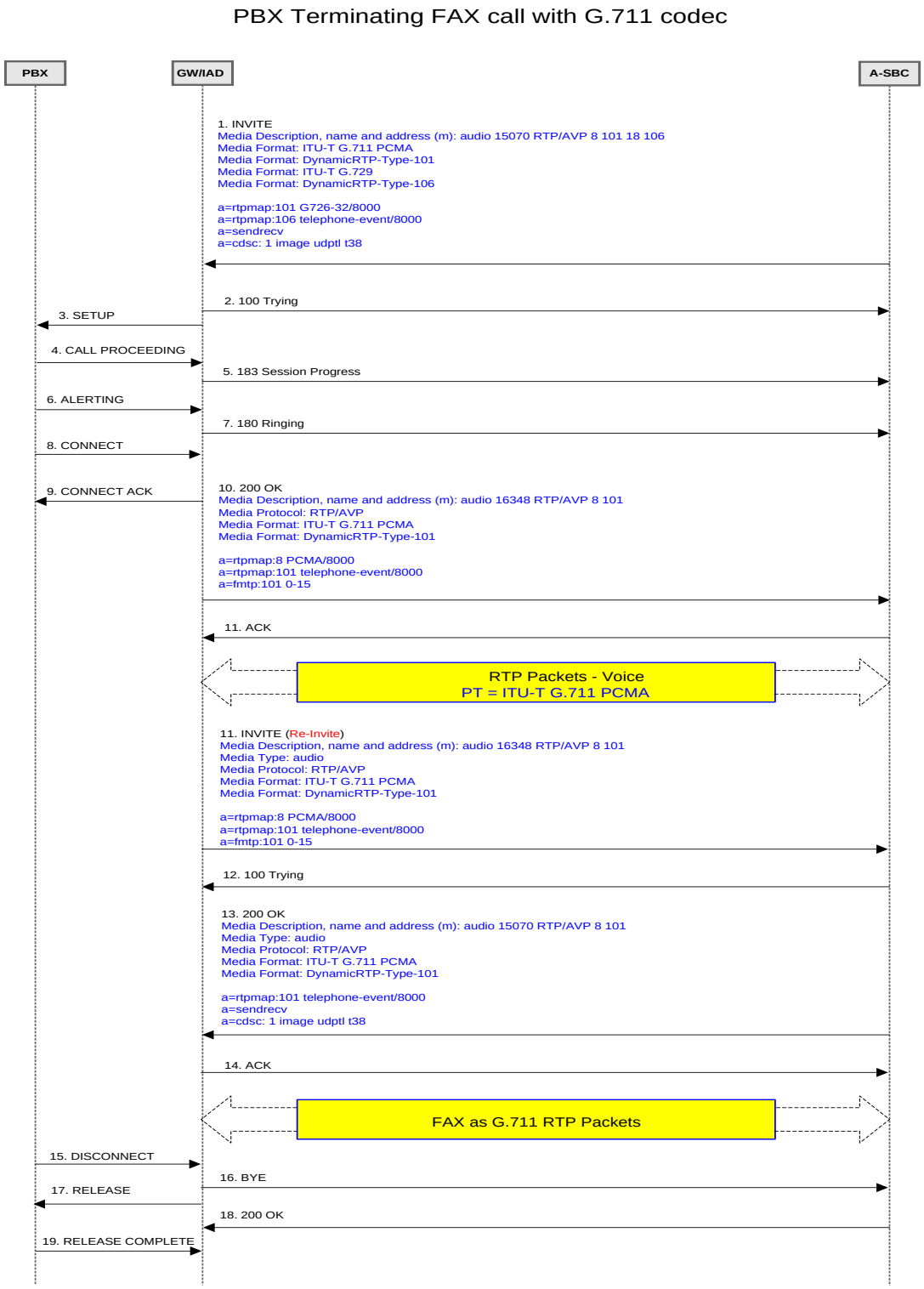



Figure 9 PBX Terminating FAX with G.711

## 10.3 DTMF

The local gateway should support out-of-band DTMF information exchange as described in RFC 2833.

The usage of dedicated RTP payloads is recommended because in case of calls with low-rate codecs the reproduction of the DTMF codes cannot be guaranteed.

# 11 Security requirements

## 11.1 Encryption

The local gateway SHOULD optionally support TLS V1.0 for signaling encryption. The following encryption algorithms SHALL be supported:

### 11.1.1 Signalling

As defined in RF3261 for SIPS.

### 11.1.2 Media

SRTP

SDES (RFC4568) for SRTP key negotiation.

# History

| Document history | | |
|---|---|---|
| PA2 | 24th of May 2011 | Released for Review |
| PA3 | 25th of July 2011 | Chapter 6.2.1 “SBC detection method” updated. |
| PA4 | 6th of November 2011 | Chapter 3: Scenario 2 highlighted as the chosen scenario for Phase 1.<br>Chapter 3.2: Requirement Vocabulary changed with reference only to RFC2119.<br>Chapter 4: SIPConnect 1.1 recommendation has been added and also a Note about the new BITKOM Position Paper<br>Chapter 6.1(CLIP) and 6.2 (CLIR) reworked.<br>Chapter 7.2.2. Reworked. Figure update.<br>Chapters 7.3.14, 7.3.2.5 reworked<br>Other small format and editorial changes. |
| PA5 | 6th of November 2012 | General format changes.<br>Chapter 5.1: Changed description for B-side to reflect normal and CFW scenarios. Added description for C-side.<br>Chapter 5.1: Changed description of CLIP Service in order to cover both Clip No Screening Scenarios (Active and Passive).Added example of incoming INVITE in international number format.<br>Chapter 7.3.2.6 ‘Privacy’ header field format deleted<br>Added Chapter 6.3.2.6. ‘Diversion’ format<br>Chapter 12.1 corrected<br>Chapter 4.2 updated because of the publication of the new BITKOM Position Paper referenced there. |
| PA6 | 26th of November 2012 | Chapter 5.1: 4th Paragraph corrected: part of sentence “with CLIP” replaced with “without CLIR”<br>Chapter 11.1.2 – added SRTP<br>Chapter 11.2 – SDES and SRTP added to Glossary |
| A | 17th of April 2013 | Chapter 5: Parameter “user=phone” added to P-Preferred-Id header.<br>Chapter 5.2: updated |
| V 1.0 | 28th of July 2016 | Restructuring, new Vodafone Layout |
| V 1.1 | 11th of March 2019 | “SIP Trunking 2.0” replaced by product name “Anlagen-Anschluss Plus” |
| V 1.2 | 20th of April 2020 | Introduction of Clearmode support |