1TR118
Technical Specification of the SIP-Trunking Interface between a SIP-PBX with DDI and the NGN Platform of Telekom Deutschland

Telekom Deutschland GmbH

Version 1.1
Stand 31.10.2016

Life is for sharing.

Imprint

Publisher

Deutsche Telekom AG

Order Information

Kurztitel / Title: 1TR118

Version	**Stand**
1.1	31.10.2016

Author

Abteilung FMED-93

64295 Darmstadt

Responsible

Deutsche Telekom Technik GmbH
Fixed Mobile Engineering Deutschland
Abteilung FMED-93
64295 Darmstadt

Change History

Version	Stand	Editor	Changes / Commentary
1.0	12.06.2015	L. Liess, N. Rathke, A. Seus	- Media Security - Support P-Early-Media header
1.1	10.10.2016	L. Liess M. Lochmann N. Rathke	- Changes in the section 2.6 “Fax and Modem” - Change in section 2.7.2 “Domain Names and DNS queries for the Telekom SIP Outbound Proxy and Registrar” - Change in the title of section 2.16 “Early Media Support (planned) ” - New section 2.18 “Call Hold and Announcements (Music-on-Hold) ” - Note added to section 2.19.2 “COLP/COLR (TIP/TIR)” - New section 2.19.7 “Call Forwarding by Deflection (302)” - Changes in section 2.10 “NAT-Traversal” - Editorial changes

Foreword

The present document describes the SIP-interface between the Next Generation Network (NGN) of Telekom Deutschland (hereinafter called NGN) and SIP-PBXs using Direct Dial In (DDI) capability. The specification is based on the already published specification 1TR114 [2] and describes the SIP-Trunking specific aspects, additionally.

Basically there are two different mechanisms for connecting SIP-PBXs with the NGN:

1) Business MSN (Multiple Subscriber Number)
   The SIP-PBX is connected to the NGN similarly to a private customer end device (IAD), as a SIP UE with multiple phone numbers, according to the Deutsche Telekom specification 1TR114. For SIP-PBXs connected in this mode, each individual MSN of the SIP-PBX is provisioned within the NGN. All telephony features are performed as described in the 1TR114 specification. The interface to SIP-PBXs connected in this way is not subject of this specification.

2) SIP-Trunk (DDI)
   For SIP-PBXs connected using SIP-trunks only the prefix numbers are provisioned in the NGN. The allocation of the respective extensions is done by the SIP-PBX itself using the DDI feature.

   The specific aspects for the interface to SIP-PBXs connected in this mode are described in this specification.

   According to the SIP-Connect 1.1 recommendation, there are two modes of connectivity for SIP-PBXs using SIP-trunks: Registration Mode and Static Mode.

   - Registration Mode SIP-PBXs
     This kind of SIP-PBXs publish their IP-address to the NGN using a SIP REGISTER message according to the RFC 6140 [16].
     SIP-PBXs which do not support the RFC 6140 yet, may register according to the RFC 3261 [8] and ETSI TS 182 025 [7]. However, Deutsche Telekom recommends the usage of the RFC 6140, according to [4] and [5].

   - Static Mode SIP PBXs
     This kind of SIP-PBXs do not register, but the IP-address or the enterprise domain name is configured within the NGN or published in the DNS.

This Technical Specification (German: Technische Richtlinie,TR) has been produced by the department FMED-321 of Deutsche Telekom Technik GmbH, Fixed Mobile Engineering Deutschland.

Scope

The existing PSTN/ISDN network of Telekom Deutschland will be substituted by an IP-based Next Generation Network (NGN) using the SIP protocol.
The present Technical Specification (TR) is applicable to the SIP- and media (RTP) interface between a business customer's SIP-PBX with DDI and the NGN according to the AGB [1] of Deutsche Telekom.

Figure 1 depicts the scope of the relevant technical specifications.

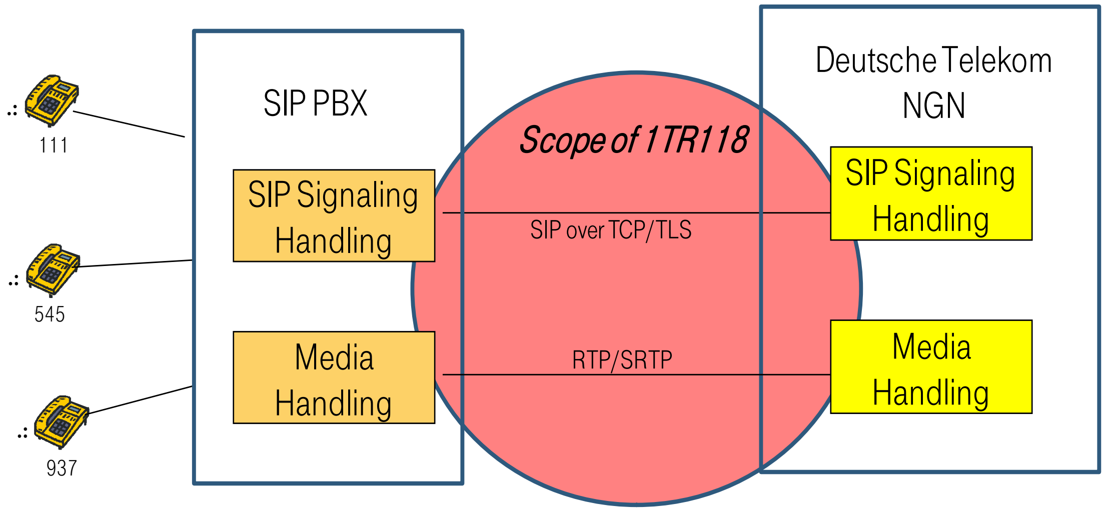


Figure 1: Scope of this technical specification

Table of Contents

List of Figures

1 Introduction

The existing PSTN/ISDN technology of the Deutsche Telekom will be replaced by an IP-based Next Generation Network (NGN) using the SIP protocol. The interface between the NGN and its end devices and the features supported by the NGN at this interface are described in the Deutsche Telekom specification 1TR114. For connecting SIP-PBXs with DDI, Deutsche Telekom additionally supports the SIPConnect 1.1 Technical Recommendation [5] with the amendments described in the BITKOM Recommendation "SIP Trunking –Detailempfehlungen zur harmonisierten Implementierung in Deutschland" [4] and with the amendments described in this specification.

The NGN for voice switching is mainly based on the architecture defined by the IMS model. 3GPP extended the TS 24.229 [6] in order to ensure the compatibility with SIPConnect 1.1 [5].

The figure below shows the principle of endorsement used within this document.

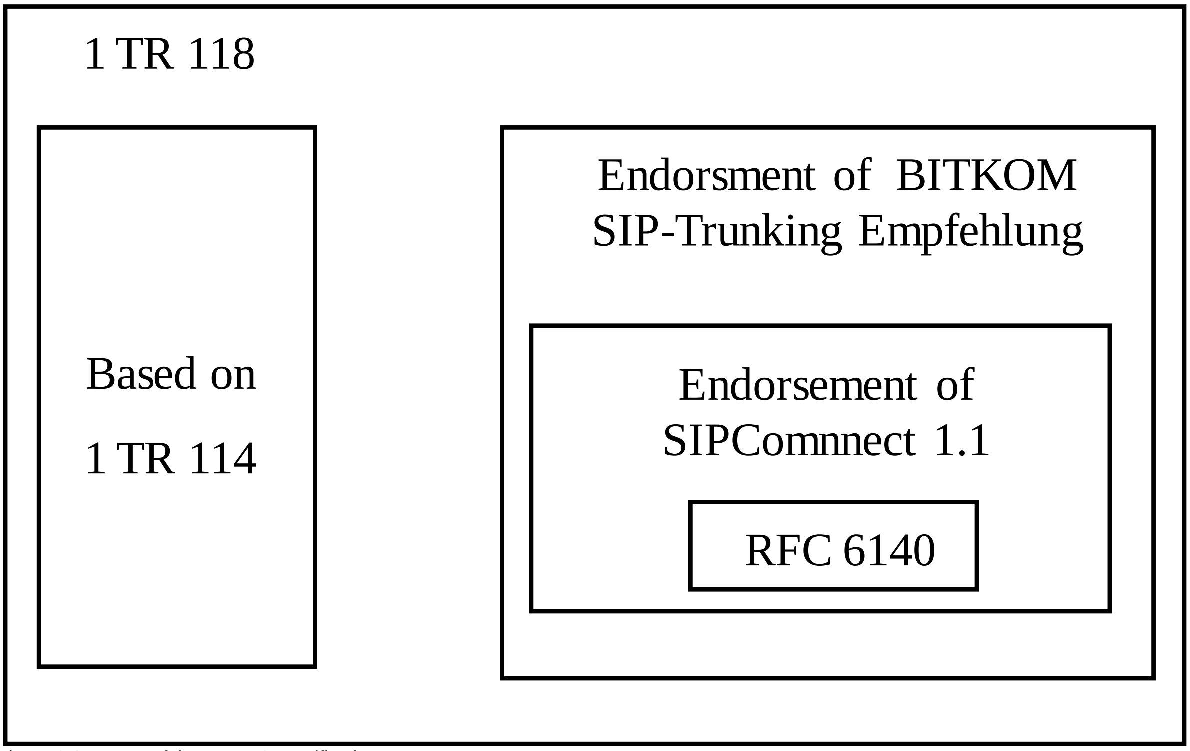


Figure 2 Structure of the 1TR118 specification

2 Capabilities

2.1 SIPConnect 1.1 Modes of Operation

The NGN is able to connect SIP-PBXs in both Registration Mode and Static Mode, according to [4] and [5].

Due to reduced administrative effort for setup and to better technical compatibility with the IMS-model, Deutsche Telekom strongly recommends the usage of the Registration Mode.

2.2 Identities configured for the SIP-PBX

The SIP-PBX phone number blocks and a default phone number (which has to be a routable E.164 number) are configured at the NGN and at the SIP-PBX.

Example:
Phone number blocks: +49 711 25733, +49 711 25734, +49 711 25735
Default phone number: +49 711 25734-100

2.3 Registration Mode of Operation

For SIP-trunking, the SIP-PBX must send only one REGISTER request to the NGN for all phone number blocks configured for the SIP-PBX. When the REGISTER is received, the NGN changes the status of all phone number blocks configured for the SIP-PBX (and with this of all phone numbers within these blocks) to “available”.

2.3.1 From: and To: Header Fields in the REGISTER request

The SIP-URIs in the From: and To: header fields of the REGISTER request must contain the prefix of one of the phone number blocks configured for the SIP-PBX.

Example:
Phone number blocks of the SIP-PBX: +49 711 25733, +49 711 25734, +49 711 25735.
Default phone number: +49 711 25734-100

```
To: <sip: +4971125733@sip-trunk.telekom.de>
From: <sip: +4971125733@sip-trunk.telekom.de>;tag=a23589
```

2.3.2 Registration According to SIPConnect 1.1 (RFC 6140 [16])

The NGN supports the Registration Mode according to [5], [16] and [4]. The NGN-specific differences from these specifications are described in sections 3.1 and 3.2.

The registration method according RFC 6140 [16] is the default registration-mode for IP-PBXs to the NGN.

.

2.3.2.1 Supported RFC 6140 [16] Sections

The NGN supports following sections of the RFC 6140:

- Section 5 – “Registering for Multiple Phone Numbers”
- Section 6 - “SSP Processing of Inbound Requests”
- Section 7.3 –“Client-Initiated (Outbound) Connections “
- Section 8 – “Examples”

- Section 9.1 - “New SIP Option Tag”
- Section 9.2.1 – “'bnc' SIP URI Parameter”

The NGN does currently not support the following sections:

- 7.1 “Globally Routable User Agent URIs (GRUU)”
- 7.2 “Registration Event Package”
- 7.4 – “Non-Adjacent Contact Registration (Path) and Service-Route Discovery”
- 9.2.2 “'sg' SIP URI Parameter” and
- 9.3 “New SIP Header Field Parameter”

2.3.2.2 Contact: Header Field

The Contact: header of the REGISTER request must contain the IP-address of the IP-PBX in the host-part and the “bnc”-parameter according to the RFC 6140 [16].

Example:

```
Contact: sip:164.168.138.1:5060;bnc
```

2.3.3 Registration Based on RFC 3261 and ETSI TS 182 025

SIP-PBXs connected in Registration Mode which do not yet support the registration according to the RFC 6140 [16] may register according to RFC 3261 [8], ETSI TS 182 025 [7] and 3GPP TS 24.229 [6]. Note that only one REGISTER-request must be sent by the SIP-PBX.

2.3.3.1 Contact: Header Field in the REGISTER request

The Contact: header of the REGISTER request must contain the prefix of one of the phone number blocks configured for the SIP-PBX in the user-part and the IP-address of the SIP-PBX in the host-part, according to RFC 3261.

```
Contact: sip: +4971125733@164.168.138.1:5060
```

2.3.4 SIP-PBX Authentication in Registration Mode

In registration mode, the NGN uses the SIP-Digest authentication. When TLS is used in registration mode, the SIP-PBX authenticates the NGN using the Outbound-Proxy’s TLS server certificate.

2.4 Static Mode of Operation

The NGN supports the Static Mode according to SIPconnect 1.1 [5] and BITKOM [4]. Differences between Telekom Deutschland’s NGN and these specifications are described in sections 3.1 and 3.2.
The IP-address of the SIP-PBX must be provisioned in the NGN.

2.4.1 SIP-PBX Authentication in Static Mode

In static mode, the NGN authenticates the SIP-PBX using the PBX’s IP-address. Support of TLS client certificates as required by SIPconnect 1.1 is planned for future releases. SIP-Digest authentication is not supported in static mode.
The SIP-PBX authenticates the NGN using the Outbound Proxy’s TLS server certificate.

2.5 Telephony Codecs

1TR114 [2] applies with following modification:

1) SIP-PBXs used for SIP-trunk must support G.711a and should support G.722. In case of a failed negotiation a fallback to G.711a must be possible.
2) The codecs G.711 µ , G.729 and clear channel (RFC 4040[12]) will not be modified in offers for calls via the NGN. They can be used if all involved elements (the B-party’s end device as well as e.g. other carrier’s nodes) agree in negotiating them.

2.6 Fax and Modem

1TR114 [2] applies with following modifications:

- SIP-PBXs used for SIP-trunk must support fax based on G.711a at least.
- The NGN supports the transmission of T.38 fax, in a passive, transparent way, if both user entities (caller and callee) are attached to the NGN using SIP-Trunks and they agree to use T.38 fax (offer-answer).
- Note: T.38 over UDPTL media encryption is not supported.

Support of V.152 modem according to 1TR114 [2] section 4.2.3.

2.7 Phone Numbers Format

The NGN uses SIP URIs containing E.164 phone numbers and the “user=phone” parameter for the SIP signalling.

Callee phone number:

- The SIP-PBX must send an E.164 phone number in the R-URI, excepting in the context of a private numbering plan and special phone numbers. (The special numbers can be found at the following links provided by the BNetzA: 110, 112 , 115 , 116xyz , 118xy)
- The phone number in the To: header field is not checked or used for routing by the NGN.

Caller phone number:

- The SIP-PBX must send E.164 phone numbers in the SIP header fields containing the caller identity (From:, P-Asserted-Identity, P-Preferred-Identity header fields).

2.7.1 Domain Names and DNS queries

2.7.2 Domain Names and DNS queries for the Telekom SIP Outbound Proxy and Registrar

The SIP-PBX must support domain names up to 64 characters for outbound proxy and registrar. The domain names for the outbound proxy and registrar are subdomains of the domain sip-trunk.telekom.de.
The SIP-PBX must support receiving up to four Proxy-Destinations in SRV-records resulting from a DNS-query. If more than one IP-addresses are received, the SIP-PBX must resolve and try them sequentially.

2.7.3 Domain Names for the SIP-PBX Identities

When sending INVITE requests, a SIP-PBX may use any domain name for its own identities, e.g. in the From: , P-Asserted-Identity and P-Preferred-Identity header fields. However, at the NGN the domain will be replaced with a Telekom subdomain. The SIP-PBX must be able to accept responses containing the replaced domain name.

2.8 IP-addresses

A SIP-PBX connected to the NGN must use the same Source-IP-address for SIP-signalling and media in the IP-packets. Different IP-addresses for SIP and media, according to SIPConnect 1.1, are currently not supported by the NGN, but it is planned for a later version.

2.9 Transport Protocols

A SIP-PBX connected to the NGN must use TCP or TLS as transport protocol for SIP-signalling. For security reasons, UDP is not allowed for SIP-trunking signalling.

2.10 NAT-Traversal

The NGN provides support for NAT-traversal. The NGN NAT-traversal functionality relies on the SIP-PBX to comply to following requirements:

- SIP-PBXs knowing their public IP-address and public port information must send this information in the VIA and CONTACT-Header.
- SIP-PBXs not knowing the public IP-address and public port information must send a private IP-address (RFC 1918) in the VIA and CONTACT-Header. In that case

the SIP-PBX must send media streams with at least 3 RTP packets after retrieving or generating an SDP answer, even though no media needs to be played and ignoring any inactive, send-only or receive-only attributes.

- SIP-PBXs must set-up the SIP transport protocol sessions, monitor their status, send keep-alive messages and activate or failover accordingly.
- SP-PBXs must use the same IP-address for SIP-signaling and media traffic (see also section 2.8 “IP-addresses”).
- The SIP-PBX must reuse already existing TCP and TLS-connections to send and receive SIP-messages.

STUN (RFC 5389), TURN (RFC 5766) and ICE (RFC 5245) are not supported by the NGN for SIP-Trunk customers because these methods are either insufficient or not broadly supported by the SIP-PBXs.

2.11 Signalling and Media Security

The NGN supports end-to-network encryption for signalling and RTP-media. End-to-end encryption, for signalling or media, is not supported.

2.11.1 SIP Security

The SIP signalling may be secured using TLS. TLS v1.2 is used by the NGN.

1) In Registration Mode, SIP over TLS with encryption and server authentication (server certificate) is supported by the NGN. MD5 SIP Digest client authentication (password) is used to authenticate the SIP-PBX. The TLS-connection must be initiated and maintained by the SIP-PBX and it must be successfully setup before the SIP-PBX sends the REGISTER request.
2) In Static Mode, SIP over TLS with encryption and server authentication is supported by the NGN, the SIP-PBX is authenticated using the IP-address from the IP-Layer. Using client certificates is planned for a later version. MD5 SIP Digest client authentication (password) is not supported in static mode.

In both modes of operation, the SIP-PBX is responsible for initiating, maintaining and reinitiating the TLS-connection.

2.11.2 Media Encryption

The NGN supports media encryption between the SIP-PBX and the NGN optionally. RTP-traffic may be encrypted using SRTP (RFC 3711 [11]) between the SIP-PBX and the Telekom Deutschland’s NGN (end-to-network access encryption). SDES (RFC 4568 [13]) is used for SRTP key exchange. Media encryption is used only in conjunction with SIP over TLS.

For calls from the SIP-PBX over SIP-trunks which use TLS for signalling, the NGN accepts SDP-offers for both RTP and SRTP.

For calls to the SIP-PBX and SIP-trunks which use TLS for signalling, the NGN only offers SDP with the profile RTP/SAVP and crypto-attribute, according to the RFC 4568. If the SIP-PBX rejects the RTP encryption, the call is lost, Fallback to RTP is not allowed according to the RFC 4568 [13].

A SIP-PBX must not use TLS for the SIP-signalling if it is not prepared to accept SRTP in the SDP-offers, otherwise all calls to the SIP-PBX will definitively fail.

Media traffic using other transport protocols than RTP, e.g. T.38 Fax over UDPTL, is transmitted unencrypted.

2.12 Caller Identity Handling for Outgoing Calls (from the SIP-PBX)

The handling described below applies for registration mode as well as for static mode, after the subscriber's SIP-PBX was reliable identified by the NGN Call Control.

The caller phone number processing in NGN is divided in three steps:

Step1 : Computing P-Asserted-Identity (PAI)

The SIP-PBX must send a geographical E.164 phone number from the phone number block(s) assigned to the SIP-PBX in the P-Preferred-Identity or P-Asserted-Identity header field. The NGN checks both fields in exactly this order and enters the first match into the P-Asserted-Identity header field. If there is no match, the NGN enters the configured default SIP-PBX identity (which must be a routable phone number) into the P-Asserted-Identity header field. For a transition period, also the From:- header field is considered for building the P-Asserted Identity. However, sending SIP-requests without a proper P-Preferred-Identity or P-Asserted-Identity is not recommended.

Step 2 – Recognizing Originating Identification Restriction (OIR)

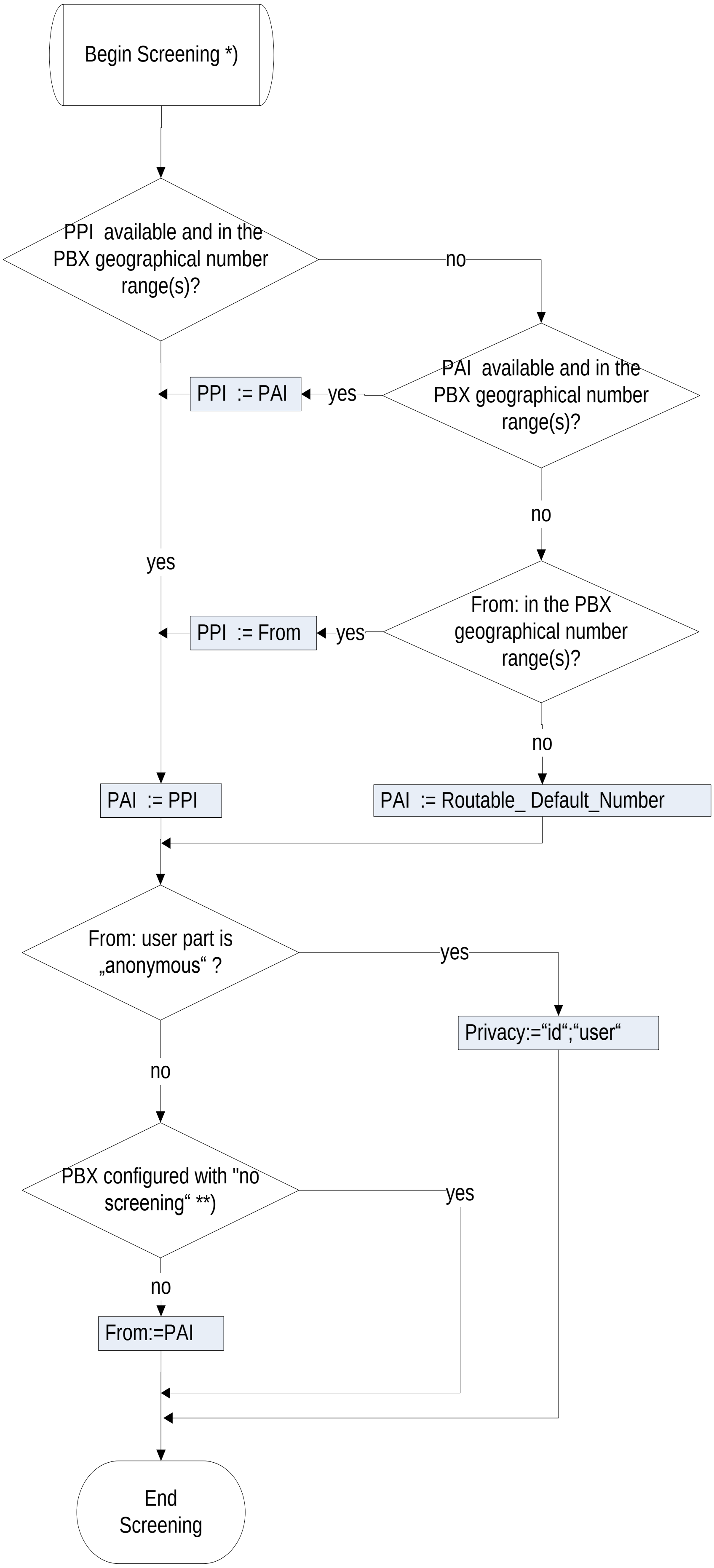
If the SIP-PBX sent sip:anonymous@anonymous.invalid in the From header field, the NGN sets the Privacy header field to “id” and “user” (in case that the SIP- PBX does not support the Privacy header). Then step 3 is skipped.

Step 3 – From: header handling for “screening” and “no screening” in case of Originating Identification Presentation (OIP)

If the SIP-PBX is configured with the “no screening” feature, the From: header field is left unchanged, otherwise the P-Asserted-Identity value is entered into the From: header field. If OIR (CLIR) is not activated, most SIP end devices including the fixed network SIP end devices display the phone number in the user part of the From: header field. They may also display the P-Asserted-Identity as a second Calling Party Number.

Note: The NGN SIP-PSTN Gateways map the PAI to the ISUP Calling Party Number and the From: to the Generic Number (Additional Calling Party Number). PSTN end devices display first the Generic Number (Additional Calling Party Number) and eventually second the Calling Party Number.)

The SDL-diagram below shows the caller identity handling for SIP-trunking outgoing calls within the NGN.



*) The identification and validation of the originating SIP-PBX was done before

Figure 3: SDL diagram - Caller phone number handling within the NGN Call Control

Use cases examples

SIP-PBX phone numbers block:	+49 288 181-0 to +49 228 181-9
SIP-PBX routable Default-ID:	+49 228 181-0
Additionally, the customer owns the numbers	+49 800 7654321

1) The INVITE sent by the PBX contains:
```
From:   +49 228 181 56
No PPI
No PAI
```

Result after the “Screening” function:

- “screening” :
  ```
  From:   +49 228 181 56
  PAI:    +49 228 181 56
  No PPI
  ```

  Display at a PSTN end device
  Generic Number : +49 228 181-56
  (Calling Party Number: +49 228 181-56)

- “no screening”:
  ```
  From:   +49 228 181 56
  PAI:    +49 228 181 56
  No PPI
  ```

  (Note: Display at a PSTN end device
  GenericNumber : +49 228 181-56
  (Calling Party Number: +49 228 181-56))

1) The INVITE sent by the PBX contains:
```
From:   +49 228 181 56
PPI:    +49 228 181 56
No PAI
```

Result after the Screening function:

- “screening”:
  ```
  From:   +49 228 181 56
  PAI:    +49 228 181 56
  No PPI
  ```

  (Note: Display at a PSTN end device
  GenericNumber : +49 228 181-56
  (Calling Party Number: +49 228 181-56))

- “no screening”:
  ```
  From:   +49 228 181 56
  PAI:    +49 228 181 56
  No PPI
  ```

  (Note: Display at a PSTN end device
  GenericNumber : +49 228 181-56
  (Calling Party Number: +49 228 181-56))

2) The INVITE sent by the PBX contains:
```
From:   +49 228 181 56
No PPI
No PAI
```

Result after the “Screening” function:

- “screening” :
```
From:   +49 228 181 56
PAI:    +49 228 181 56
No PPI
```

  Display at a PSTN end device
  Generic Number : +49 228 181-56
  (Calling Party Number: +49 228 181-56)

- “no screening”:
```
From:   +49 228 181 56
PAI:    +49 228 181 56
No PPI
```

  (Note: Display at a PSTN end device
  GenericNumber : +49 228 181-56
  (Calling Party Number: +49 228 181-56))

3) The INVITE sent by the PBX contains:
```
From:   +49 800 7654321
PPI:    +49 228 181 56
No PAI
```

Result after the Screening function:

- “screening”:
```
From:   +49 228 181 56
PAI:    +49 228 181 56
No PPI
```

  (Note: Display at a PSTN end device
  GenericNumber : +49 228 181-56
  (Calling Party Number: +49 228 181-56))

- “no screening”:
```
From:   +49 800 7654321
PAI:    +49 228 181 56
No PPI
```

  (Note: Display at a PSTN end device
  GenericNumber : +49 800 7654321
  (Calling Party Number: +49 228 181-56))

4) The INVITE sent by the PBX contains:
```
From:   +49 800 7654321
No PPI
No PAI
```

Result after the Screening function:

- "screening":
```
From:   +49 228 181 0
PAI:    +49 228 181 0
No PPI
```
  (Note: Display at a PSTN end device
  GenericNumber : +49 228 181-0
  (Calling Party Number: +49 228 181-0))

- "no screening":
```
From:   +49 800 7654321
PAI:    +49 228 181 0
No PPI
```
  (Note: Display at a PSTN end device
  GenericNumber : +49 800 7654321
  (Calling Party Number: +49 228 181-0))

5) The INVITE sent by the PBX contains:
```
From:   +49 228 181 56
PPI:    +49 228 181 23
No PAI
```

Result after the Screening function:

- "screening":
```
From:   +49 228 181 23
PAI:    +49 228 181 23
No PPI
```
  (Note: Display at a PSTN end device
  GenericNumber : +49 228 181-23
  (Calling Party Number: +49 228 181-23))

- "no screening" :
```
From:   +49 228 181 56
PAI:    +49 228 181 23
No PPI
```
  (Note: Display at a PSTN end device
  GenericNumber : +49 228 181-56
  (Calling Party Number: +49 228 181-23)

  Note: Deutsche Telekom's PSTN would assert the identity +49 228 181-0.)

6) The INVITE sent by the PBX contains:

```
From:   +49 89 21 58 15627
PPI:    +49 228 181 23
No PAI
```

In this use case the initial call was diverted by the SIP-PBX and the customer intends the number of the original caller to be displayed to the called party.

Result after the Screening function:

- "screening":

```
From:   +49 228 181 23
PAI:    +49 228 181 23
No PPI
```

(Note: Display at a PSTN end device
GenericNumber : +49 228 181-23
(Calling Party Number: +49 228 181-23))

- "no screening":

```
From:   +49 89 21 58 15627
PAI:    +49 228 181 23
No PPI
```

(Note: Display at a PSTN end device
GenericNumber : +49 89 21 58-15627
(Calling Party Number: +49 228 181-23))

Note: If the SIP-PBX-operator is not authorized to use the phone number +49 89 2158-15627, this use case does not comply to the regulatory law, e.g. TKG. Using the "no screening" feature, the SIP-PBX-operator is responsible for compliance with all relevant legal requirements!

7) The INVITE sent by the PBX contains:

```
From:   "anonymous"
PPI:    +49 228 181 23
No PAI
```

Result after the Screening function:

- For both "screening" and "no screening":

```
From:   "anonymous"
PAI:    +49 228 181 23
No PPI
```

2.13 Callee Identity in Incoming Calls (to the SIP-PBX)

2.13.1 Registration Mode According to SIPConnect 1.1 (RFC 6140 [16])

The NGN conveys the callee phone number in the R-URI user part, according to the SIPconnect 1.1 recommendation and to RFC 6140 [16].

2.13.2 Registration Mode Based on ETSI TS 182 025 (RFC 3261)

In cases when the SIP-PBX does not support the RFC 6140 yet, the NGN conveys the callee's phone number in the P-Called-Party-ID header field. The R-URI contains the phone number prefix received in the Contact: header field at the registration.

2.13.3 Static Mode According to SIPConnect 1.1

The NGN conveys the callee phone number in the R-URI user part, according to the SIPconnect 1.1 recommendation Section 10.1.1.

2.14 Emergency Calls

2.14.1 Emergency Calls from a SIP-PBX to the NGN

The NGN detects emergency calls based on the phone number in the R-URI containing 110 or 112 (eventually with carrier prefix).
For SIP-PBXs using an access provided by Telekom Deutschland, the user location information is determined using the source-IP-address in the IP-packet carrying the INVITE-message. Otherwise the user location information declared in customer's contract or provisioned by the customer using the webbased customer-self-care-interface s used.

2.15 DTMF

DTMF is supported according to 1TR114 [2].

2.16 Early Media Support (planned)

Early media and the P-Early-Media header must be supported according to 1TR114 [2], otherwise announcements and ringback tones may not work properly. A SIP-PBX which does not support the P-Early-Media header should be able to detect early media and be prepared to generate the ringback tone locally if no early media is received.

2.17 AOC

AoC is currently not supported.

2.18 Call Hold and Announcements (Music-on-Hold)

A SIP-PBX may initiate Call Hold according to SIPconnect 1.1 [5] section 14.8.

Note: The NGN does not provide announcements or MOH on behalf of a SIP-PBX connected to the NGN via a SIP-Trunk. The NGN Announcement Server is not triggered in case of Call Hold initiated by a SIP-PBX which is connected via a SIP-trunk to the NGN.

2.19 Network Services

2.19.1 CLIP/CLIR (OIP/OIR)

The NGN-based CLIP/CLIR (OIP/OIR) service is described in [2]. For SIP-trunking, CLIP (OIP) enables displaying the telephone number of the originating A-subscriber towards terminating B-subscriber (feature's user) depending on the information provided. The telephone number of the A-subscriber is transferred to the B-subscriber, irrespective of whether the user entities' device displays the information provided for the B-subscriber and can process it or not. The feature can be configured for permanent or per single call.

CLIR (OIR) restricts the presentation of the telephone number of the A-subscriber (feature's user) at the B-subscriber. The feature can be configured for permanent or per call. The feature's state of CLIP/CLIR applies on SIP-trunk-level.

If an anonymized From: header field or a Privacy header field set to "id" is received, then a Privacy header field is set to "user,id" by the NGN.

2.19.2 COLP/COLR (TIP/TIR)

The NGN-based TIP/TIR service is described in [2].
For SIP-trunking, COLR provides the restriction of the presentation of the phone number from the called party to the calling party, permanent or per call. COLP provides the presentation of the phone number from the called party to the calling party (COLP). By this the returned phone number of the actually reached calling-subscriber is sent. The feature's state of COLP/COLR applies on SIP-trunk-level.

Note: For the COLP/COLR service to work properly, the callee has to support this service.

2.19.3 CLIP no Screening

CLIP no screening allows the presentation of an arbitrary choosen number even out of range of the prefix assigned to the SIP-Trunk to called party. No verification of the phone number sent by the terminal in the From: header field is done by the NGN. The feature's state of CLIP no screening applies at the SIP-trunk-level.

2.19.4 Call Forwarding Unconditional

All calls will be forwarded towards a previous configured call forwarding destination. Call Forwarding unconditional applies on the SIP-trunk-level.

2.19.5 Call Forwarding Failure Condition

In case of a failure condition all calls will be forwarded towards a previous configured call forwarding destination. Call Forwarding Failure Condition applies on SIP-trunk-level.

2.19.6 Call Forwarding on PBX Not Logged-in (CFNL)

In case of PBX Not Logged-in all calls will be forwarded towards a previous configured call forwarding destination. Call Forwarding PBX Not Logged-In applies on SIP-trunk-level.

2.19.7 Call Forwarding by Deflection (302)

A SIP-PBX may initiate network based Call Forwarding by responding to a SIP INVITE with a 302 SIP response which contains the new target in the Contact:- header. The NGN will forward the INVITE to the new target and sends an 181 SIP response to the caller.

2.19.8 Preselection

The feature Preselection allows the PBX to select a permanent VoIP Service Provider differing from Deutsche Telekom. All calls are routed via the selected network provider. Preselection applies on SIP-trunk-level.

2.19.9 Call by Call

The feature Call by Call allows the PBX to select a VoIP Service Provider differing from Deutsche Telekom for single calls. The customer selects the Service Provider by adding a 010 prefix followed by terminal network operator code and the desired destination number.

2.19.10 Closed User Group (CUG)

The feature CUG makes sure that defined SIP-PBX' extension numbers or the whole prefix can be reached only via service numbers. Direct incoming-calling of these defined extension numbers is prevented.

2.19.11 Call Barring

Barring of numbers is supported for incoming and outgoing calls. Barring is used by the administrating a blacklists and/or whitelists. Barring can be administered by the VoIP provider and the business customer. Special numbers as emergency numbers are excluded from barring by the VoIP provider. Additionally, Anonymous Call Rejection (ACR) is supported. Configured black- and/or whitelists applies on SIP-trunk-level.

3 Protocol Profiles

This section profiles and endorses [4] and [5].
Markings used within the text with following meaning:
Text modified due to Deutsche Telekom's requirements that is added or deleted is shown as cursive (*example for added text*) or cursive and strucked (~~*example for deleted text*~~).

3.1 Modifications to the BITKOM Recommendation, Chapter 5

1) "P-Asserted-Identity" header field for Outgoing Calls from the Enterprise to the Service Provider

~~*The SP-SSE will provide a „screening function" to verify the content of the PAI. If identification is unsuccessful,*~~
~~*it may be overwritten by the SP-SSE.*~~

A received P-Asserted-ID header it is handled as specified in Section 2.12 of this document. The "screening function" described in the BITKOM recommendation should not be mistaken for the "screening/no screening" feature which affects the handling of the From:-header field.

If the SIP-PBX sends a P-Preferred-ID, ~~*it may be ignored by the SP_SSE. , this is handled according to*~~ *it is handled by the NGN as specified in Section 2.12 of this document.*

2) Privacy header field for Outgoing Calls from the Enterprise to the Service Provider

The NGN supports the “Privacy” header field as described in [4].

3) Forwarding a Call using a new dialog INVITE request
The NGN does not support the Diversion:-header field.

4) 5.13 Fax calls
The NGN supports the end-to-end transmission of T.38. T.38 fax gateways are not provided.

5) 5.14 Registration Mode
The NGN does not support the Non-Adjacent Contact Registration (Path) as specified in the RFC 6140 [16].

6) 5.17 IPv6
The NGN supports IPv6.

7) 5.18 Putting a Session on Hold
The NGN does not support receiving SDP session descriptions that have the ‘c=’ field set to all zeros (0.0.0.0), when the “addrtype” field is IPv4. The “Call Hold” feature is supported as described in [4].

3.2 Additional Modifications to the SIP-Forum „SIPconnect 1.1 Technical Recommendation”

1) 16.2 Signaling Security
The following requirements for using TLS apply to SIP-PBX and SP-SSE implementations supporting Static mode:
~~*Both SIP-PBX and SP-SSE **MUST** support the TLS Mutual Authentication model, whereby both the SP-SSE and the SIP-PBX provide their respective certificate as part of the TLS establishment phase.*~~

The NGN does currently not support TLS client certificates, only TLS server certificate is supported. The NGN verifies the IP-address of the SIP-PBX. Client certificates are planned for future releases.

A List of Abbreviations

Abbreviations and definitions, not listed hereafter, are defined in the reference documents in clause 3.
For the purposes of the present document, the following abbreviations apply:

-1-	
3GPP	Third Generation Partnership Project
-A-	
AAA	Authorization Authentication Accounting
ACR	Anonymous Communication Rejection
AGB	Allgemeine Geschäftsbedingungen
AOC	Advice Of Charge
-B-	
-C-	
CC	Call Control
CCBS	Completion of Communications to Busy Subscriber
CDIV	Communication Diversion Services
CFNL	Call Forwarding Not Logged-in
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CN	Calling Number (Calling Party Number), e.g. <CN>
COLP	Connected Line Identification Presentation
COLR	Connected Line Identification Restriction
CW	Call Waiting
-D-	
DDI	Direct Dial In
DNS	Domain Name System
DT	Deutsche Telekom
-E-	
ETSI	European Telecommunication Standardisation Institute
-F-	
FQDN	Fully Qualified Domain Name
-G-	
GRUU	Globally Routable User Agent URI
-H-	
HTTP	Hypertext Transfer Protocol
-I-	
IAD	Integrated Access Device
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISDN	Integrated Services Digital Network
-J-	
-K-	
-L-	
-M-	
MGC	Media Gateway Controller
MSN	Multiple Subscriber Number
-N-	
NAT	Network Address Translation

NGN	Next Generation Networks
-O-	
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
-P-	
PAI	P-Asserted-Identity
PPI	P-Preferred-Identity
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
-Q-	
QoS	Quality of Service
-R-	
RFC	Request for Comments
RTCP	Real Time Control Protocol
RTP	Real Time Transport Protocol
-S-	
SDES	Session Description Protocol Security Descriptions
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SRTP	Secure Real-time Transport Protocol
STUN	Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs);
-T-	
TBC/TBD	To be clarified/To be done
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TIP	Terminating Identification Presentation
TIR	Terminating Identification Presentation Restriction
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TR	Technical Recommendation
TURN	Traversal Using Relays around NAT
-U-	
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UDPTL	UDP Transport Layer
UE	User Equipment
URI	Universal Resource Identifier
URL	Uniform Resource Locator
-V-	
VoIP	Voice over Internet Protocol
-W-	
-X-	
-Y-	
-Z-	

B Definitions

For the purposes of the present document, the following terms and definitions apply:

Term	Definition / Remark
User Equipment	Any SIP device (terminal) at the subscriber premises used by an end user to communicate. It can be e.g. an IAD or telephone set, or any other telecommunication device.
User Agent	See RFC 3261[8].
Call Control	In telephony, call control refers to the software within a telephone switch that supplies its central function. Call control decodes addressing information and routes telephone calls from one end point to another. It also creates the features that can be used to adapt standard switch operation to the needs of users. Call control software, because of its central place in the operation of the telephone network, is marked by both complexity and reliability.
NGN or NGN platform	The entire amount of central servers and gateways, as well as software within the DT IP- network which provides voice services.
VoIP line	A VoIP line is equivalent to a MSN in ISDN; Multiple VoIP lines can be assigned to a VoIP account of the NGN
IP	Considering the expected parallel availability of IPv4 and IPv6 the term “IP” in this document is related to both internet protocol versions.
SIP-/IP-PBX	Private Branch Exchange using SIP
SIP-trunking interface	The interface between the NGN and a SIP-PBX with DDI which complies with this specification.

C References

References are either specific (identified by date of publication and/or edition number or version number) or non specific. For a specific reference, subsequent revisions do not apply.
For a non-specific reference, the latest version including amendments, errata and corrigenda applies. Date of publication in square brackets [ ] refer just to the last known version while this document was in revision.

[1] AGB: Allgemeine Geschäftsbedingungen der Deutschen Telekom AG (see: www.telekom.de/agb)
[2] 1TR114 version 3.0.0: Technical Technical Specification of the SIP (Gm) interface between the User Equipment (UE) and the NGN platform of the Deutsche Telekom
[3] DT 1TR127: Technical Specification for SIP User Equipments (UE) providing IMS simulation services via ISDN (DSS1) interfaces (ISDN/SIP interworking) using the NGN platform of Deutsche Telekom
[4] BITKOM: SIP Trunking –Detailempfehlungen zur harmonisierten Implementierung in Deutschland unter besonderer Berücksichtigung der SIPconnect 1.1 Technical Recommendation des SIP-Forum
[5] SIP Forum SIPconnect 1.1 Technical Recommendation: “SIP-PBX / Service Provider Interoperability; SIP Forum Document Number: TWG-2”
[6] 3GPP TS 24.229 V8.7.0 (2009-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 8)
[7] ETSI TS 182 025: "Business trunking; Architecture and functional description".
[8] IETF RFC 3261: "SIP: Session Initiation Protocol”
[9] IETF RFC 3263: "SIP: Session Initiation Protocol: Locating SIP Servers”
[10] IETF RFC 3325: "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks”
[11] IETF RFC 3711: "The Secure Real-time Transport Protocol (SRTP)
[12] IETF RFC 4040: "RTP Payload Format for a 64 kbit/s Transparent Call”
[13] IETF RFC 4568: "Session Description Protocol (SDP) Security Descriptions for Media Streams”
[14] IETF RFC 4961: "Symmetric RTP / RTP Control Protocol (RTCP)”
[15] IETF RFC 5246: " The Transport Layer Security (TLS) Protocol Version 1.2”
[16] IETF RFC 6140: "Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)".