Technical Specification of the SIP-Trunking Interface for CompanyFlex of Deutsche Telekom

1TR119

Version 1.12.0

28. November 2022

Herausgeber / Publisher

Deutsche Telekom AG

Verantwortlich / Responsible

Deutsche Telekom Technik GmbH

Services & Platforms, Voice & Messaging

Abteilung One VM Design

53227 Bonn

Bestellangabe / Order Information

Kurztitel / Title: 1TR119

Ausgabe / Version: Version 1.12.0

Bezugsanschrift / Order address

Deutsche Telekom Technik GmbH

Services & Platforms, Voice & Messaging

Abteilung One VM Design

53227 Bonn

Change History

Version	Date	Changes / Commentary
1.0	02.04.2019	First Official Version
1.1	28.06.2019	Changes in 5.1, 10.2, 10.3, 11.1, 12.2, 13.3, 13.4, 13.5, 13.6
1.2	18.07.2019	new Root Certificate
1.3	14.08.2019	Editorial changes, updates for pTime in chapter 6.1
1.4	30.10.2019	Updates for maxpTime and Codec Lockdown, SIP 403 and 488 for PPI and PAI, Outbound Proxy and SIP Options
1.5	22.11.2019	Amendment for Call Forwarding in chapter 13.5 and media supervision in chapter 13.10 and inclusion of clause 12.3 and 9.5
1.5.1	04.12.2019	Editorial Update of Product Name
1.6.0	30.04.2020	Update of the Example in Chapter 5.1, Amendment in Chapter 8.1.1
1.7.0	07.09.2020	Update in Chapter 4.1 for the user name, 10.2 telesec certificate
1.8.0	15.10.2020	Update for REFER in chapter 13.11, update in chapter 10.3 for media encryption clarifications, editorial clean-up, missing references added to chapter 2, clarification on VIA header field included in chapter 4.1, clarifications for emergency call centres included in chapter 14.4, update for supervision timer in clause 12.3
1.9.0	03.02.2021	Update in chapters 8, 10.3, 11.1 and 11.2
1.9.1	05.10.2021	Correction of URL for TeleSec Root certificates in chapter 10.2
1.10.0	02.11.2021	Addition of chapter 9.6 for SIP Message Size and clarification for Provider Data in chapter 14.4
1.11.0	04.04.2022	Clarification of CLIP no Screening behaviour in chapter 13.3; addition of Outbound Proxy reselection behaviour in chapter 8.1.2; chapter 13.10 was reworked and split up in two parts for sending and receiving SIP OPTIONS
1.12.0	28.11.2022	Minor editorial changes; removed reference for future implementation of static mode; clarification on SIP302 transport parameter; outlook on NG eCall protocol profile added

Contents

Foreword

This Technical Specification (Technische Richtlinie, TR) has been produced by the One VM Design Squad of Deutsche Telekom Technik GmbH, Services & Platforms, Voice & Messaging (in the following named as Deutsche Telekom) and contains the description of the SIP (Gm) interface between SIP-PBXs using Direct Dial In (DDI) capability and the NGN platform of Deutsche Telekom.

This TR contains the current status of the SIP (Gm) interface of SIP-PBXs using Direct Dial In (DDI) capability which will be supported by the NGN platform of Deutsche Telekom.

Modifications in the main body as well as in the annexes of this document cannot be excluded at this point of time due to the still ongoing work on the referenced standards (e.g. 3GPP, ETSI) and some open decisions concerning the supported options.

The present document describes the final NGN platform of Deutsche Telekom; deviations to the currently provided solution of the NGN platform of Deutsche Telekom are possible (e.g. not yet realized service features).

1 Scope

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 for the new Deutsche Telekom Product CompanyFlex.

The present Technical Specification (TR) is applicable to the signalling (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.

The Deutsche Telekom NGN is an IMS Network. Therefore, the specification 1TR114 [2] is a valid reference for more details.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

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 (see: www.telekom.de/agb)

[2] 1TR114: Technical Specification of the SIP (Gm) interface between the User Equipment (UE) and the NGN platform of the Deutsche Telekom

[3] ETSI TS 182 025: "Business trunking; Architecture and functional description".

[4] IETF RFC 3261: "SIP: Session Initiation Protocol"

[5] IETF RFC 3711: "The Secure Real-time Transport Protocol (SRTP)"

[6] IETF RFC 4568: "Session Description Protocol (SDP) Security Descriptions for Media Streams"

[7] IETF RFC 4733: "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals"

[8] IETF RFC 4734: "Definition of Events for Modem, Fax, and Text Telephony Signals"

[9] IETF RFC 5244: "Definition of Events for Channel-Oriented Telephony Signalling"

[10] IETF RFC 7044: "An Extension to the Session Initiation Protocol (SIP) for Request History Information"

[11] IETF RFC 3329: "Security Mechanism Agreement for the Session Initiation Protocol (SIP)"

[12] IETF draft-dawes-sipcore-mediasec-parameter: "Security Mechanism Names for Media"

[13] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3"

[14] IETF RFC 6140: "Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP) "

[15] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication"

[16] IETF RFC 4040: "RTP Payload Format for a 64 kbit/s Transparent Call"

[17] IETF RFC 3263: "Session Initiation Protocol (SIP): Locating SIP Servers"

[18] IETF RFC 1918: "Address Allocation for Private Internets"

[19] IETF RFC 5626: "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP) "

[20] IETF RFC 3551: "RTP Profile for Audio and Video Conferences with Minimal Control"

[21] IETF RFC 5922: "Domain Certificates in the Session Initiation Protocol (SIP) "

[22] SIP Forum SIPconnect 2.0 Technical Recommendation

[23] 3GPP TS 24.628: "Common Basic Communication procedures using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification"

[24] IETF RFC 6442: "Location Conveyance for the Session Initiation Protocol"

[25] IETF RFC 7433: "A Mechanism for Transporting User-to-User Call Control Information in SIP"

[26] IETF RFC 7315: "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP"

[27] IETF RFC 7852: "Additional Data Related to an Emergency Call"

[28] ITU-T Recommendation G.168: "Digital network echo cancellers"

[29] IETF RFC 2119: "Key words for use in RFCs to Indicate Requirement Levels"

[30] IETF RFC 8787: "Location Source Parameter for the SIP Geolocation Header Field"

[31] IETF RFC 5491: "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations"

[32] IETF RFC 8147: “Next-Generation eCall”

3 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 [4].
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 number 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 an 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.
Pilot User	A Pilot User is represented by the identity which needs to be registered by a PBX in order to establish a Trunk Group between SIP-PBX and NGN (‘Registrierungsrufnummer’)
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. A single SIP Trunk may contain one or multiple Trunk Groups.
Trunk Group	A Trunk Group is a route to the PBX, as recognized by the NGN (established by the registration of a Pilot User)
Shall	As usual within standards and documents of Deutsche Telekom, 3GPP, ETSI and ITU-T the word shall is used to indicate a procedure or requirement as mandatory. (NOTE)
Should	As usual within standards and documents of Deutsche Telekom, 3GPP, ETSI and ITU-T the word should is used to indicate a procedure or requirement as optional (NOTE)

NOTE: The key words "SHALL", "SHALL NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [29].

4 General Description

4.1 Identities configured for the SIP-PBX and Addressing

The SIP-PBX phone number blocks, single numbers and one or multiple pilot number(s) (which are used only for registration purposes) are configured at the NGN and at the SIP-PBX. All headers that are used to carry Public Identities like From, To, Request-URI, P-Preferred-Identity, P-Asserted-Identity shall support a SIP URI format with the user part in E.164 format.

A default number is neither configured nor required as it is mandatory to provide a valid identity of the SIP Trunk in any call attempt.

Example:

Phone single number / Phone number blocks:	sip:+49228123xxxx@tel.t-online.de
Pilot number:	sip:+49199296100xxxx@tel.t-online.de

The SIP-PBX shall send an E.164 phone number from the phone numbers 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 call will be REJECTED. This applies also when OIR/CLIR is active.

NOTE: Phone numbers in the P-Preferred-Identity or P-Asserted-Identity header field which are not assigned to the SIP-PBX will be rejected with SIP 403 whereas a Pilot number of the SIP-PBX in those headers will be rejected with SIP 488.

If the identity in the From header is different from the identity provided in P-Preferred-Identity/P-Asserted-Identity header, then the identity in the From header will be overwritten with the identity in P-Preferred-Identity/P-Asserted-Identity header

NB: SIP-PBX must provide the DDI in the SIP INVITEs that the customer wishes to see in his bill (Nebenstellenindividuelle Abrechnung).

Please note that if no SBC is deployed between SIP-PBX and NGN, the IP addresses of the SIP Via header fields in REGISTER and INVITE requests need to be identical to unambiguously identify the contact.

5 Mode of Operation

5.1 Registration mode

The SIP-PBX shall send only one initial REGISTER request based on RFC 3261 [4] to the NGN using the provided pilot number for that trunk. After a successful authentication all numbers related to the SIP trunk are implicitly registered.

Registrations as per RFC 6140 [14] are NOT supported at this stage and might be added in later versions.

The NGN uses the SIP-Digest authentication. Nextnonce mechanism as per RFC 2617 [15] shall be used to reduce signalling load (refer to 1TR114 [2] for more details about Nextnonce).

Private Identity and Password for every Trunk Group of a SIP Trunk are provided by Deutsche Telekom as part of the customer contract and are accessible in the customer web portal (‘Telefonie Benutzername/Passwort’)

NOTE: ‘Telefonie Benutzername’ has to be configured on SIP-PBX exactly as provided in customer web portal (with domain ‘@tel.t-online.de’).

NB: The private identity is equal to the pilot number for the trunk to be registered as depicted in the example below

Example:

```
REGISTER sip:tel.t-online.de:5060;transport=tcp SIP/2.0

    To: <sip:+49199296100xxxx@tel.t-online.de:5060;transport=tcp>

    From: <sip:+49199296100xxxx@tel.t-online.de:5060;transport=tcp>;tag=abc

    Call-ID: 1-2234@192.168.100.xxx

    CSeq: 1 REGISTER

    Authorization: Digest username=+49199296100xxxx@tel.t-online.de",realm="tel.t-
online.de",cnonce="6b8b4567",nc=00000001,qop=auth,uri="sip:tel.t-
online.de:5060;transport=tcp",nonce="xxx",response="yyy",algorithm=MD5

    Contact: <sip:+49199296100xxxx@192.168.100.xxx:5060>"
```

The 200 OK to the Register Request will not include any P-Associated-URI header field, as it is anyway not honoured by SIP-PBX Vendors, which learn the associated Numbers to a Trunk by other means.

The implicitly registered identities for a given pilot user registration can be seen in the customer self-administration portal of the ‘CompanyFlex’ product.

Example:

```
Session Initiation Protocol (200)
   Status-Line: SIP/2.0 200 OK
   Message Header
      Via: SIP/2.0/TCP 192.168.0.xxx:35823;received=80.156.51.xxx;rport=35823;branch=z9hG4bK940653da78f6efaef
         Transport: TCP
         Sent-by Address: 192.168.0.xxx
         Sent-by port: 35823
         Received: 80.156.51.xxx
         RPort: 35823
         Branch: z9hG4bK940653da78f6efaef
      To: <sip:+49199296100xxxx@tel.t-online.de;user=phone>;tag=h7g4Esbg_f9a0d6b6025035750d20116f11f5bbb
      From: <sip:+49199296100xxxx@tel.t-online.de;user=phone>;tag=b0248eef84
      Call-ID: 03fbee8c2385e5e6
      CSeq: 1040858242 REGISTER
      Contact: <sip:+49199296100xxxx@192.168.0.xxx:5060;transport=tcp>;expires=600;description="<sip:+49199296100xxxx@tel.t-online.de>"
```

The Reregistration timer shall be maximum 600 seconds.

5.2 Static mode

The static mode of operation is out of scope for this specification.

6 Codecs

6.1 Telephony Codecs

SIP-PBXs used for SIP-trunk shall support G.711a and should support G.722. A fallback to G.711a shall be possible.

The codecs G.711µ, G.729 and clear channel (RFC 4040 [16]) 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.

It is highly recommended to use a packetization Time (pTime) of 20ms for all Voice Codecs. Codecs with other pTime values up to and including 30ms shall be understood. A successful call setup for larger pTime values is not guaranteed.

It is recommended to use a maximum packet time (maxpTime) of 20ms for all Voice Codecs.

To avoid Codec Lockdown, it is highly recommended to only send one voice codec in the SDP answer.

6.2 Fax

SIP-PBXs used for SIP-trunk shall 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). (For details please refer to 1TR114 [2])

T.38 media encryption is not supported. Negotiations within an established connection for T.38 to a UE using encryption will be rejected with SIP Error code 488, so that fax transmission will use G.711 with encryption instead.

6.3 Video

Video is currently NOT supported.

7 Outbound Proxy Selection

If the access-line is provided by Deutsche Telekom, then the DNS server that is typically learned during the PPPoE Session setup shall be used for Outbound Proxy discovery.

The SIP-PBX shall discover the serving Outbound Proxy based on RFC 3263 [17]. That means, the SIP-PBX utilizes DNS NAPTR to determine the supported protocols (TCP or TCP over TLS) for the domain and SRV and A/AAAA Queries to determine hostnames, priorities, the IP Addresses and Port number of the NGN Outbound Proxy.

The outbound proxies that are used look as follows:

[integer string].primary.companyflex.de the mentioned integer string, as well as the other parts of the outbound proxy is shown in the customer portal.

The SIP-PBX can use TCP with RTP or TLS with SRTP as per Enterprise policy.

Standard query

Queries

[integer string].primary.companyflex.de: type NAPTR, class IN

Standard query response

Answers

[integer string].primary.companyflex.de. IN NAPTR 50 50 "s" "SIPS+D2T" _sips._tcp.primary.companyflex.de.

[integer string].primary.companyflex.de. IN NAPTR 100 50 "s" "SIP+D2T" _sip._tcp.primary.companyflex.de.

Standard query

Queries

_sips._tcp. [integer string].primary.companyflex.de: type SRV, class IN

Standard query response

Answers

_sips._tcp. [integer string].primary.companyflex.de: type SRV, class IN, priority 0, weight 5, port 5061, target server001.voip.t-ipnet.de

_sips._tcp. [integer string].primary.companyflex.de: type SRV, class IN, priority 1, weight 5, port 5061, target server002.voip.t-ipnet.de

_sips._tcp. [integer string].primary.companyflex.de: type SRV, class IN, priority 2, weight 5, port 5061, target server003.voip.t-ipnet.de

Additional records

server001.voip.t-ipnet.de: type A, class IN, addr 217.1.x.x

server002.voip.t-ipnet.de: type A, class IN, addr 217.1.y.y

server003.voip.t-ipnet.de: type A, class IN, addr 217.1.z.z

The SIP-PBX shall use the hostname with the highest priority as a Primary Outbound Proxy. Hostnames with lower priority shall be used only in case of failure of the Primary Outbound Proxy.

8 Redundancy and Failover

The SIP-PBX may detect an outage of a SIP Outbound Proxy with help of different methods:

- The NGN responds with a 503 without retry after
- The NGN does not respond at all (TCP Timeout)
- The SIP-PBX might actively monitor the NGN with SIP OPTIONS packets in a frequency not shorter than 30 seconds.
- The NGN might ask explicitly the SIP-PBX to register to another destination by the means of a SIP 305 Packet where the alternative destination resides in the contact header.

In case that the SIP-PBX detects a failure as described above, the SIP-PBX shall use the hostname determined with the DNS NAPTR/SRV procedure with the lower priority.

The SIP-PBX shall NOT initiate any connection (TCP, SIP) to secondary A-record answer if no failure on the Primary is detected.

It is recommended that the IP-PBX does not switch back to the primary SIP outbound proxy within 15 minutes in order to ensure that the environment there is in a stable condition again.

If an outage was detected and the SIP PBX switched to the secondary or tertiary A-Record, it should not stay permanently on this Proxy IP address, but should monitor the availability of the SIP Outbound proxy of the primary A-record, e.g. via SIP OPTIONS, and switch back in a timely manner as described above.

Permanent operation on the SIP Outbound proxy of the secondary or tertiary A-record shall be avoided.

8.1 SIP N-way Redundancy

To support an N-way-redundancy the SIP-PBX shall register (N-1) redundant trunks with dedicated pilot numbers different than the one used for the first trunk (see chapter 4.1)

It is highly recommended to use another access for the redundant trunks to decouple access problem from SIP Problem as in the following figure.

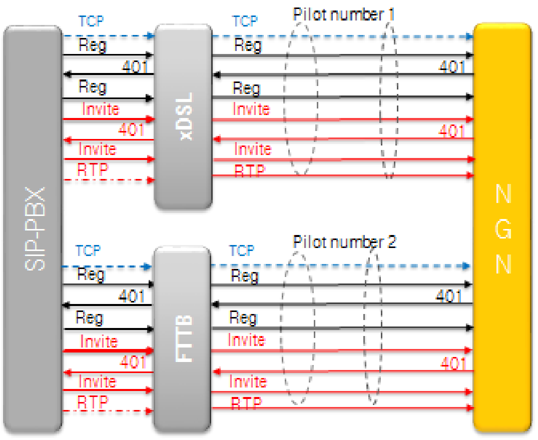

Figure 8-1: Redundant trunk registration (N=2) – simplified flow

In case of redundancy, the SIP registration of every pilot number implicitly registers the same set of number resources (DDI ranges or single numbers) which is associated with this redundant SIP Trunk.

Routing policies and number resources for the redundant SIP Trunk can be configured by the customer via NGN SIP Trunk Self-Administration portal.

Potential policies for a redundant SIP Trunk setup are load-sharing, failover, capacity management etc.

It is possible to register the second Trunk to a different outbound Proxy by using the domain [integer string].secondary.companyflex.de. The procedure is the same as explained in Chapter 7.

8.1.1 Trunk Capacity Management

The customer's administrator may configure limits on active incoming calls, active outgoing calls, or all active calls (the sum of incoming and outgoing calls) for every dedicated redundant trunk.

For each new outgoing call, the NGN checks the capacity limits for all active calls and active outgoing calls. If the new call does not violate the capacity limits, then the NGN allows the call to continue. However, if the new call exceeds the capacity limit for all calls or for outgoing calls, the NGN blocks the call by sending a SIP 403 (Forbidden) response to the SIP INVITE request.

SIP-PBX which support SIP N-Way Redundancy according to clause 8.1 shall re-attempt to send an outgoing initial SIP INVITE request via an alternative trunk in case in case the NGN responds with SIP 403 (Forbidden) on the initial call attempt.

Details of the retry mechanism are SIP-PBX implementation specific but a SIP 403 (Forbidden) is used by the NGN to indicate that the capacity limit for a specific trunk is exceeded and re-routing shall be applied.

8.1.2 Outbound Proxy Reselection due to changed DNS response

As described in section 7, IP addresses of Outbound Proxys are learnt via DNS procedures.

When results of the DNS procedures deliver new hostnames or IP addresses it is expected that the SIP-PBX honours those changes and adjust the registration behaviour accordingly.

When doing so, SIP-PBX need to consider active calls, as these are bound to the currently used Outbound Proxy IP address. When registration is switched during active calls, calls will be aborted.

For installations with continuous operations, without any phase without calls, multiple trunks need to be set up. In this case a trunk will be drained of active calls and reject new calls before registration is switched to a different IP address, to avoid aborted calls.

9 IP and Transport

9.1 IP-addresses

If NAT is not applied, a SIP-PBX connected to the NGN may use different IP-addresses for SIP-signalling and media. IPv6 and IPv4 are supported.

Both SIP-signalling and media shall use either IPv4 or IPv6, but no mixture.

9.2 IPv6

The IPv6 multicast (ff00::/8) addresses shall NOT be used for SIP Trunking.

Global unicast Addresses shall be used instead (fc00::/7 -- fc00:: - fdff::).

It is highly recommended NOT to use NAT in IPv6 Networks.

9.3 Transport Protocols

A SIP-PBX connected to the NGN shall use TCP or TLS over TCP as transport protocol for SIP-signalling.

UDP is not supported as transport protocol for SIP-signalling.

Voice (RTP/SRTP) however uses UDP as transport protocol.

9.4 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 shall send this information in the VIA and CONTACT header fields.
- SIP-PBXs not knowing the public IP-address and public port information shall send a private IP-address (RFC 1918 [18]) in the VIA and CONTACT header fields. In that case the SIP-PBX shall 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 shall set-up the SIP transport protocol sessions, monitor their status, send CR/LF keep-alive messages as per RFC 5626 [19] and activate or failover accordingly.
- SIP-PBXs shall use the same IP-address for SIP-signalling and media traffic
- The SIP-PBX shall reuse already existing TCP and TLS-connections to send and receive SIP-messages.

For keeping the NAT-Pinholes open for media, empty (no payload) RTP packets with payload type of 20 shall be sent by the SIP-PBX to the next hop session media ports: If the value 20 has already been negotiated then some other unused static payload type from Table 5 of RFC 3551 [20] shall be used.

SIP OPTIONS and Frequent Reregistration shall NOT be used as a keep-alive mechanism for NAT-Traversal.

9.5 TCP Connection Re-Use

If a SIP UA with a public IP address establishes a TCP connection on an ephemeral TCP port (e.g. 12345) and sends an INVITE where the Contact header field is not filled with its IP address and the ephemeral port but e.g. 5060, Requests will not be sent in the existing TCP session but the P-CSCF will establish a new TCP session.

9.6 SIP Message Size

A SIP Message Size of 8kB shall be supported to guarantee a successful call setup.

NOTE: One example for such large calls is a VoLTE emergency call with UE provided location information.

10 Signalling and media security

The NGN supports end-to-access-edge encryption for signalling and (S)RTP-media as in 1TR114 [2]. End-to-end encryption for signalling or media is not supported.

10.1 SIP security

SIP over TLS (v1.2 or higher) 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 shall be initiated and maintained by the SIP-PBX and it shall be successfully setup before the SIP-PBX sends the REGISTER request.

Rekeying is NOT supported.

10.2 Deutsche Telekom Certificate download

SIP-PBX shall install locally the certificate of Telesec Root-CA (manually) or it is pre-installed by the vendor of the corresponding operating system / SIP software.

The certificate is **T-TeleSec GlobalRoot Class 2** with fingerprint 590d2d7d884f402e617ea562321765cf17d894e9

https://telesec.de/de/root-programm/informationen-zu-ca-zertifikaten/root-zertifikate/

Conversion into other certificate formats can be done using tools like OpenSSL. This link is subject to change by Telesec.

NB: Depending on the certificate being used, only Telesec Root Certificate is required.
SIP-PBX shall check the validity of the certificate provided by P-CSCF with help of root certificate.

NB: Although RFC 5922 [21] is not allowing wildcard certificates, Deutsche Telekom expects and requires PBX-Vendors to support it

10.3 Media Encryption

The NGN supports media encryption between the SIP-PBX and the NGN optionally. RTP-traffic may be encrypted using SRTP (RFC 3711 [5]) between the SIP-PBX and the Deutsche Telekom’s NGN (end-to-access edge encryption). SDES (RFC 4568 [6]) 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 only for 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 [6]. If the SIP-PBX rejects the RTP encryption, the call is lost, Fallback to RTP is not allowed according to the RFC 4568 [6].

A SIP-PBX which is configured to use TLS with SRTP shall only provide RTP/SAVP in SDP offer.

A SIP-PBX which is configured to use TCP with RTP shall only provide RTP/AVP in SDP offer.

A SIP-PBX shall 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.

In case of media encryption, the transmission of fax is only possible via SRTP. T.38 Fax over UDPTL is rejected.

If media encryption is applied, the mediasec header field parameter as defined in chapter 7.2A.7 of 3GPP TS 24.229 [13] and draft-dawes-sipcore-mediasec-parameter [12] and the header fields Security-Client, Security-Server and Security-Verify as defined in RFC 3329 [11] shall be supported. Additionally, an SDP "a=3ge2ae:requested" attribute as described in chapter 6.1.2 of 3GPP TS 24.229 [13] shall be included in every Request and Response with SDP.

NOTE: While a registration may be successful without the parameters mentioned above, incoming and/or outgoing calls may not be possible.

10.3.1 REGISTER

For an initial REGISTER without Authentication Challenge, the SIP header fields

- `Security-Client: sdes-srtp;mediasec`
- `Proxy-Require: mediasec`
- `Require: mediasec`

shall be included. The platform will reply with SIP 401 Unauthorized including the SIP header fields

- `Security-Server: msrp-tls;mediasec`
- `Security-Server: sdes-srtp;mediasec`
- `Security-Server: dtls-srtp;mediasec`

indicating the possible encryption methods.

For the following REGISTER with Authentication Challenge, in addition to the originally included SIP header fields Security-Client, Proxy-Require, Require, the SIP header fields

- `Security-Verify: msrp-tls;mediasec`
- `Security-Verify: sdes-srtp;mediasec`
- `Security-Verify: dtls-srtp;mediasec`

shall also be included. In accordance with RFC3261, the Security-Verify header fields can also be combined as one single header field.

Please see Figure 10-1 for an exemplary call flow.

```
IP-PBX                                           P-CSCF
   |                                               |
   |----(1) REGISTER------------------------------>|
   |        Security-Client: sdes-srtp;mediasec    |
   |        Proxy-Require: mediasec                |
   |        Require: mediasec                      |
   |                                               |
   |<---(2) 401 UNAUTHORIZED-----------------------|
   |        Security-Server: msrp-tls;mediasec     |
   |        Security-Server: sdes-srtp;mediasec    |
   |        Security-Server: dtls-srtp;mediasec    |
   |                                               |
   |----(3) REGISTER (with Authorization Header)-->|
   |        Security-Client: sdes-srtp;mediasec    |
   |        Proxy-Require: mediasec                |
   |        Require: mediasec                      |
   |        Security-Verify: msrp-tls;mediasec     |
   |        Security-Verify: sdes-srtp;mediasec    |
   |        Security-Verify: dtls-srtp;mediasec    |
   |                                               |
   |<---(4) 200 OK---------------------------------|
```

Figure 10-1: Exchange of media security mechanisms at initial registration

10.3.2 INVITE/UPDATE

In order to signal the use and type of encryption, the initial INVITE shall include the SIP header fields

- `Proxy-Require: mediasec`
- `Require: mediasec`
- `Security-Verify: msrp-tls;mediasec`
- `Security-Verify: sdes-srtp;mediasec`
- `Security-Verify: dtls-srtp;mediasec`

Additionally, the SDP shall include the attribute

- `a=3ge2ae:requested`

to define the range of the encryption, that is between IP-PBX and registration server. In accordance with RFC3261, the Security-Verify header fields can also be combined as one single header field.

If a Re-INVITE or UPDATE is initialised from the SIP client, the SIP header fields and SDP attribute mentioned above shall be included again.

Please see Figure 10-2 for an exemplary call flow.

```
IP-PBX                                           P-CSCF
   |                                               |
   |----(1) INVITE (SDP)-------------------------->|
   |        Proxy-Require: mediasec                |
   |        Require: mediasec                      |
   |        Security-Verify: msrp-tls;mediasec     |
   |        Security-Verify: sdes-srtp;mediasec    |
   |        Security-Verify: dtls-srtp;mediasec    |
   |        a=3ge2ae:requested                     |
   |        a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:EpcgtOdT5...
   |                                               |
   |<---(2) 100 TRYING-----------------------------|
   |                                               |
   |<---(3) 180 RINGING----------------------------|
   |                                               |
   |<---(4) 200 OK (SDP)---------------------------|
   |        a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:lnfakjh2s...
```

Figure 10-2: Exchange of media security mechanisms for INVITE

10.3.3 Response

An incoming INVITE from the platform will include the SDP attribute

- `a=3ge2ae:applied`

All responses with SDP (e.g. 18x or 200OK) shall include the SDP attribute

- `a=3ge2ae:requested`

Please see Figure 10-3 for an exemplary call flow.

```
IP-PBX                                           P-CSCF
   |                                               |
   |<---(1) INVITE (SDP)---------------------------|
   |        a=3ge2ae:applied                       |
   |        a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:EpcgtOdT5...
   |                                               |
   |----(2) 100 TRYING---------------------------->|
   |                                               |
   |----(3) 180 RINGING--------------------------->|
   |                                               |
   |----(4) 200 OK (SDP)-------------------------->|
   |        a=3ge2ae:requested                     |
   |        a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:lnfakjh2s...
```

Figure 10-3: Exchange of media security mechanisms for Responses

10.4 NTP

Although NTP is not required for basic SIP Trunking several SSL/TLS clients mandate NTP to successfully verify the certificate revocation list during TLS connection setup.

11 Emergency Calls and Special Numbers

11.1 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 (also including carrier prefix).

As priority, user location information is determined using the source IP address in the IP packet carrying the INVITE message. With second priority, location information is determined via the identity (i.e. phone number, see clause 4.1). If location information can be determined by neither method, the emergency call centre will be determined via NDC of the caller.

Further details can be found under https://hilfe.companyflex.de/.

11.2 Special numbers

Special numbers shall be sent as dialled and not in E.164 format towards NGN according to Bundesnetzagentur.

The List of special numbers is as follows and where x = 1-9 and y = 0-9:

- 010xy, Call by Call e.g. 010130<NDC><SN>
- 0100yy, Call by Call e.g. 0100490<NDC><SN>
- 116xxy, e.g. 116116
- 118xy, e.g. 11833
- 1180yy
- 11800x
- 110 and 112

NOTE: The administration's call 115 has been changed to a geographical number, hence it can either be dialled with NDC or as 115 which will subsequently be normalized to 0<NDC>115.

11.3 DTMF

For DTMF events RFC 4733 [7] and RFC 5244 [9] shall be supported.

For support of DTMF RTP Out-of-Band in binary format (RFC 4733 [7] and RFC 4734 [8]) shall be supported.

NOTE: In cases where the remote Endpoint does not support RFC4733 [7] it shall be possible to send DTMF in-band.

11.4 Early Media Support

Early media and the P-Early-Media header field shall 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 field should be able to detect early media and be prepared to generate the ringback tone locally if no early media is received.

12 Basic Call

12.1 Incoming Calls from the Service Provider to SIP-PBX

The UE/SIP-PBX shall display the identity provided in the From Header, since a P-Asserted-Identity header field may not be available in all cases.

The Identity of the callee is in the Req-URI as per SipConnect 2.0 [22]. The UE/SIP PBX must support the SIP History-Info header field as specified in RFC 7044 [10].

```
Request-Line: INVITE sip:+499125580xxxx@tel.t-online.de; transport=tcp SIP/2.0
Message Header
   Max-Forwards: 68
   Via: SIP/2.0/TCP 80.156.151.xxx:5060;branch=z9hG4bKg3Zqkv7ic1pmi9jo7htl6mhvj2i8slzno
   To: <sip:+499125580xxxx@tel.t-online.de;user=phone>;cscf
   From: <sip:+492284225xxxx@tel.t-online.de;user=phone>;tag=h7g4Esbg_2044599896-1531919887568-
   Call-ID: BW151807568180718318543956@10.102.237.2
   CSeq: 382023273 INVITE
   Contact: <sip:sgc_c@80.156.151.xxx;transport=tcp>
   Record-Route: <sip:80.156.151.xxx;transport=tcp;lr>
   Accept-Contact: *;explicit;description="<sip:+49199296100xxxx@tel.t-online.de>";require
   Min-Se: 900
   Privacy: none
   Session-Expires: 1800;refresher=uac
   Supported: 100rel
   Supported: timer
   Content-Type: application/sdp
   Content-Length: 164
   Recv-Info: x-broadworks-client-session-info
   Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY, UPDATE
   Accept: application/btbc-session-info
   Accept: application/dtmf-relay
   Accept: application/media_control+xml
   Accept: application/sdp
   Accept: multipart/mixed
   History-Info: <sip:+499125580xxxx@tel.t -online.de;transport=tcp;user=phone >;index=1,
                 <sip:+49170780xxxx@tel.t -online.de;transport=tcp;user=phone>;index=1.1,
                 <sip:+496151583xxxx@tel.t-online.de;transport=tcp;user=phone;cause=302>;index=1.1.1
```

12.2 Outgoing calls from SIP-PBX to the service provider

The SIP-PBX shall not make use of diversion header fields in outgoing calls. These header fields when coming from SIP-PBXs are ignored in the NGN.

The session Timer shall be set to 1800.

```
Request-Line: INVITE sip:+492284225xxxx@tel.t-online.de;user=phone;transport=tcp SIP/2.0
Message Header
    Via: SIP/2.0/TCP 192.168.2.xxx:37673;branch=z9hG4bK92c218a2a66b89b0f;rport
    Route: <sip:80.156.151.xxx;lr;transport=tcp>
    Max-Forwards: 70
    From: <sip:+499125580xxxx@tel.t-online.de;user=phone>;tag=4b73a8d7eb
    To: <sip:+492284225xxxx@tel.t-online.de;user=phone>
    Call-ID: 988a2dd34c2ba580
    CSeq: 1914213343 INVITE
    Allow: INVITE, ACK, OPTIONS, BYE, CANCEL, REGISTER, INFO, UPDATE
    Contact: <sip:+49199296100xxxx@192.168.2.xxx:37673;transport=tcp;user=phone>
    Min-SE: 900
    Session-Expires: 1800
    Supported: 100rel, timer
    P-Preferred-Identity: <sip:+4991255804xxxx@tel.t-online.de;user=phone>
    User-Agent: SIP-PBX-VENDOR
    Content-Type: application/sdp
    Content-Length: 306
```

12.3 Sending of non-100-Responses

When the UA receives an initial INVITE, the UA shall immediately send a non-100 response corresponding to its status (e.g. 180 Ringing, 181 Call is being forwarded, 183 Session Progress) in order to trigger playing ringtone to the calling party and to avoid cancelling or rerouting of the call to an alternative trunk group. Rerouting and call cancelling are applied by the NGN after 3s without receiving a non-100 response on an initial INVITE.

NOTE: The supervision timer of currently 3s can be configured per trunk group in the CompanyFlex portal.

13 Supported Services

Most of the NGN based services can be configured by the customer in the NGN SIP Trunk Self Administration portal.

13.1 CLIP/CLIR (OIP/OIR)

CLIP (OIP) enables displaying the telephone number of the originating A-subscriber towards the 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. CLIP/OIP is always enabled for NGN SIP Trunks and can't be disabled.

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 CLIR can be controlled by the customer in the self-administration portal of the product.

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.

13.2 COLP/COLR (TIP/TIR)

The NGN-based TIP/TIR service is described in 1TR114 [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 COLR/TIR can be controlled by the customer in the self-administration portal of the product. COLP/TIP is always enabled for NGN SIP Trunks and can't be disabled.

13.3 CLIP no Screening

CLIP no screening allows the presentation of an arbitrary chosen E.164 number in the From header field even out of prefix ranges assigned to the SIP-Trunk of calling party.

If the phone number in the From header field is not in E.164 format, then the NGN converts it to international E.164 format.

- NGN strips any national prefix.
- NGN prepends a plus sign and the country code from the called number.

In the P-Preferred-Identity or in the P-Asserted-Identity header a number from the range of the prefix of the SIP-Trunk shall be provided. Otherwise calls will be rejected.

The feature's state of CLIP no screening applies at the SIP-trunk-level.

It is in the responsibility of the calling party not to use forbidden numbers in From header field according to TKG §66k/TKG§120.

In the future, calls using forbidden numbers in From header field according to TKG§120 will be rejected.

13.4 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 SIP-PBX shall add a SIP History-Info header field.

The SIP-PBX shall not insert the transport parameter in the Contact header of the 302 SIP response.

The NGN will forward the INVITE to the new target and send a 181 SIP response to the caller.

13.5 Call Forwarding by New INVITE

To forward with a new INVITE (on or out of dialog), the SIP-PBX must follow the procedures in SIPCONNECT 2.0 [22] Chapter 11.1 with the following clarifications:

- The request-URI identifying the forwarded-to target destination.
- A History-Info header field containing the Enterprise Public Identity of the forwarding user
- A P-Asserted-Identity header field or P-Preferred-Identity header field containing a valid identity of the forwarding user.
- In order to enable the NGN to supervise the status of the call setup towards a SIP-PBX in case of call forwarding, the SIP-PBX shall generate a 18x response message (181 (Call is Being Forwarded) or 183 (Session Progress) without SDP) and send it to the originating user as soon as the call forwarding has been applied.
- In case a 181 response is sent to the originating user with information about the diverted-to identity, the SIP-PBX shall include a SIP URI of the diverted-to user into a History-Info header field in a 181 (Call Is Being Forwarded) response message and send it to the originating user. As it is not known what the diverted-to user's TIR settings are, a Privacy header field with a priv-value set to "history" needs to be included in escaped form in the hi-entry representing the diverted-to user.
- In case a 180 (Ringing) has been received from the diverted-to user, a 180 response (with or without SDP) shall be sent to the originating user.

Please note that in case of Call Forwarding without proper History-Info header field, the identity in FROM-header field will be screened by the network. In case the original caller identity shall be transported transparently, then either History-Info header field or CLIP No Screening is necessary.

13.6 Call Transfer

Call Transfer is supported using INVITES/re-INVITE. This is in accordance with the recommendations of SIPCONNECT 2.0 [22].

13.7 Call by Call

The feature Call by Call allows the SIP-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.

13.8 Advice of Charge

AoC is currently not supported.

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

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.

13.10 Sending and Receiving SIP Options

13.10.1 Sending SIP Options (to P-CSCF)

SIP OPTIONS may be sent by the PBX with an interval of at least 30s to check the availability of the P-CSCF. SIP OPTIONS will only be successfully acknowledged with SIP 200 (OK) if the IP address of the P-CSCF is sent in both the Request Line and the To header field, otherwise they will be declined with a SIP 403 (Forbidden).

SIP OPTIONS should only be sent to those P-CSCF where a registration is present, using the same transport (TCP connection) as used for the registration.

13.10.2 Receiving SIP Options (from P-CSCF, only Emergency Centres)

SIP OPTIONS are used to check the availability of a PSAP-PBX. The PBX shall respond to an OPTIONS request with 200 OK if it is running properly.

13.11 REFER

The REFER method is not supported. For details on how to interwork a REFER method to an INVITE, please see chapter 4.7.2.9.7 of 3GPP TS 24.628 [23].

Annex

14 Annex for Emergency Centres

This annex describes the special implementation behaviour of Emergency End devices used by PSAP e.g. police force, fire brigade etc. Additionally, to the listed features/configuration in this TR, the PSAP-PBX shall support the requirements in this annex.

14.1 Caller Identity Handling for Outgoing Calls (from the PSAP-PBX)

Within the context of an PSAP-PBX the PBX is not allowed to send outgoing calls, i.e. no INVITE.

The PSAP-PBX shall have the possibility to configure such a profile or Outgoing Call Barring for registered PSAP IMPUs.

NOTE: The NGN has a specific profile for PSAPs which also blocks the related PSAP IMPUs for outgoing calls.

14.2 Network Services

14.2.1 CLIR (OIR) Override

CLIR (OIR) restricts the presentation of the telephone number of the A-subscriber (feature's user) at the B-subscriber. For PSAP-PBX accounts the OIR override feature for terminating calls is permanently configured for the PSAP-MSN.

If privacy extensions are received it shows that the originating party has subscribed to the OIR services. Nevertheless, in any case the PSAP-PBX shall present the identity of the originating party.

NOTE: Based on the network configuration such privacy extensions may be deleted.

14.2.2 COLP/COLR (TIP/TIR)

For SIP-trunking, COLR (TIR) provides the restriction of the presentation of the phone number from the called party to the calling party, permanent or per call. For the PSAP-PBX the TIR service is activated permanently.

14.2.3 Call Barring

Barring of numbers is supported for incoming and outgoing calls. Barring is used by administrating a blacklist and/or whitelist. Barring can be administered by the VoIP provider and the business customer. Configured black- and/or whitelists applies on SIP-trunk-level.

Outgoing call barring is permanently activated on network level for a PSAP-PBX.

Outgoing call barring on PSAP-PBX level may apply in addition.

14.3 Echo Cancellation

In case where an echo can appear the PSAP-PBX shall support a proper echo cancelation according to international standards like ITU-T G.168 [28].

14.4 Protocol Profiles

According to the emergency requirements in Germany, a PSAP-PBX shall support the following SIP Elements:

- SIP Geolocation Header Field and PIDF-LO MIME-Body according to RFC 6442 [24] and RFC 5491 [31]
- SIP Location Source Header Field Parameter according to RFC 8787 [30]
- SIP User to User Information (UUI) Header Field according to RFC 7433 [25] for the transport of Provider Info, eCall Indicator and Location Data
- SIP Emergency Provider Info according to RFC 7852 [27] for the transport of Provider Data. Earlier draft versions of RFC 7852 [27] instead used the ContentType "application/EmergencyCall.ProviderInfo+xml" and the XML Element "emergencyCall.ProviderInfo" for the transmission of the Provider Data. Deutsche Telekom has no influence on the sent Provider Data and strongly recommends Emergency Call Centres to support both types for backward compatibility reasons.
- eCall Indicator using Comment Block of RFC 7852 [27] or earlier draft versions as described in TR Notruf
- Originating access information using P-Access-Network-Information (PANI) Header Field according to RFC 7315 [26]
- Outlook: In future MIME Bodys application/EmergencyCallData.eCall.MSD and application/EmergencyCallData.Control+xml according to RFC 8147 [32] will be used to transport NG eCall data. This is subject for future regulation.

NOTE 1: If multiple P-Access-Network-Info header fields are received, they will be combined and sent as a single header field with multiple comma-separated header field values, e.g. P-Access-Network-Info: 3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=2620100791d31a00;network-provided,3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=2620100791D31A00

NOTE 2: Deutsche Telekom is forwarding all additional emergency call-related information in headers and bodies received from the originating telephony domains like fixed line or mobile domains of Deutsche Telekom or other Carriers transparently to the Emergency Call Centres. Hence, originating domains are responsible for SIP message size, headers and bodies.

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
NDC	National Destination Code
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-	
R-URI	Request-URI
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
SN	Subscriber Number
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-	