

Dokumentation Schnittstellenbeschreibung Business VoiP

Version 1.0

Inhaltsverzeichnis

1	Einleitung	4
2	Referenzen	4
2.1	Normative Referenzen	4
2.2	Informative Referenzen	5
2.3	Referenz Quellen	5
3	Anschlussinformationen	6
3.1	Anbindung und Redundanz	6
3.2	Rufnummern.....	7
4	SIP-Trunk-Eigenschaften.....	8
4.1	Internet Protocol (IP)	8
4.2	Firewall, NAT, STUN	8
4.3	Session Initiation Protocol (SIP).....	10
4.3.1	SIP Header eingehende Anrufe.....	10
4.3.1.1	'Request-URI' Format	10
4.3.1.2	'From' Header Format.....	10
4.3.1.3	'To' Header Format	10
4.3.1.4	'P-Asserted-Identity' Header Format	11
4.3.1.5	Diversion Header.....	11
4.3.2	SIP Header abgehende Anrufe.....	11
4.3.2.1	'Request-URI' Format	11
4.3.2.2	'From' Header Format.....	12
4.3.2.3	'To' Header Format	12
4.3.2.4	'P-Asserted-Identity' Header Format	12
4.3.2.5	'P-Preferred-Identity' Header Format	12
4.3.2.6	'Diversion' Header Format	13
4.3.3	Reliability of Provisional Responses – PRACK (RFC 3262).....	13
4.3.4	Offer/Answer Model (RFC 3264)	13
4.3.5	Privacy (RFC 3323 und 3325)	13
4.3.6	Display Name (RFC 3261).....	13
4.3.7	History Info (RFC 4244)	13
4.3.8	OPTIONS Ping (RFC 3261).....	13
4.3.9	P-Early Media-Header (RFC 5009).....	14
4.3.10	UPDATE Method (RFC 3311)	14
4.4	Session Description Protocol (SDP).....	14
4.4.1	Payload Types.....	14
4.4.2	Media Description (m=)	14
4.4.3	Bandwidth (b=)	14
4.5	Verschlüsselung (TLS/sRTP).....	14
4.6	Abbildung von ISDN-Leistungsmerkmalen	15
4.6.1	CLIP (OIP)	15
4.6.2	CLIP–no-screening	15
4.6.3	CLIR (OIR)	15
4.6.4	COLP (TIP).....	16
4.6.5	COLR (TIR)	17
4.6.6	Rufumleitung.....	18
4.6.7	Halten (Call Hold).....	19

4.7 Nutzkanal-Eigenschaften..... 19

4.7.1 Codecs..... 19

4.7.2 DTMF (Named Telephone Events) 19

4.7.3 Fax 19

5 Timer configuration..... 19

6 Notruf..... 20

7 Definitionen und Abkürzungen..... 21

1 Einleitung

Der Vodafone **Business VoIP-Anschluss** bietet die Möglichkeit, eine IP-TK Anlage oder ein ISDN Gateway direkt über IP unter Verwendung des Session Initiation Protocols (SIP) mit dem Telekommunikationsnetz von Vodafone zu verbinden und für ausgehende sowie ankommende Sprach- und Faxverbindungen zu nutzen.

Dieses Dokument beschreibt die Schnittstelleneigenschaften des Business VoIP-Anschlusses, die bei der Installation und Konfiguration einer IP-TK Anlage zu berücksichtigen sind.

Beispiele für die SIP-Signalisierung sind in vereinfachter Form dargestellt und erheben keinen Anspruch auf Vollständigkeit.

2 Referenzen

2.1 Normative Referenzen

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 4733	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 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
RFC 5009	P-Early Media

2.2 Informative Referenzen

bitkom	"SIP Trunking - Detailempfehlungen zur harmonisierten Implementierung in Deutschland", 2011, basierend auf der Technical Recommendation SIPconnect 1.1.
SIP Forum	SIPconnect 2.0 Technical Recommendation
UAK-S/AKNN	Specification of the NGN Interconnection Interface

2.3 Referenz Quellen

- 3GPP: <http://www.3gpp.org>
- bitkom: http://www.bitkom.org/de/publikationen/38337_70723.aspx
- 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 Anschlussinformationen

Vodafone liefert für einen Business VoIP-Anschluss die folgenden Informationen, die für die Konfiguration der TK-Anlage nötig sind:

- **Vodafone-Rufnummern inklusive Rufnummernblock** gemäß Vertragsdaten
- **SIP Zugangsdaten:**
 - Zuständiger SBC als Fully Qualified Domain Name (FQDN, z.B.: sbc-pool1-sipt.vf-office.net)
 - Konfigurierte P-Preferred-ID (PPI, entspricht Pilotnummer der TK-Anlage)
 - Domain der SIP URI (z.B. ims_sip_domain.de)
 - Transportprotokoll & Port

3.1 Anbindung und Redundanz

Auf dem Internet-basierenden Access ist eine feste IP-Adresse für den Business VoIP vorzusehen. Weiterhin ist QoS für die Sprachübertragung empfohlen.

Für Business Voice stehen mehrere geographisch getrennte SBC Paare als Zugangspunkte in das Vodafone Netz zur Verfügung.

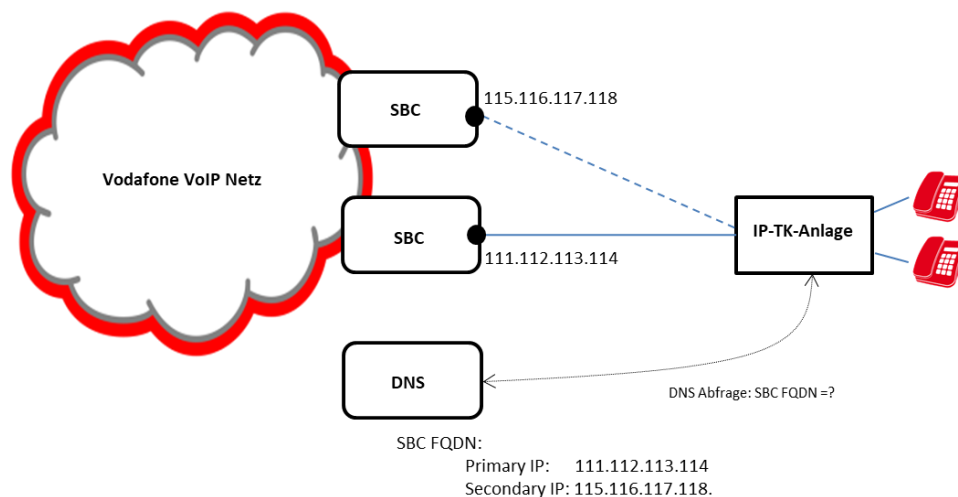


Abbildung 1: Redundante Anbindung

SBC Paare in HA (High Availability) mode sind an unterschiedlichen Standorten in Deutschland verteilt, um Geo-Redundanz und Loadsharing zu ermöglichen.

Das Vodafone Netz ist für die TK-Anlage nur über ein solches SBC-Paar erreichbar. Die TK-Anlage muss in der Lage sein, über externe DNS Auflösung des von Vodafone zur Verfügung gestellten zuständigen SBC FQDN die IP Adresse des SBC zu ermitteln. Dazu muss die TK-Anlage DNS SRV Records nach RFC 3263 unterstützen. Die DNS Auflösung liefert zwei IP Adressen mit unterschiedlicher Priorität zurück – die erste ist die primäre IP Adresse des Heimat SBC und soll ausschliesslich von der TK-Anlage für die SIP Signalisierung verwendet werden. Die zweite IP Adresse weist auf das redundante SBC Paar und soll von der TK-Anlage nur verwendet werden, wenn die primäre Adresse nicht antwortet und es zu einem Timeout kommt.

Dieser Mechanismus sollte stateless sein, das heisst, nach einem erfolgten Timeout, soll Signalisierung für neue Anrufe von der TK-Anlage wieder zu der primären Adresse geroutet werden. Ein direktes Routen zu der zweiten IP Adresse sollte nicht erfolgen.

Wenn die TK Anlage keine SRV Records unterstützt, ist keine Redundanz bei Ausfall oder Nichterreichbarkeit eines SBC HA Paares gegeben.

3.2 Rufnummern

Damit der Angerufene die korrekte Rückrufnummer angezeigt bekommt, müssen die Rufnummern der TK Anlage einem standardisierten Rufnummernplan entsprechen.

Gemäß RFC 3966 werden Rufnummern möglichst im globalen Format als E.164-Nummer (also in internationalem Format, beginnend mit + und Country Code, z.B.: +49 211 12345678) signalisiert. Teilweise werden auch nationale Formate akzeptiert, z.B.: 0211 12345678.

Falls in der TK-Anlage Rufnummern falsch konfiguriert sind (Rufnummern, die nicht zum Rufnummernblock gemäß Vertragsdaten passen), wird dem Angerufenen immer die Pilotnummer angezeigt, sofern das Feature CLIP no Screening nicht aktiv ist. Die Pilotnummer entspricht der in den SIP Zugangsdaten festgelegten PPI.

Der Business VoIP Anschluss arbeitet mit festen Rufnummernlängen. Die in der TK Anlage konfigurierten Rufnummern müssen der im Netz konfigurierten Ziffernlänge entsprechen.

4 SIP-Trunk-Eigenschaften

Um die Interoperabilität zwischen der TK-Anlage und dem Vodafone-Netz zu gewährleisten, müssen einige Voraussetzungen auf verschiedenen Protokollebenen erfüllt sein, die im Folgenden beschrieben sind.

4.1 Internet Protocol (IP)

Die TK-Anlage benötigt eine statische IP-Adresse für den IP Anlagen-Anschluss, die Vodafone bekannt sein und aus dem Netz von Vodafone erreichbar sein muss. Vodafone akzeptiert nur Verbindungsversuche von diesen IP-Adressen in Verbindung mit zugewiesenen Rufnummern.

Die SIP-Signalisierung erfolgt in beide Richtungen über UDP und Port 5060. Für RTP/RTCP werden seitens Vodafone UDP-Ports 10000 bis 25999 genutzt.

TCP wird für Business Voice nicht unterstützt, daher wechselt der SBC entgegen RFC3261 bei Überschreitung der MTU Size auch nicht auf TCP. Fragmentierte UDP-Pakete werden vom SBC akzeptiert.

4.2 Firewall, NAT, STUN

Die TK-Anlage kann möglicherweise hinter einer kundenseitigen Firewall oder einem Network Address Translation (NAT) Device stehen. Das NAT Device oder die Firewall muss SIP und RTP Verkehr zwischen dem Vodafone SBC und der TK-Anlage zulassen. Vodafone ist nicht für die Konfiguration der Firewall verantwortlich.

NAT Devices außerhalb des Vodafone Netzes werden primär in Kombination mit Fixed Broadband Access verwendet. In der Regel werden sie am Kundenstandort oder im Zugangsnetz eingesetzt. Werden mehrere NAT Devices außerhalb des Vodafone Netzes eingesetzt, ist die Annahme, dass sich der Effekt solchermaßen aufsummiert, das sie als ein einziges NAT Device betrachtet werden können.

Allgemein wird NAT Traversal für Signalisierung in 3GPP TS 23.228 und 3GPP TS 24.229 spezifiziert.

Ist die SIP Anwendung auf der Kundenseite nicht gewahr, dass sie sich hinter einem NAT Device befindet und eine private IP Adresse verwendet, bietet der Vodafone SBC eine limitierte NAT Traversal Funktionalität und schickt Antworten an die öffentliche IP Adresse, von denen er Nachrichten erhält. Die kundenseitige Firewall darf diese Antworten nicht blockieren.

Bei UDP als Transportprotokoll muss das NAT Device sicherstellen, dass die öffentlichen IP Adresse für die SIP Signalisierung den Port 5060 zum Senden und Empfangen verwendet. Abhängig vom Device, kann es gegebenenfalls STUN Binding Requests als keep-alive Mechanismus verwenden, um NAT bindings für Signalisierung über UDP aufrecht zu erhalten. Vodafone bietet keine STUN Funktionalität an und STUN Nachrichten zum STUN Server eines Drittanbieters dürfen keinen Einfluss auf die Kommunikation zwischen dem Device und dem Vodafone SBC haben.

Die TK-Anlage sollte konfigurierbare IP-Ports für SIP Signalisierung und RTP unterstützen.

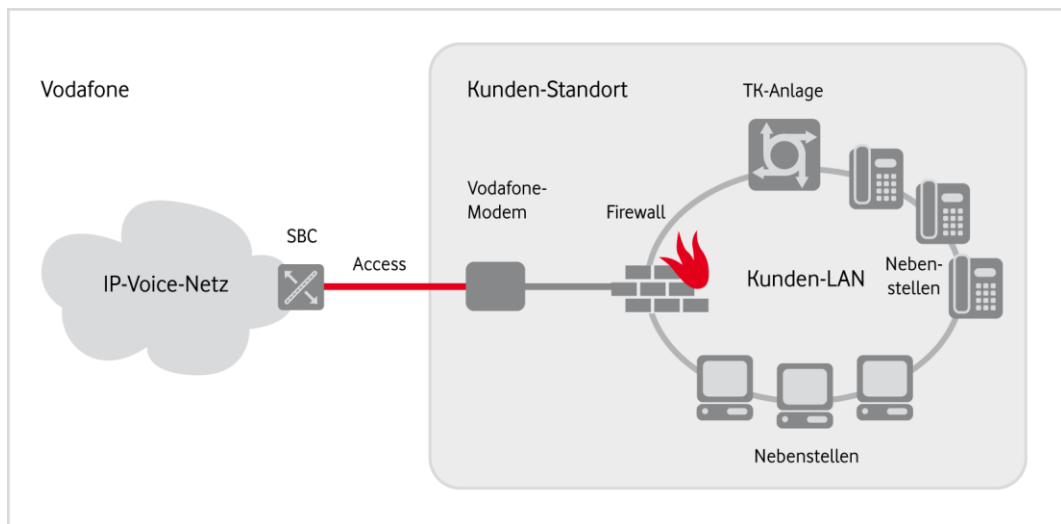


Abbildung 2: Firewall/NAT Device

Beachten Sie folgende Information zu Abbildung 22:

- **Vodafone-Router:** Der Router bildet den Daten-Access-Abschluss. Er ist über eine feste öffentliche IP-Adresse für den Business VoIP Anschluss erreichbar (im folgenden Beispiel über 111.112.113.114)
- **Firewall:** In der Konfiguration der Firewall muss sichergestellt sein, dass die netzseitige Kommunikation mit der TK-Anlage über die öffentliche IP-Adresse und die dazu gehörenden Ports erfolgt.

Beispiele	Firewall-Regeln				
	Richtung	Quelle	Ziel	Port	Protokoll
Eingehend	SBC: 111.112.113.114	Ext. IP der Firewall: 123.123.123.123	5060	UDP	Weiterleiten an 192.168.178.101:5060 ⁽¹⁾
Ausgehend	TK-Anlage: 192.168.178.101	SBC: 111.112.113.114	5060	UDP	NAT (ersetzt Source IP mit öffentlicher IP des Access) 123.123.123.123

Tabelle 1: Firewall

⁽¹⁾ Abhängig von dem am Kundenstandort eingesetzten NAT Device, muss dort gegebenenfalls auch Portforwarding konfiguriert werden. In diesem Beispiel nicht dargestellt.

4.3 Session Initiation Protocol (SIP)

Rufnummern werden mit wenigen Ausnahmen als **SIP-URI** im Global Format gemäß RFC 3966, Abschnitt 5.1.4., mit folgender Syntax übermittelt:

sip: +<CC><NDC><SN>@<hostportion>;user=phone

user part	@	host part
-----------	---	-----------

Zum Beispiel: sip: +49<Rufnummer>@ims_sip_domain.de; user=phone

Die Platzhalter haben folgende Bedeutung:

- **CC:** Country Code
- **NDC:** National Destination Code
- **SN:** Subscriber Number

Vodafone kann nicht garantieren, dass user=phone in jedem Fall vorhanden ist.

Für lokale Rufnummernformate, beginnend mit dem NDC, wird kein phone-context gemäß RFC 3966 Abschnitt 5.1.5 genutzt.

4.3.1 SIP Header eingehende Anrufe

Für Nachrichten, die vom Vodafone Netz zur TK Anlage gesendet werden, sind SIP Header wie folgt aufgesetzt:

4.3.1.1 'Request-URI' Format

Der user part der 'R-URI' wird mit der öffentlichen Rufnummer der angerufenen TK-Nebenstelle gefüllt. Er enthält immer eine Nummer in internationalem Format:

z.B.: <sip: +49691234567@ims_sip_domain.de;user=phone>

Der host part der 'R-URI' enthält die Domäne der TK-Anlage. Diese entspricht der in den SIP Zugangsdaten mitgeteilten „Domain der SIP URI“.

4.3.1.2 'From' Header Format

Wenn keine Rufnummernunterdrückung (CLIR) oder „CLIP no screening“ Feature auf der Anruferseite aktiv sind, enthält der 'From' Header die Rufnummer des Anrufers im nationalen Format mit führender ,0' und NDC oder in internationalem Format mit führendem ,+' und County Code.

z.B.: <sip: +49691234567@ims_sip_domain.de;user=phone>

oder <sip: 0691234567@ims_sip_domain.de;user=phone>

Wenn der Anrufer die Rufnummernunterdrückung aktiviert hat (CLIR permanent oder CLIR temporary), ist der ankommende From header anonymisiert. Das Format entspricht RFC3323 und RFC3325:

From: „anonymous“<sip:anonymous@anonymous.invalid>

Um Interworkingprobleme zu vermeiden, sollte die TK-Anlage beide Formate unterstützen: mit ,user=phone' parameter und ohne.

Nutzt der Anrufer das Feature "CLIP no screening", kann der 'From' header eine von der TK-Anlage aufgesetzte, beliebige Nummer und Format enthalten. Daher kann Vodafone keine Verantwortung für die Rückrufbarkeit dieser Nummer übernehmen.

4.3.1.3 'To' Header Format

Der 'To' header enthält die vom Anrufer gewählte Nummer in nationalem Format mit führender ,0' und NDC oder in internationalem Format mit führendem ,+' und County Code.

z.B.: <sip: +49691234567@ims_sip_domain.de;user=phone>

oder <sip: 0691234567@ims_sip_domain.de;user=phone>

4.3.1.4 'P-Asserted-Identity' Header Format

Generell wird die 'P-Asserted-Id' (PAI) nicht vom Netz zur TK-Anlage gesendet. Vodafone entfernt die 'P-Asserted-Identity' in ankommenden Anrufen an der Netzgrenze zur TK-Anlage, dem SBC.

Da aber für einige Leistungsmerkmale die 'P-Asserted-Identity' auf Seite der TK-Anlage benötigt wird, gibt es folgende Regel:

- Für SIP Methods (z.B. INVITE) wird keine 'P-Asserted-Identity' vom Vodafone Netz zur TK-Anlage übertragen
- Für SIP Responses wird die Übermittlung der 'P-Asserted-Identity' vom Netz zur TK-Anlage erlaubt, um das Leistungsmerkmal COLP zu unterstützen.

4.3.1.5 Diversion Header

Für Rufumleitungsinformationen in ankommender Richtung, muss die TK Anlage den Diversion Indication Header (RFC 5806) unterstützen.

4.3.2 SIP Header abgehende Anrufe

Für von der TK-Anlage abgehende Anrufe müssen die SIP Header wie folgt aufgesetzt werden:

4.3.2.1 'Request-URI' Format

Der user part der R-URI muss mit Nummerninformation in einem der in der Tabelle aufgeführten Formate gefüllt sein:

Szenario	Rufnummerninformation des Angerufenen	Beispiel
Lokaler Anruf (innerhalb des gleichen Vorwahlbereichs)	0 <NDC><SN> 00<CC><NDC><SN> +<CC><NDC><SN>	0211 533 1111 0049 211 533 1111 +49 211 533 1111
Nationaler Anruf	0 <NDC><SN> 00<CC><NDC><SN> +<CC><NDC><SN>	0211 533 1111 0049 211 533 1111 +49 211 533 1111
Internationaler Anruf	00<CC><NDC><SN> +<CC><NDC><SN>	001 222 3333333 +1 222 3333333
Kurzstellige Rufnummern	<Rufnummer>	110,112, 115, 116xy, 118xy

Der host part der 'R-URI' muss der Domäne entsprechen, die in den SIP Zugangsdaten als „Domain der SIP URI“ mitgeteilt wurde.

Zusätzlich muss der SIP-URI parameter "user=phone" aufgesetzt werden.

Beispiel einer ausgehenden R-URI:

Request-Line: INVITE sip: +49691234567@ims_sip_domain.de;user=phone

4.3.2.2 'From' Header Format

In der Regel wird der 'From' header verwendet, um Absenderinformationen zu übertragen.

Der From Header muss die Absenderrufnummer in nationalem Format mit führender,0' oder in internationalem Format , beginnend mit + oder 00 enthalten:

z.B.: <sip: **+49691234567@ims_sip_domain.de**;user=phone>

oder <sip: **0691234567@ims_sip_domain.de**;user=phone>

Für die Abrechnung wird die Nummer im From Headers verwendet. Für eine korrekte Darstellung in der Detailabrechnung muss die Rufnummerninformation also wie oben genannt aufgesetzt werden.

Falls ein anderes Nummernformat genutzt werden sollte, kann dies zu einer fehlerhaften Darstellung auf der Abrechnung führen. Dasselbe gilt für von der TK Anlage aufgesetzten Rufumleitungsinformationen.

Aus diesem Grund, sollte die TK-Anlage auch bei aktivierter Rufnummernunterdrückung den „From“ Header mit der richtigen Absenderinformation aufsetzen. Die Anonymisierung wird im Vodafone Netz durchgeführt.

Wenn das Leistungsmerkmal „CLIP no screening“ genutzt wird, kann zwar der „From“ Header beliebige, syntaktisch korrekte Informationen enthalten, die netzseitig nicht geprüft werden. Jedoch, um eine korrekte Darstellung auf der Detailabrechnung , sowie die Rückrufbarkeit zu ermöglichen, muss das hier beschriebene Format aufgesetzt werden.

4.3.2.3 'To' Header Format

Der 'To' Header enthält die gewählte Rufnummer und sollte in nationalem Format mit führender ,0' oder in internationalem Format aufgesetzt sein:

z.B.: <sip: **+49691234567@ims_sip_domain.de**;user=phone>

oder <sip: **0691234567@ims_sip_domain.de**;user=phone>

4.3.2.4 'P-Asserted-Identity' Header Format

Eine 'P-Asserted-Identity' soll nicht von der TK Anlage für abgehende Anrufe aufgesetzt werden. Wird sie dennoch aufgesetzt, so wird sie vom Netz als nicht vertrauenswürdig eingeschätzt und ignoriert.

Im Fall von Notrufen muss von Vodafone immer eine PAI mit einer anschluss- und standortbezogenen Rufnummer übermittelt werden. Die von Vodafone aufgesetzte PAI entspricht der Pilotnummer, das ist diejenige Rufnummer, die auch von der PBX in der PPI aufgesetzt werden muss.

4.3.2.5 'P-Preferred-Identity' Header Format

Für Business Voice ist jeder TK Anlage eine Pilotnummer zugeordnet. Diese wird unter anderem im Vodafone Netz verwendet, um Dialoge als von der TK Anlage kommend zu validieren.

Die P-Preferred-ID muss im internationalen Format und mit user=phone Parameter aufgesetzt werden.

z.B.: <sip: **+49691234567@ims_sip_domain.de**;user=phone>

Der host part der 'R-URI' sollte die Domäne der TK-Anlage enthalten. Diese entspricht der in den SIP Zugangsdaten mitgeteilten „Domain der SIP URI“.

Zur Übertragung der Pilotnummer wird der SIP Header 'P-Preferred-Identity' (PPI) genutzt. Für abgehende Anrufe muss daher die TK Anlage in jeder „INVITE“ eine 'P-Preferred-Identity' mit der definierten Pilotnummer (siehe „konfiguriere PPI ID“ in den SIP-Zugangsdaten) aufsetzen. Wird eine andere Nummer in der PPI aufgesetzt, wird der Anrufversuch abgewiesen (SIP error 403).

Die PPI muss ebenso in abgehenden SIP Antworten der TK Anlage enthalten sein. Dies ist zur Abbildung des Leistungsmerkmals COLP notwendig. Die 'P-Preferred-Identity' muss in diesem Fall die Nummer der verbundenen Nebenstelle enthalten (siehe auch Leistungsmerkmal COLP/COLR)

Diese Nummer aus der 'P-Preferred-Identity' wird nach Validierung im Vodafone Netz in die „P-Asserted-Identity“ übernommen und in Richtung des Anrufers (A Teilnehmers) übermittelt.

Die 'P-Preferred-Identity' soll immer im internationalen Format aufgesetzt werden.

4.3.2.6 'Diversion' Header Format

TK Anlagen können unterschiedliches Verhalten in Bezug auf das Aufsetzen von Rufumleitungsinformationen aufweisen. Einige Anlagen setzen eine Rufumleitung als abgehenden Anruf ohne weitere Zusatzinformationen auf. Setzt die TK Anlage allerdings Rufumleitungsinformation (wie die Nummer der umleitenden Nebenstelle) auf, muss die TK Anlage den SIP „Diversion Indication“ Header (RFC 5806) in der abgehenden INVITE verwenden.

Der „Diversion Indication“ Header wird im Netz transparent weitergeleitet und die enthaltene Nebenstellenummer erscheint in der Detailabrechnung, zusammen mit der Nummer aus der „P-Asserted-ID“. Wenn ein „Diversion Indication“ Header vorhanden ist, wird die darin enthaltene Nummer anstelle der aus dem „From“ Header verwendet und ersetzt diese.

4.3.3 Reliability of Provisional Responses – PRACK (RFC 3262)

Reliability of Provisional Responses werden netzseitig unterstützt.

4.3.4 Offer/Answer Model (RFC 3264)

Das Offer/Answer Model wird unterstützt. Ein Early Offer im INVITE ist erforderlich.

4.3.5 Privacy (RFC 3323 und 3325)

Ein anonymisierter From-Header wird unterstützt, soll aber wie in Kapitel 4.3.2.2 beschrieben nicht aufgesetzt werden. Sollte die TK-Anlage dennoch „anonymous“ im User-Part des From-Headers schicken, wird zusätzlich ein Privacy-Header mit *Privacy:id* eingefügt, um die Anonymität auch für die PAI zu gewährleisten.

4.3.6 Display Name (RFC 3261)

Wenn die TK-Anlage einen Display Name im From-Header übermittelt, wird dieser von Vodafone innerhalb des VoIP Netzes transparent weitergeleitet. Beim Übergang in ISDN-Netze wird die Information verworfen. Ob der Display Name bis zum Angerufenen übermittelt wird, hängt daher davon ab, über welche Netze der Anruf übertragen wird.

Bei eingehenden Anrufen hängen Präsenz und Inhalt des Display Name ebenso vom Anrufursprung ab. Wenn der Anruf aus einem ISDN-Netz stammt, wird die Rufnummer des Anrufers als Display Name im From-Header übermittelt. Beim Anruf von einem anderen SIP-Endpunkt ist das Verhalten oder der Anschluss des Endgeräts für den Display Name verantwortlich. Vodafone übergibt ihn transparent.

4.3.7 History Info (RFC 4244)

History Info wird für eingehende Gespräche nicht übermittelt. Es wird nur der Diversion Indication Header verwendet.

4.3.8 OPTIONS Ping (RFC 3261)

Vodafone sendet alle 30 Sekunden einen OPTIONS Ping zu der IP-Adresse der TK-Anlage, um die Erreichbarkeit zu überprüfen.

4.3.9 P-Early Media-Header (RFC 5009)

Der P-Early Media-Header wird in erster Linie für die beiden folgenden Anwendungsfälle unterstützt:

1. Eingehende Anrufe aus ISDN- oder Mobilfunk-Netzen zur Telefonanlage, bei denen die TK-Anlage Early-Media, z. B. einen individuellen Klingelton oder eine Ansage, vor einem 200OK übermitteln möchte. Vodafone übermitteln im INVITE P-Early-Media: supported. Die TK-Anlage muss im 180 Ringing oder 183 Session Progress einen P-Early-Media-Header übermitteln, damit Vodafone die Information ins ISDN- oder Mobilfunknetz weitergeben kann.
2. Eingehende Anrufe aus ISDN- oder Mobilfunk-Netzen, die von der TK-Anlage zu einem ISDN- oder Mobilfunkteilnehmer weitergeleitet werden. Die TK-Anlage muss im INVITE für die Weiterleitung P-Early-Media: supported signalisieren. Wenn die TK-Anlage als Antwort ein 180 Ringing oder 183 Session Progress mit einem P-Early-Media-Header empfängt, muss sie diese Nachricht mit dem Header in Richtung Anrufer weiterleiten.

4.3.10 UPDATE Method (RFC 3311)

Die SIP UPDATE Methode (RFC3311) muss von der TK Anlage unterstützt werden, um Interworkingprobleme mit Diensten zu verhindern, die diese Methode nutzen müssen.

4.4 Session Description Protocol (SDP)

Dieser Abschnitt bietet einen Überblick über die wichtigsten SDP-Funktionen und deren Unterstützung.

4.4.1 Payload Types

Gemäß RFC 3264 sollte die TK-Anlage mit dem vom Netz vorgeschlagenen Payload Type antworten und auch im Fall von re-INVITES den Payload Type aus vorhergehenden SDP Offers übernehmen.

4.4.2 Media Description (m=)

Die Media Description für Audio enthält die unterstützten Audio-Codexs und den Media-Port. Der Payload Type für Named Telephone Event (DTMF) sollte grundsätzlich am Ende stehen, damit der Payload Type auf keinen Fall an die erste Stelle rückt, falls nicht unterstützte Codexs aus der Liste entfernt werden. Manche Endgeräte lehnen INVITES ab, bei denen Named Telephone Event an erster Stelle steht.

4.4.3 Bandwidth (b=)

Gemäß RFC 4566 sind mehrere Zeilen erlaubt. Einige Endgeräte lehnen aber eine Verbindung mit mehreren Zeilen ab, da in dem Vorgänger-RFC 2327 nur eine Zeile vorgesehen war. Es wird daher empfohlen, dass die TK-Anlage maximal eine Bandwidth-Zeile schickt.

In RFC 3890 wurde mit TIAS ein weiterer Bandwidth Modifier definiert. Obwohl Endgeräte gemäß RFC 2327 und RFC 4566 unbekannte Modifier ignorieren sollen, lehnen einzelne Endgeräte eine Verbindungen mit b=TIAS im SDP ab. Deshalb wird empfohlen, auf diesen Parameter zu verzichten.

4.5 Verschlüsselung (TLS/sRTP)

Verschlüsselung der Signalisierung mittels TLS und des Sprachkanals mittels sRTP wird nicht für Business VoIP unterstützt. Voraussetzung für TLS ist die Nutzung von TCP als Transportprotokoll.

4.6 Abbildung von ISDN-Leistungsmerkmalen

4.6.1 CLIP (OIP)

Calling Line Identification Presentation (CLIP) ermöglicht dem Angerufenen, die Identität - in Form der Rufnummer – des Anrufers zu erhalten. Die angezeigte Rufnummer wird im From Header übertragen, sofern der Anrufer keine Anonymität wünscht.

Für den Business VoIP Anschluss ist standardmässig eine Überprüfung der übermittelten Rufnummer (CLI screening) eingerichtet, wenn der TK-Anlage ein Rufnummernblock zugeordnet ist. Sind einem Business VoIP Anschluss, also einer TK-Anlage mehrere Rufnummernblöcke zugeordnet, wird ein CLI screening nicht durchgeführt und es ist standardmässig das Leistungsmerkmal „CLIP no Screening“ (Siehe Kapitel 4.6.2) aktiviert.

Im Netz wird die Rufnummer in From mit den für den Anschluss konfigurierten Nebenstellennummern verglichen. Wenn keine Übereinstimmung besteht, wird die Rufnummer in From durch die Pilotnummer der TK Anlage ersetzt.

Generell kann aber die Rufnummer im From-Header vom Anrufer selbst aufgesetzt und ggfs. im Ursprungsnetz nicht überprüft worden sein (wenn der Anrufer das Leistungsmerkmal „CLIPno screening“ nutzt)

Die Rufnummer steht im User-Part der SIP-URI.

Beispiel einer eingehenden INVITE:

Beispiel:

```
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
```

Details zum "From" Header für eingehende Anrufe sind in Kapitel 4.3.1.2 beschrieben.

4.6.2 CLIP–no-screening

CLIP - no screening ermöglicht die Übermittlung einer kundenindividuellen Rufnummerninformation an den angerufenen Anschluss. Die im From Header aufgesetzte Rufnummer wird dann netzseitig nicht mehr mit den für den Anschluss konfigurierten Nebenstellennummern verglichen. Dieses Leistungsmerkmal ist für Business VoIP nicht automatisch aktiv (es sei denn mehrere Rufnummernblöcke sind der TK-Anlage zugewiesen, siehe Kapitel 4.6.1) und muss bei Vodafone beauftragt werden.

Wenn die Rufnummer von der TK-Anlage aufgesetzt wird, ist der Kunde dafür verantwortlich, dass er gemäß § 66k (2) TKG über die Nutzungsrechte an dieser Rufnummer verfügt.

Wenn sichergestellt werden soll, dass die Rufnummer aus der PAI nicht beim B-Teilnehmer angezeigt wird, sollte ein Privacy-Header mit „Privacy: id“ geschickt werden. Siehe auch Kapitel 4.6.3

Im Fall einer Anrufweitschaltung kann der From-Header die Rufnummer des Anrufers enthalten.

4.6.3 CLIR (OIR)

Calling Line Identification Restriction (CLIR) ermöglicht dem Anrufer, die Übermittlung seiner eigenen Identität an den Empfänger zu unterdrücken.

Im Normalfall ist netzseitig keine Rufnummernunterdrückung aktiviert, sodass die Rufnummernunterdrückung seitens der TK-Anlage flexibel angefordert werden kann. Es kann aber auch eine permanente Rufnummernunterdrückung und Deaktivierung pro Anruf konfiguriert werden.

- Aktivierung der Rufnummernunterdrückung auf der TK-Anlage:

Die TK-Anlage muss die Unterdrückung der Rufnummer mittels Privacy nach RFC3323 und RFC 3325 unterstützen. *Privacy: id* bezieht sich gemäß RFC 3325 nicht auf den From header. Da der From header nicht von der TK-Anlage anonymisiert aufgesetzt werden soll, wie auch in Kapitel 4.3.2.2 beschreiben, muss von der TK-Anlage zusätzlich *privacy: user* aufgesetzt werden. Der From header wird dann netzseitig anonymisiert, bevor er zum B-Teilnehmer übertragen wird.

Beispiel einer von der TK Anlage abgehenden INVITE, mit CLIR:

```
INVITE sip:+4971193309821@ims_sip_domain.de;user=phone SIP/2.0
From: <sip:+4951112455480@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@user_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
```

Beispiel einer ankommenden INVITE, für die der Anrufer CLIR gesetzt hat:

```
INVITE sip:+4971193309821@ims_sip_domain.de;user=phone 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
```

- Permanente Aktivierung der Rufnummernunterdrückung im Vodafone Netz

Hat der Kunde die optionale, permanente Rufnummernunterdrückung bei Vodafone beauftragt, werden im Netz, unabhängig davon, was die TK-Anlage schickt, alle SIP header anonymisiert.

CLIR wird bei Wahl einer Notrufnummer aufgehoben.

4.6.4 COLP (TIP)

Connected Line Presentation (COLP) ermöglicht dem Anrufer die Rufnummer des verbundenen Anschlusses zu sehen. Dazu kann die TK-Anlage bei einem eingehenden Anruf, sofern mit dem option tag "from-change" angefragt, dem Anrufer im 200OK die Rufnummer der Nebenstelle übermitteln, die den Anruf angenommen hat.

Die Rufnummer muss als PPI signalisiert werden. Die Rufnummer in der PPI muss ein globales oder nationales (optional) Format aufweisen.

Beispiel:

```
P-Preferred-Identity:
<sip:+496921691234@ims_sip_domain.de;user=phone>
```

Die PPI wird vom Vodafone SBC durch die PAI ersetzt und an den Anrufer übertragen.

Im Vodafone Netz wird keine Validierung der von der TK Anlage aufgesetzten Rufnummerninformation in der PPI durchgeführt. Es ist somit immer „COLP – no screening“ aktiv.

Beispiel einer '200 OK' mit COLP Informationen, vom Angerufenen in Richtung Netz


```
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
```

Beispiel einer '200 OK' mit COLP Informationen, vom Netz in Richtung Anrufer

```
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
```

In diesem Beispiel sind:

Anrufer:	0511124554820
Gewählte Nummer:	071193309821
Verbundene Nummer:	071193309827

4.6.5 COLR (TIR)

Connected Line Presentation Restriction (COLR) ist eine Funktion der TK Anlage, wenn der Angerufene nicht wünscht, daß die verbundene Nebenstellenummer übertragen wird.

Dazu soll die TK Anlage in der '200 OK' die Rufnummer in der PPI signalisieren und gleichzeitig ‚Privacy: id‘ aufsetzen, wie in 3GPP TS 24.509, Rel8 beschrieben.

Ein netzseitiges COLR wird nicht angeboten.

Beispiel einer '200 OK' Nachricht mit COLR, vom Angerufenen in Richtung Netz:

```
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
```

Die PAI wird nicht an den Anrufer übertragen.

Beispiel einer '200 OK' Nachricht mit COLR, vom Netz in Richtung Anrufer:

```
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
```

In diesem Beispiel sind:

Anrufer: 0511124554820
 Gewählte Nummer: 071193309821
 Verbundene Nummer: 071193309827

4.6.6 Rufumleitung

Wenn die TK Anlage Rufumleitungsinformationen aufsetzt, muss sie wie in Kapitel 4.3.2.6 beschrieben, den ‚Diversion‘ Header verwenden.

Beispiel einer abgehenden INVITE von einer TK Anlage, die Weiterleitungsinformationen aufsetzt:

```
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
```

In diesem Beispiel sind:

Anrufer: 0511124554820
 Gewählte Nummer: 071193309821
 Weitergeleitete Nummer: 02115349900
 Pilot Nummer: 07119330980

Ist die TK Anlage nicht in der Lage oder konfiguriert, Rufumleitungsinformationen aufzusetzen, wird die Weiterleitung als normaler, abgehender Anruf signalisiert. R-URI und To enthalten die weitergeleitete Nummer. Das From Feld enthält entweder die weiterleitende Nummer (B) oder den ursprünglichen Anrufer (A)

```
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
```

oder

```
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
```

Es ist möglich, eine anschlussweite oder eine nebenstellenabhängige, sofortige Rufumleitung im Netz zu setzen. Diese gilt entweder **immer** (static call deflection) oder nur **bei Ausfall** (dynamic call deflection). Die netzbasierten Rufumleitungen nutzen den Diversion Header um Rufumleitungsinformationen zu übermitteln.

Die Rufumleitung bei Ausfall greift im Netz, wenn die TK Anlage nicht erreichbar ist. Dies erkennt das Vodafone Netz anhand der SIP error codes: 404, 603 und 500.

4.6.7 Halten (Call Hold)

Das Leistungsmerkmal „Halten“ muss gemäß RFC 3264 Abschnitt 8.4 (Verwendung der SDP „a“ Parameter) implementiert sein. Beim Übergang in leitungsvermittelnde Netze unterstützt Vodafone a=sendonly und a=inactive.

Die Übermittlung der IP-Adresse 0.0.0.0 gemäß RFC 2543 für „Halten“ wird im RFC 3264 und von BITKOM nicht mehr empfohlen.

4.7 Nutzkanal-Eigenschaften

Die Eigenschaften des Nutzkannals beziehen sich in erster Line auf den Übergang zum PSTN, der durch Media-Gateways von Vodafone realisiert ist. Bei Verbindungen zu anderen VoIP-Endgeräten im Vodafone-Netz oder im Netz anderer VoIP-Anbieter, mit denen Vodafone einer VoIP-Zusammenschaltung betreibt, können Abweichungen möglich sein.

4.7.1 Codecs

Da die verwendeten Codecs ausgehandelt werden und somit von der Gegenseite abhängen, kann keine vollständige Liste an garantiert von allen VoIP Endgeräten unterstützen Codecs aufgeführt werden. Es wird empfohlen, daß die TK Anlage die gängigen Codecs G.729A und G.726 unterstützt. Mindestens unterstützen muss sie jedoch den Codec:

- G.711 (a-law)

und

- telephone-event

Die empfohlene Framesize für G.711 A/μ-law beträgt 20 ms.

4.7.2 DTMF (Named Telephone Events)

Die DTMF-Übertragung sollte gemäß RFC 2833/4733 als RTP Named Telephone Event (NTE) erfolgen.

4.7.3 Fax

Für die Gruppe-3-Fax-Übertragungen muss mindestens der Passthrough-Modus (T.30 über G.711 A-law) unterstützt werden.

Gruppe-4-Fax wird gemäß Leistungsbeschreibung nicht unterstützt. Die Nutzung von ITU-T.38 zur FAX-Übertragung führt häufig zu Interoperabilitätsproblemen.

5 Timer configuration

Die TK Anlage sollte SIP timer nach RFC 3261 und RFC 4028 unterstützen.

6 Notruf

Die Notrufnummern 110 und 112 werden auf Basis der rufenden Nummer sowie statischer Informationen in der Vodafone-Teilnehmerdatenbank zu der zuständigen Notrufleitstelle weitergeleitet. Es liegt in der Verantwortung des Kunden, Vodafone über Änderungen der Teilnehmerdaten zu informieren.

Es muss von der TK-Anlage sichergestellt werden, dass ein **PPI-Header** mit einer Rufnummer aufgesetzt wird, die dem realen Standort des Teilnehmers entspricht. Wie für alle Rufnummern, von denen ein Notruf abgesetzt werden kann, gilt auch hier die gesetzliche Verpflichtung, dass die standortbezogene Rufnummer rückrufbar sein muss, die Nebenstelle also einem anderen Teilnehmer oder besser einer Sammelrufnummer zugeordnet ist. Im **From-Header** muss immer die Rufnummer der Nebenstelle stehen, von der der Notruf ausgeht.

7 Definitionen und Abkürzungen

Für das vorliegende Dokument gelten die folgenden Definitionen und Abkürzungen:

Begriff/Abkürzung	Erklärung
Abgehender Anruf	Anruf von der TK-Anlage des Kunden über das Vodafone-Netz
Diversion Indication	SIP-Erweiterung, die dem Angerufenen im Diversion Header anzeigt, von wem und warum der Anruf umgeleitet wurde, siehe RFC 5806
DNS	Domain Name System
Eingehender Anruf	Anruf über das Vodafone-Netz zur TK-Anlage des Kunden
FQDN	Fully Qualified Domain Name
HA	High Availability
History Info	SIP-Header mit History-Informationen aus Verbindungsanfragen; ermöglicht diverse erweiterte Dienste durch Übertragung der Information, wie und warum ein Anruf an einen bestimmten Anwender oder eine bestimmte Anwendung geleitet wird. Siehe RFC 4244.
INVITE	SIP-Methode, die zum Aufbau eines Session-Dialogs verwendet wird, üblicherweise zum Aufbau eines Telefongesprächs
MTU Size	Maximum Transmission Unit Size
NAT	Network Address Translation
NDC	National Destination Code, entspricht der Ortsnetzkennzahl ONKZ
OIP	Originating Identification Restriction
OIR	Originating Identification Restriction
PAI	P-Asserted Identity; private SIP-Erweiterung, die einem Netzwerk vertrauenswürdiger Server ermöglicht, die Identität authentisierter Nutzer zu erklären, siehe RFC 3325
P-Early Media	SIP-Header-Feld zur Steuerung des Media Flows in einem frühen Stadium des Dialogs zwischen unterschiedlichen SIP-Netzen, siehe RFC 5009
PPI	P-Preferred Identity; SIP-Header, der die Public User Identity enthält, die ein Benutzer für den Verbindungsaufbau verwenden möchte, siehe RFC 3325
Reliability of Provisional Responses	SIP-Erweiterung, die eine vorläufige Antwortmeldung bereitstellt, siehe RFC 3262
RTP	Real-Time Transport Protocol; Protokoll zur kontinuierlichen Übertragung von Streams über IP-Netzwerke
SBC	Session Border Controller; Netzwerkkomponente zur sicheren Kopplung unterschiedlicher oder unterschiedlich sicherer Netze, ermöglicht die Steuerung der Signalisierung sowie des Verbindungsauf- und -abbaus von Telefonaten
SDP	Session Description Protocol; liefert Regeln zur Beschreibung des Aufbaus von Multimedia-Sessions, siehe RFC 4566
SIP	Session Initiation Protocol; von der IETF MMUSIC Working Group entwickeltes Protokoll, das zum Aufbau, Verwalten und Beenden von Kommunikationssitzungen verwendet werden kann
SIPconnect	Initiative und Forum für den direkten Austausch von IP-Verkehr zwischen SIP-fähigen Endkunden-TK-Anlagen und VoIP-Netzen der Netzanbieter
SIP-URI	SIP-Telefonnummer (Uniform Resource Identifier); liegt in einem E-Mail-ähnlichen Format vor. Syntax: sip:subscriber@host:port. Siehe RFC 3261.
SRV Resource Records	Service Resource REcords

Begriff/Abkürzung	Erklärung
STUN	Session Traversal Utilities for NAT; Protokoll zur Erkennung von Firewalls und NAT-Routern sowie Ermittlung und Übertragung der öffentlichen IP-Adresse eines SIP-Telefons, siehe RFC 5389
TCP	Transmission Control Protocol
tel-URI	tel Uniform Resource Identifier; Angabe des Empfängers mit einer herkömmlichen Telefonnummer zur Integration des älteren leitungsvermittelnden Telefonnetzes. Siehe RFC 3966.
TIP	Terminating Identification Presentation
TIR	Terminating Identification Restriction
TK-Anlage	Telekommunikationsanlage
UDP	User Datagram Protocol
VoIP	Voice over IP