Documentation

OpenScape Voice V6
Interface Manual: Volume 6, SIP Interface to Service Providers

Description

A31003-H8060-T100-06-7618

Siemens Enterprise Communications
www.siemens-enterprise.com

SIEMENS

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standard certified by an external certification company.

Siemens Enterprise Communications GmbH & Co. KG is a Trademark Licensee of Siemens AG

Reference No.: A31003-H8060-T100-06-7618

Siemens Enterprise Communications
www.siemens-enterprise.com

Contents

Fully Qualified Domain Name 150

History of Changes

Issue	Date	Changes
1	April, 2011	V6 Issue 1 Following enhancements: • SDP size up to 10 Kbytes • Best Effort SRTP with MIKEY enhancements and, ensuring SDP compatibility for best effort SRTP between devices that do support the best effort SRTP mechanism and devices that do not • Flexible Ethernet Port and IP Address Configuration • OpenScape Branch: SIP Service Provider Support, Addressing SIP Service Provider via FQDN or IP Address
2	June, 2011	V6 Issue 2 • Further details added to Issue 1 enhancements.
3	August, 2011	V6 Issue 3 • Port conventions added for the different SIP Signaling Transport Protocols (see Section 4.3.10, “Transport Protocol”)
4	February, 2012	V6 Issue 4: • Limited RF3262 (SIP PRACK) supported in OpenScape Voice to address interoperability with a Media Server when early-media or IVR is used in the network. Refer to Section 6.3.8, “PRACK”, Section 6.4.27, “RAck” and SIP Endpoint Attribute PRACK Enabled in Chapter 7, “Configuration options for SIP Service Provider interoperability”. • OpenScape Voice supports sending a SIP INVITE or SIP UPDATE request with a P-Asserted-Identity header containing the “calling” name and number, when it receives the caller identity within a Remote-Party-ID header received in a SIP INVITE or delayed SIP INFO message, respectively. Refer to: Section 6.4.31, “Remote-Party-ID”, Section 6.3.5, “INVITE”, Section 6.3.4, “INFO”, Section 6.3.12, “UPDATE”, Section 5.1.1, “Calling Line Identification Presentation (CLIP)”.
5	March, 2012	V6 Issue 5: Support for sending different display and authentication numbers in From and PAI headers. Refer to: • Section 5.1.1.1, “CLIP procedures by OpenScape Voice:” • Section 6.4.17, “From” • Section 6.4.21, “P-Asserted-Identity” • Chapter 7, “Configuration options for SIP Service Provider interoperability”
6	October, 2012	V6 Issue 6: Updated the OPTIONS method with a better description: • Section 6.3.7, “OPTIONS”

1 General Information

1.1 Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no guarantee of 100% accuracy is implied. Siemens shall have neither liability nor responsibility to any person or entity with respect to the correctness of the information contained herein, other than to correct mistakes that are subsequently discovered in the text. Incorrect text shall not be construed as a promise or commitment on the part of Siemens to modify its products to achieve described operation, although Siemens is willing to work with its customers to provide requested functionality.

1.2 References

1.2.1 Normative References

RFC2045 [1]	“Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies”; N. Freed / N. Borenstein
RFC2046 [2]	“Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types”; N. Freed / N. Borenstein
RFC2119 [3]	“Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, Bradner, S.
RFC2246 [4]	“The TLS Protocol Version 1.0”, T. Dierks, C. Allen
RFC2560 [5]	“X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”; M.Myers / R.Ankney / A. Malpani / S. Galperin / C.Adams
RFC2833 [6]	“RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”; H. Schulzrinne / S. Petrack
RFC3261 [8]	"SIP: Session Initiation Protocol"; J. Rosenberg / H. Schulzrinne / G. Camarillo / A. Johnston / J. Peterson / R. Sparks / M. Handley / E. Schooler
RFC3262 [9]	"Reliability of Provisional Responses in the Session Initiation Protocol (SIP)"; J. Rosenberg / H. Schulzrinne
RFC3263 [10]	“SIP: Locating SIP Servers”; J. Rosenberg / H. Schulzrinne
RFC3264 [11]	"An Offer/Answer Model with SDP"; J. Rosenberg / H. Schulzrinne
RFC3265 [12]	“Session Initiation Protocol (SIP)-Specific Event Notification”; A. B. Roach

RFC3268 [13]	“Advanced Encryption Standard (AES) Ciphersuites for TLS”; P. Chown
RFC3280 [14]	“Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”; R. Housley / W. Polk / W. Ford / D. Solo
RFC3311 [15]	"The Session Initiation Protocol (SIP) UPDATE Method"; J. Rosenberg
RFC3323 [16]	“A Privacy Mechanism for the Session Initiation Protocol (SIP)”; J. Peterson
RFC3325 [17]	“Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks”; C. Jennings / J. Peterson / M. Watson
RFC3515 [19]	“The Session Initiation Protocol (SIP) Refer Method”; R. Sparks
RFC3550 [20]	“RTP: A Transport Protocol for Real-Time Applications”; H. Schulzrinne / S. Casner / R. Frederick / V. Jacobson
RFC3581 [21]	“An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing”; J. Rosenberg / H. Schulzrinne
RFC3605 [22]	“Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)”; C. Huitema
RFC3711 [23]	“The Secure Real-time Transport Protocol (SRTP)”; M. Baugher / D. McGrew / M. Naslund / E. Carrara / K. Norrman
RFC3761 [24]	“The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)”; P. Faltstrom / M. Mealling
RFC3830 [25]	“MIKEY: Multimedia Internet KEYing”; J. Arkko / E. Carrara / F. Lindholm / M. Naslund / K. Norrman
RFC3842 [26]	“A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)”; R. Mahy
RFC3891 [27]	“The Session Initiation Protocol (SIP) "Replaces" Header”; R. Mahy / B. Biggs / R. Dean
RFC3892 [28]	“The Session Initiation Protocol (SIP) Referred-By Mechanism”; R. Sparks
RFC3966 [29]	“The tel URI for Telephone Numbers”; H. Schulzrinne
RFC4028 [30]	“Session Timers in the Session Initiation Protocol (SIP)”; S. Donovan / J. Rosenberg
RFC4566 [31]	“SDP: Session Description Protocol”; M. Handley / V. Jacobson / C.Perkins (obsoletes RFC2327)
SIP Forum [33]	“IP PBX / Service Provider Interoperability”, “SIPconnect 1.0 Technical Recommendation”, March 2006
ITU-T T.38 [34]	“ITU-T T.38, Series T: Terminals for Telematic Services, Procedures for real-time Group 3 facsimile communication over IP networks, Annex D: SIP/SDP call establishment procedures”, 04/2004
ITU-V.152 [38]	“ITU-T V.152, Series V: Data communication over the telephone network, Interworking with other networks, Procedures for supporting voice-band data over IP networks”, 01/2005.

RFC3362 [39]	G. Parsons, “Real-time Facsimile (T.38) - image/t38 MIME Sub-type Registration”, RFC 3362, August 2002
RFC3725 [40]	Rosenberg, Peterson, Schulzrinne, Camarillo, “Best Current Practices for Third Party Call Control in SIP”, HYPERLINK "http://www.ietf.org/rfc/rfc3725.txt" RFC 3725, April 2004
RFC3312 [41]	G. Camarillo, “Integration of Resource Management and Session Initiation Protocol (SIP)”, RFC 3312, October 2002
RFC3959 [42]	G. Camarillo, “The Early Session Disposition Type for the Session Initiation Protocol (SIP)”, RFC 3959, December 2004
draft-ietf-sip-privacy [43]	SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks, draft-ietf-sip-privacy-04, February 2002

1.2.2 Informative References

draft-ietf-sip-connect-reuse-05	“Connection Reuse in the Session Initiation Protocol (SIP)”; R. Mahy / V. Gurbani / B. Tate, February 2006 (Expires: August 2006)
Draft-camarillo-sipping-sbc-funcs-04.txt	“Requirements from SIP (Session Initiation Protocol) Session Border Control Deployments”; J. Hautakorpi / G. Camarillo /R. Penfield / A. Hawrylyshen / M. Bhatia
Diversion	“Diversion Indication in SIP, S. Levy / J.R. Yang; RFC 5806, Historic
AT&T	“AT&T BVOIP Network SIP Specification for IP PBXs”, Issue 1.1, October 24, 2005”; Jim Amster
TR114	“Schnittstellenbeschreibung VoIP, TR, 1 TR 114/Vorversion 3 (Update1 für Abschnitt 5” (1TR114 Februar06 Update1.pdf), Deutsche Telekom AG, T-Com, 28.09.2006
SIP_CONN	“The SIPconnect Interface Specification, An Industry Standards-Based Approach to Direct IP Interoperability between SIP-Enabled IP PBXs and SIP-Enabled VoIP Service Provider Networks“, Draft Version 1.0, February 2005
VERIZON	“OpenScape Voice Gateway Interface Requirements”, Verizon Business, Version 1.3, 07/27/2006
TISPAN_CCBS	ETSI Requirement Specification, TISPAN: NGN Signaling Control Protocol: CCBS & CCNR, ETSI TS <03035> v<0.0.8> (2005-07)
ACME_CONFIG	Net-Net Session Director, Configuration Guide, Release Version 2.2 Document Number: 400-0061-22A
ACME_RADIUS	Net-Net RADIUS Reference Guide, Release Version 2.2 Document Number: 400-0015-22A
SIP_TEL_NP	J. Yu, “NP Parameters for the "tel" URI”, <draft-ietf-iptel-tel-np-11.txt>, August 2006
SIP_CPC	R. Mahy, “The Calling Party's Category tel URI Parameter”, <draft-ietf-iptel-cpc-05.txt>, October 2006
CMSS	PacketCable “CMS to CMS Signaling Specification” PKT-SP-CMSS-I02-021205

1.3 Figures

Throughout the document, the symbols shown below are used

OpenScape Voice Softswitch:	
SIP Service Provider: *Note: this symbol represents the entire Service Provider infrastructure, including any border proxies or SBCs.*	
SIP-Aware Firewall/NAT Router (SBC):	
Ordinary Firewall/NAT Router: (This entity is not SIP-aware.)	
SIP Gateway:	
SIP Client:	
Native SIP Trunking Connection:	
SIP UA Connection:	

Figure 1 Definition of Symbols

1.4 Terminology

In this document, if the words “must”, “must not”, “should”, “should not”, and “may” are used, they are not intended to be “normative” (as described in RFC2119 [3]); rather, they are used to indicate a capability or desired behavior. In addition, when the word “may” is used, it generally implies that the capability is controlled via configuration or provisioning options.

Refer to the Glossary for other terms used in this document.

1.5 Keyword/Descriptor

- SIP Interfaces
- SIP Trunking
- Peering
- Carrier Interconnect
- Service Provider Interconnect

2 Purpose

2.1 Scope

The goal of this document is to describe the SIP interface used between an OpenScape Voice system and a Service Provider (SP). The Service Provider (SP) interface may be used only to provide PSTN access, or may also be used to provide SIP interconnection, via the SP, to subscribers in other branches of the same Enterprise or in other Enterprises.

A simplified view of the OpenScape Voice SIP trunking interface to the SP can be found in Figure 2. This document applies only to the interface annotated as SIP Trunking in Figure 2; other OpenScape Voice interfaces are outside the scope of this document. The SIP Forum Reference Architecture for IP PBX/Service Provider Interoperability (RFC4028 [30]) is reproduced below as Figure 3 for information only. It is not mandatory that this or any other particular architecture be used for IP PBX/Service Provider interconnection; local agreements between Enterprises and Service Providers may result in different architectures.

Chapter 4, “Architecture” presents typical system scenarios that can be found in many customer projects. Section 4.3, “Signaling and Network Requirements” presents a range of additional network requirements which must be considered when operating an OpenScape Voice system.

Chapter 5, “Features” describes telephony features using those signaling building blocks from Chapter 6, “Building Blocks and Protocol Compliance”. Details on the implementation of particular telephony features may be provided in separate feature-specific documents.

Chapter 6, “Building Blocks and Protocol Compliance” defines the interface by introducing signaling building blocks, which are based on the SIP protocol and SIP protocol enhancements (see RFC3261 [8] and others) as well as other existing specifications.

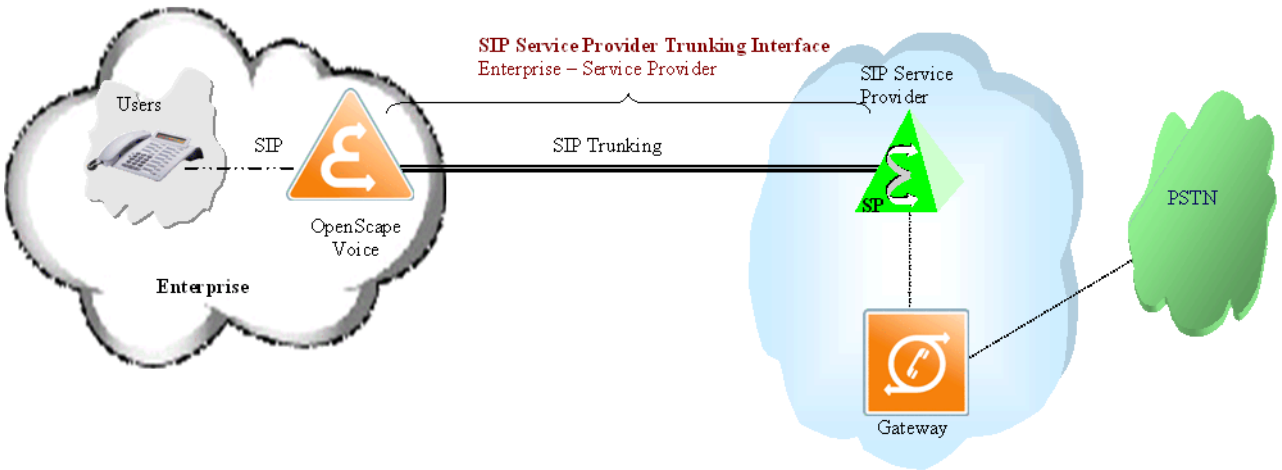


Figure 2 SIP Trunking Interface to Service Provider

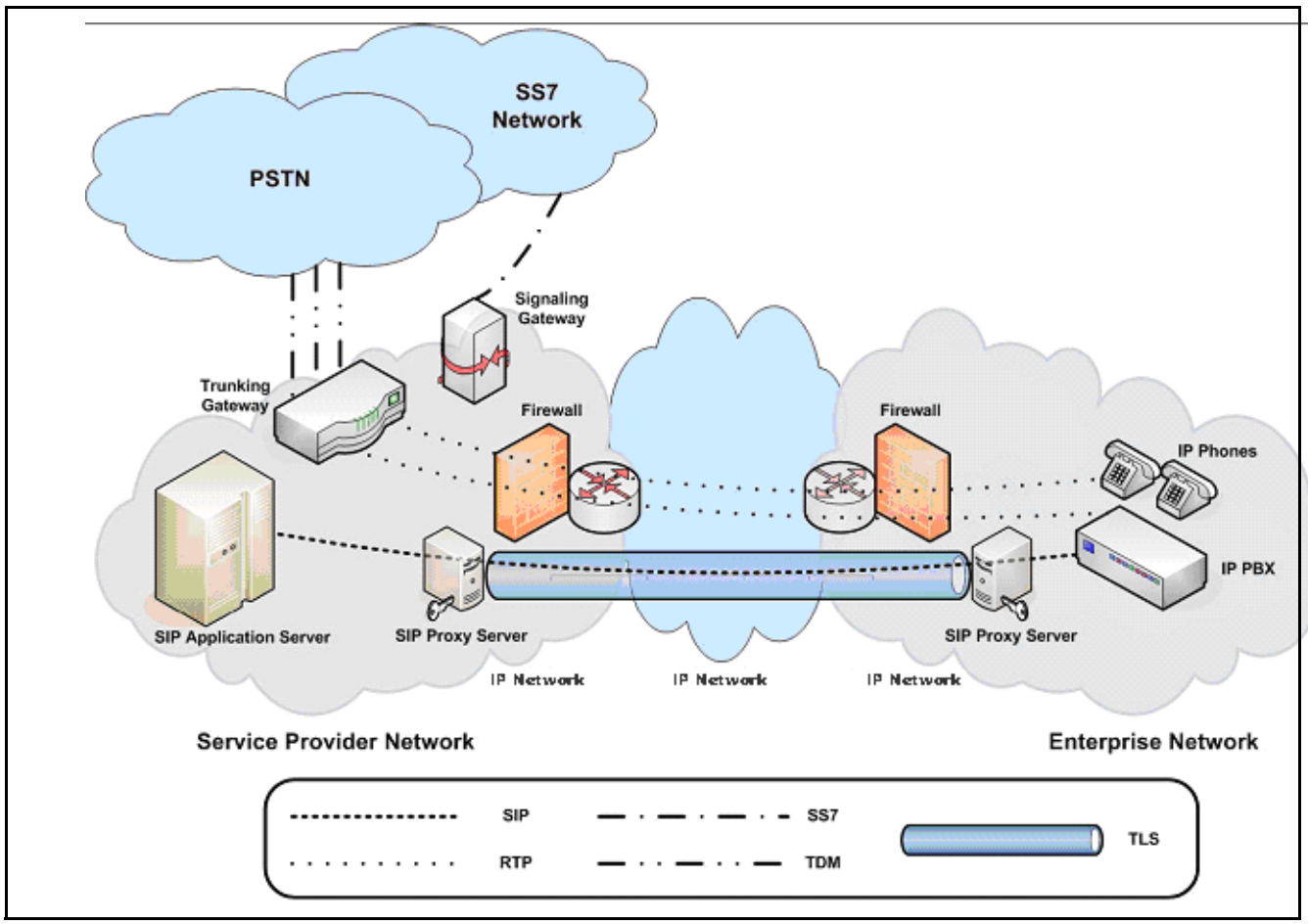


Figure 3 SIP Forum Reference Architecture Diagram

3 Conformance

In order to interoperate correctly, OpenScape Voice and the SP should conform to the requirements in this document.

3.1 Interoperability Testing

Adherence to the normative statements that are presented in this document does *not* guarantee full interoperability of OpenScape Voice with the various SIP Service Providers.

In many cases, the requirements from the Service Providers are different from each other because there is/was no standardized interoperability specification available. There are several specifications from different stakeholders in the VoIP business available that vary in format and contents. Often, no description of how telephony features are executed is provided. Therefore, in addition to this document, which specifies the default behavior, separate Service Provider specific annex documents will be provided which detail specific requirements that are different from this default behavior.

For these reasons, it is absolutely necessary to perform interoperability testing with each Service Provider and OpenScape Voice in order to guarantee successful interoperation between OpenScape Voice and Service Provider products.

Note: Some Service Providers may require formal certification procedures prior to interconnection to their network.

---

4 Architecture

This section contains *informative* descriptions of possible OpenScape Voice deployment scenarios. These are limited to those scenarios which are considered as basic interconnection scenarios of OpenScape Voice systems with Service Providers.

Furthermore, additional network requirements are presented, which partly are normative. These requirements have to be considered when connecting OpenScape Voice systems to Service Providers. These requirements are not an exhaustive list; it is expected that additional requirements will be added to this section in future versions of this document.

4.1 Network Elements

Within an OpenScape Voice system, the following SIP network elements are considered:

- B2BUA (also referred to as SIP Server)
- SIP Proxy/Registrar
- SBC
- SIP Gateway
- SIP Media Server

Furthermore, the following (SIP and non-SIP) network elements are considered:

- SIP Service Provider (may be represented by a SIP proxy or SBC as a single point of entry)
- DNS Server

The following network entities are not considered in this document:

- Clients (phones and softclients)

Note: Wherever clients are mentioned in this document or wherever clients are depicted in figures, it is for illustrative purposes only.

4.2 Enterprise System Connection Scenarios

The following figures show typical scenarios of how an OpenScape Voice system can be connected to the SIP Service Provider network.

4.2.1 Connection via Session Border Controller (SBC)

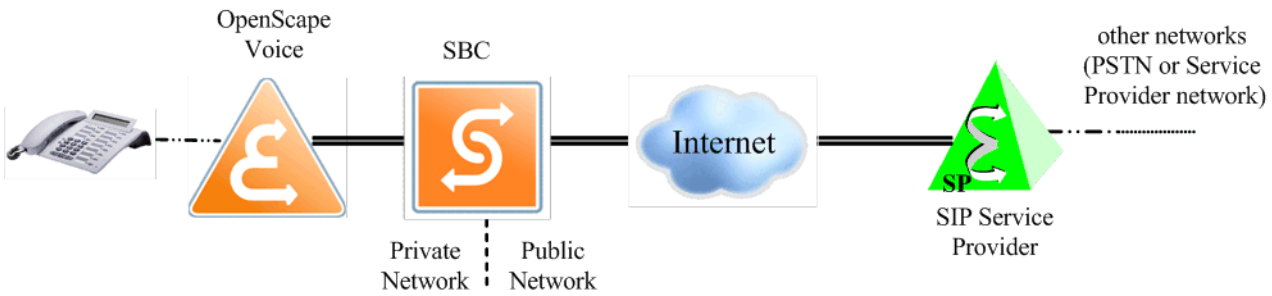


Figure 4 Service provider Connection via Session Border Controller

The scenario depicted in Figure 4 utilizes a session border controller at the boundaries of the OpenScape Voice network. SIP messages that traverse the network boundary through the SBC are modified so that only public IP addresses and ports are visible outside the Enterprise system. The Session Border Controller may be:

- Acme Packet NN2600 or NN3800 series Session Border Controller
- OpenScape Session Border Controller
- OpenScape Branch Proxy including an SBC

4.2.2 Connection via SBC and Virtual Private Network (VPN) Tunnel

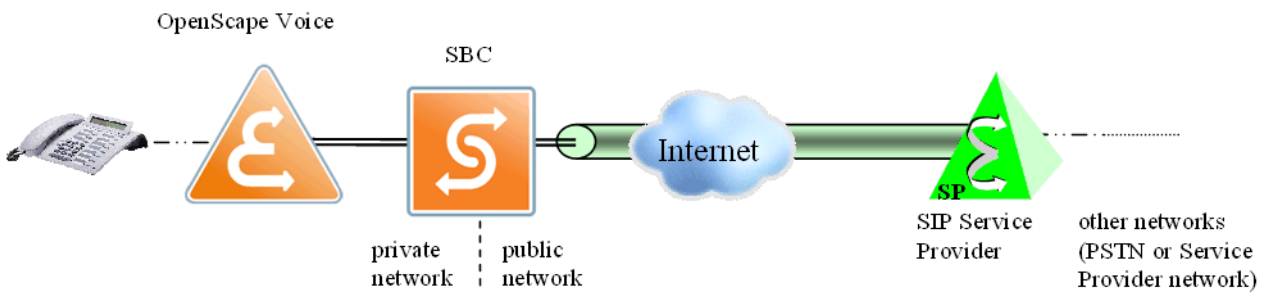


Figure 5 Service Provider Connection via VPN Tunnel

The scenario depicted in Figure 5 shows an Enterprise system that is connected via a VPN tunnel to the Service Provider.

The VPN tunnel is transparent to both the Enterprise system as well as to the Service Provider. SIP signaling may be modified by the SBC—for example, for replacing internal IP addresses or in order to hide the Enterprise topology from the Service Provider.

The VPN tunnel is established by the border devices at the edges of the Enterprise system and the Service Provider system.

4.2.3 Connection via OpenScape Branch (SBC)

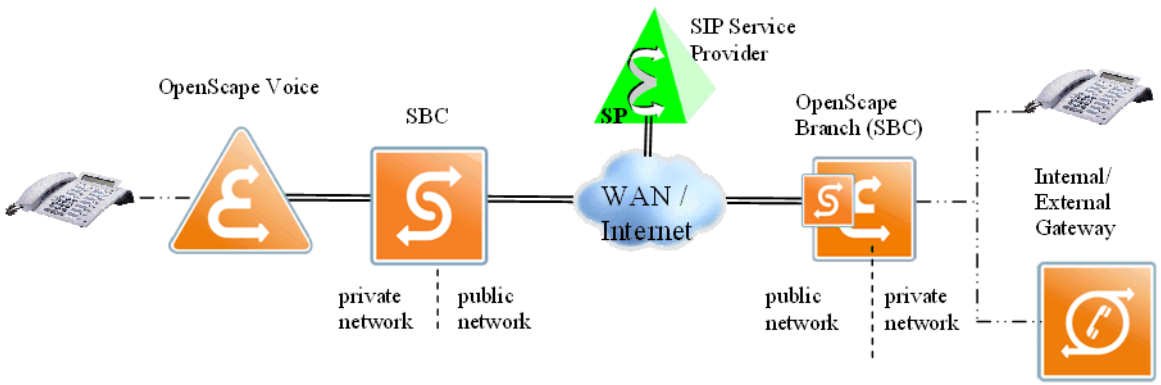


Figure 6 Service Provider Connection via OpenScape Branch (SBC)

The scenario depicted in Figure 6 utilizes the OpenScape Branch (Proxy) and Session Border controller functionality to interface with the Service Provider. When the OpenScape Voice server is not accessible, OpenScape Branch operated in a survivability mode, providing service to local branch users, including service with the SIP Service Provider.

4.2.4 Multi-Tenant IP-PBX Scenario

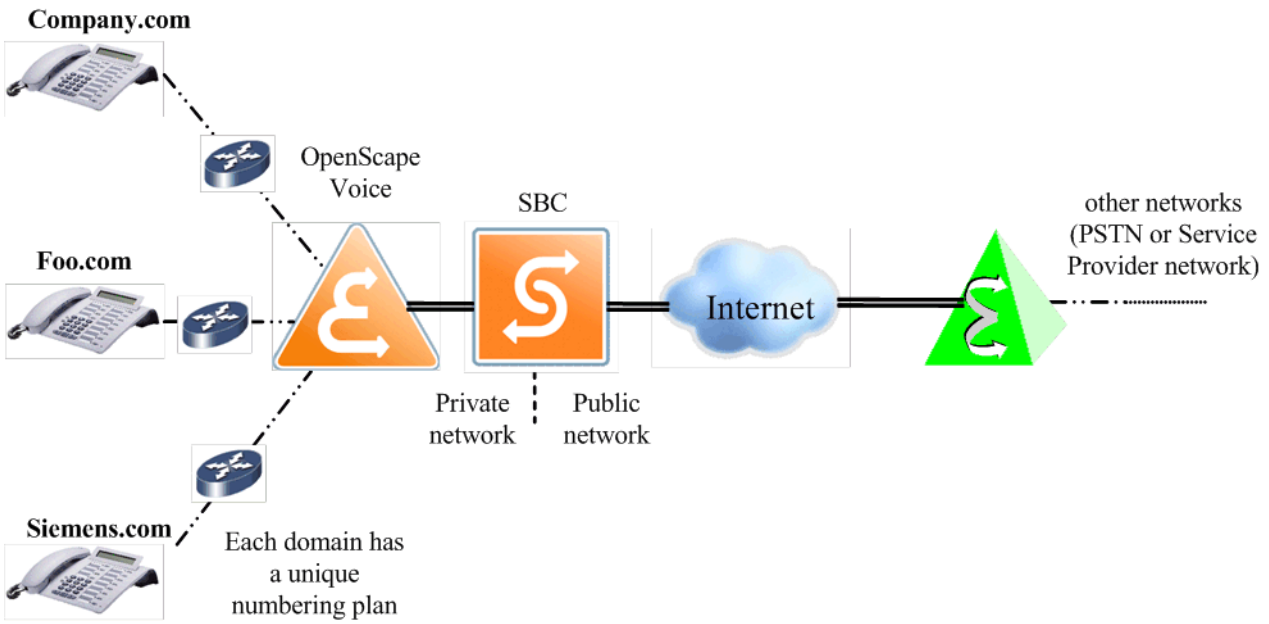


Figure 7 Service Provider Connection in Multi-Tenant Scenario

The scenario depicted in Figure 7 shows a multi-tenant hosted scenario. The Enterprise system hosts more than one Enterprise customer at the same SIP server. Each Enterprise customer is either connected to the same Service Provider, or to different Service Providers (not shown in Figure 7). Enterprise system internal calls—for example, from Foo.com to Siemens.com—may be treated as external calls.

4.2.5 Laboratory Testing Scenario

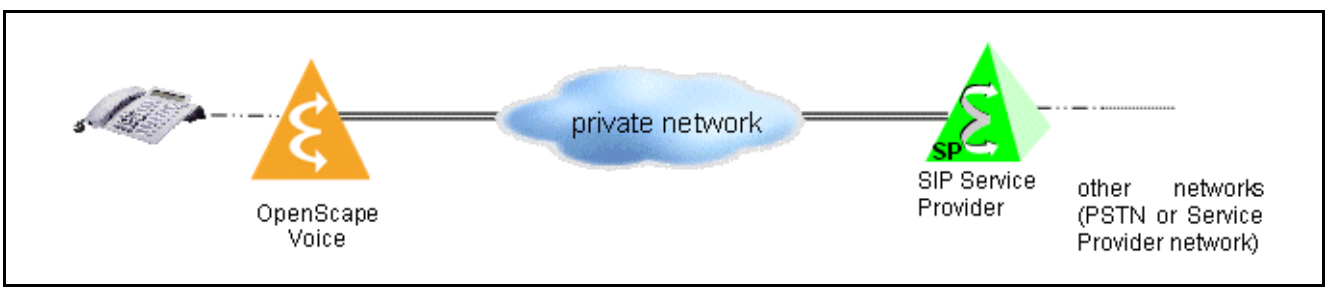


Figure 8 Laboratory Testing Scenario

In a laboratory interoperability testing environment (Figure 8), where OpenScape Voice and the Service Provider system are connected to the same private LAN, use of an SBC may not be necessary. In this scenario, OpenScape Voice and the SP will communicate using private IP addresses.

4.3 Signaling and Network Requirements

This section contains network requirements that are mainly relevant for interconnecting OpenScape Voice systems with Service Providers.

Furthermore, signaling requirements for support of higher-level features are presented as well.

4.3.1 Locating SIP Servers

A DNS SRV entry in a publicly accessible DNS server (that is authoritative for the OpenScape Voice domain) should be provided if the SP does not know the IP address of the OpenScape Voice server by other means. The DNS server does not necessarily have to be inside the OpenScape Voice server domain. It may be a public DNS server—for example, provided by the SP—or it may be a DNS server that resides within a demilitarized zone of the system.

When the OpenScape Voice nodes are geographically separated and more than one OpenScape Voice server location is detected, the SP shall be able to route SIP requests to the alternative OpenScape Voice server in case of failure conditions.

Outbound Requests:

The SBC connected to the OpenScape Voice system may send queries to the SP DNS server to retrieve SRV records (IP addresses). The SBC connected to the OpenScape Voice system will use these query results for subsequent outbound requests to the SP.

If DNS lookups are used and more than one SIP server location is detected, the SBC connected to the OpenScape Voice system is able to route SIP requests to the alternative SP SIP servers in case of failure conditions.

It is possible to use other mechanisms than DNS lookups if the SP and the OpenScape Voice system have a mutual agreement. In this case, the SBC connected to the OpenScape Voice system may be statically configured with the SP IP address or IP addresses.

Note: In the laboratory testing scenario (where there is no SBC), OpenScape Voice will itself make the DNS queries if necessary, and provide alternate routing to alternative SP SIP servers in the case of failure conditions. OpenScape Voice currently only supports DNS queries for A-records; support for NAPTR/SRV queries may be provided in a future release.

4.3.2 Registration

OpenScape Voice does not currently support dynamic registration of any Address of Record (AoR) with a Service Provider.

SIP REGISTER requests are not sent between OpenScape Voice and SP.

The Contact information for the set of Direct Inward Dialing (DID) numbers—for example, from 5617221000 to 5617225999—that is assigned to the OpenScape Voice Enterprise server should be provisioned (static registration) at the Service Provider. The Service Provider sends all incoming call requests that are directed to any of the DID numbers to the Contact address that has been statically registered for the OpenScape Voice system. The Service Provider is not aware of actually existing or currently registered clients within the OpenScape Voice system.

When a SP does not support static registration and requires IP PBX's to register then the "Surrogate Registration" capability of the SBC may be utilized.

Authentication of SIP requests to/from a SP is supported; see Section 4.3.3, “Authentication”.

4.3.3 Authentication

The OpenScape Voice system supports digest authentication towards the Service Provider.

When authentication is used, the Service Provider should challenge the OpenScape Voice system.

The Service Provider should challenge the first request of a dialog, unless it contains already valid authentication credentials. All other SIP requests may be challenged.

If authentication is used it will be on an “endpoint basis”—that is, a single set of credentials will be used for authentication of calls on the OpenScape Voice to SP interface; individual subscriber authentication will not be used. Authentication credentials are provisioned at the OpenScape Voice server via provisioning using the SIP → HTTP Authentication → Realm menu/screen. A Realm is created for each SP and associated authentication credentials are specified.

Although not normally required, the OpenScape Voice server may be configured to also challenge SIP requests received from a SP in the same manner as described above for the SP side.

Note: Use of digest authentication between the OpenScape Voice server and the SBC used to connect to the Service Provider is often not required, as the SBC and SP may be considered trusted entities. If digest authentication is used, the impact on traffic capacity and system performance must be considered as authentication introduces additional SIP messages during call establishment.

4.3.4 NAT Traversal

Virtually every OpenScape Voice system and Service Provider has NAT devices deployed at the network edges. NAT presents a range of problems to a VoIP system: private IP addresses and ports are translated into public IP addresses and ports, which makes incoming signaling and media stream handling difficult.

OpenScape Voice makes use of an SBC to handle the NAT traversal problem.

4.3.4.1 Session Border Controller

OpenScape Voice connects to Service Providers via an SBC (e.g. ACME Packet Net-Net 38xx/42xx SD, SD 2600, or OpenScape SBC, etc.).

- How it works:

An SBC is able to modify SIP signaling messages and MIME bodies (including SDP) to reflect the public IP addresses and ports that must be used for signaling and media traffic (see Figure 9). The SBC understands the used protocols (for example: SIP, SDP, and so on), is session-aware, and has knowledge about the public IP addresses and ports that are used for each session.

Note: This section assumes that an on-the-path SBC with topology hiding is deployed. *On-the-path SBC* means that the SBC has both an internal as well as a public IP address. Hence, all signaling and media traffic must traverse this device. A *topology-hiding SBC* hides internal IP addresses from the outside world and it hides public IP addresses from the internal network.

- SIP Signaling Traffic

  An SBC should place its public IP address and port or a domain name (for example, of the OpenScape Voice system or of the Service Provider) into each SIP message that is sent to the Service Provider.

  The following SIP message header fields may contain public IP addresses, unless they contain a domain name:

  – *Request URI*

  – *Contact* header field

  – *From/To* header fields

  – *Via* header field (with received tag and *rport* tag, if supported)

  – *Record-Route* header field

  – *P-Asserted-Identity* header field

  – SDP bodies and other MIME bodies

- Media Traffic:

  An SBC should support sending and receiving media streams as indicated in Figure 9.

  In order to achieve this, the SBC should rewrite any sent SIP request and response that contains an SDP body with its own public IP address and port that is intended to receive the incoming media stream from the public network. Furthermore, the SBC should rewrite any received SIP request or response with an SDP body with its own internal IP address and port that is intended to receive the outgoing media stream from the internal network.

  This is illustrated in Figure 9. Any incoming SDP body (that is, from the SBC's internal side into the OpenScape Voice internal network) contains only the SBC's internal address and port. Any outgoing SDP body (that is, from the SBC's public side to the internet) contains only the SBC's public IP address and port.

- Security:

  An SBC may offer TLS origination and termination services of SIP signaling traffic in order to secure the trunking connection between the OpenScape Voice system and the Service Provider. Furthermore, it may support creation of VPN tunnels via IPSec or any other VPN protocol.

  An SBC must also support at least pass-thru of encrypted media (SRTP) and key exchange protocols and may also provide mediation between different key exchange protocols e.g. MIKEY#0 and SDES.

  Note: An SBC may also provide firewall protection, DoS prevention, or VPN tunnel support capabilities.

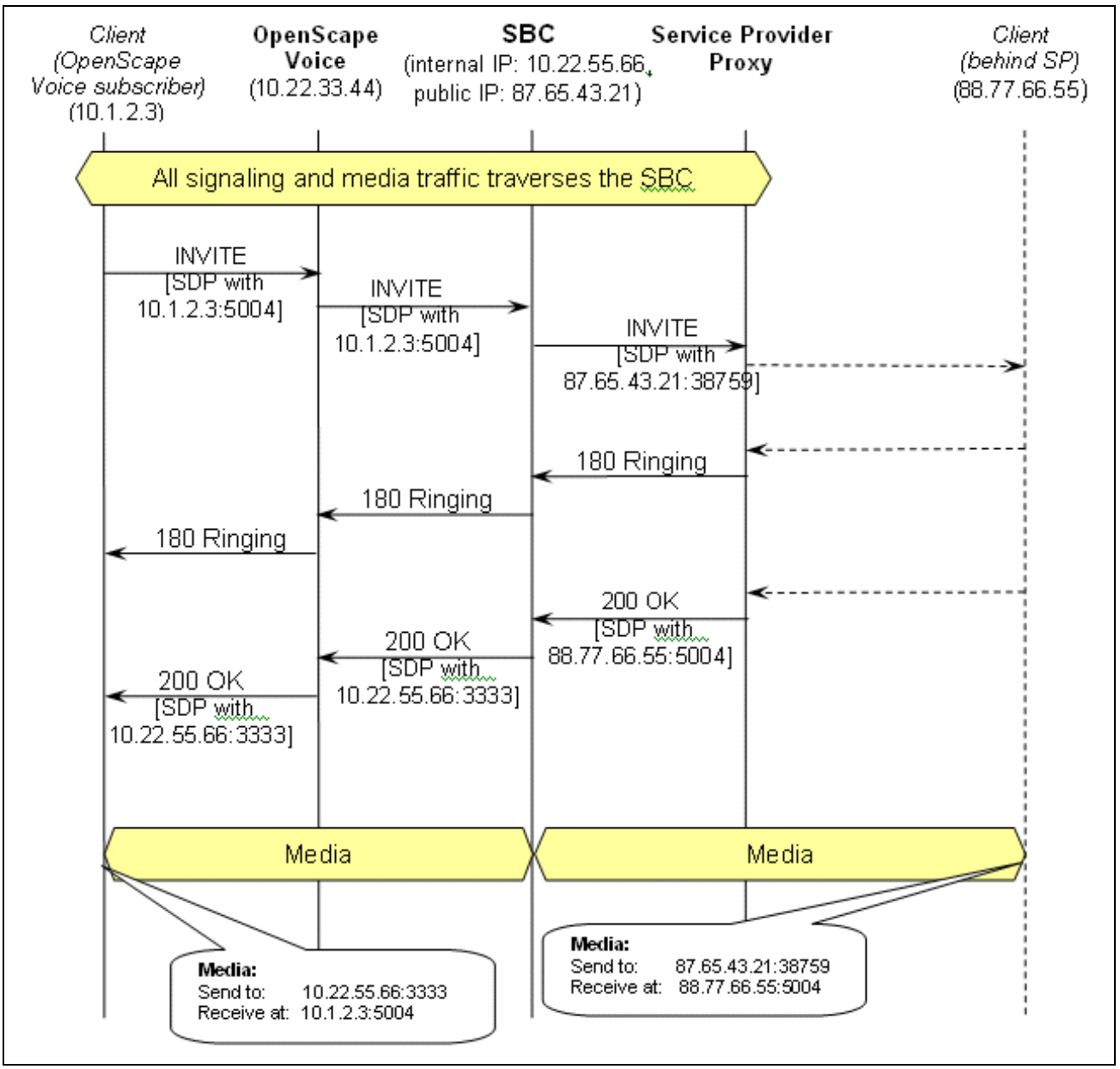


Figure 9 Example SBC at the OpenScape Voice System Boundary

4.3.5 Session Timers

Session Timers are defined in RFC4028 [30]. This mechanism ensures that SIP sessions are periodically refreshed in order to make sure that no stale sessions remain in session-aware SIP network elements should a BYE request be lost due to endpoint or network failures.

OpenScape Voice supports SIP Session Timing using SIP reINVITE requests as the session refresh mechanism.

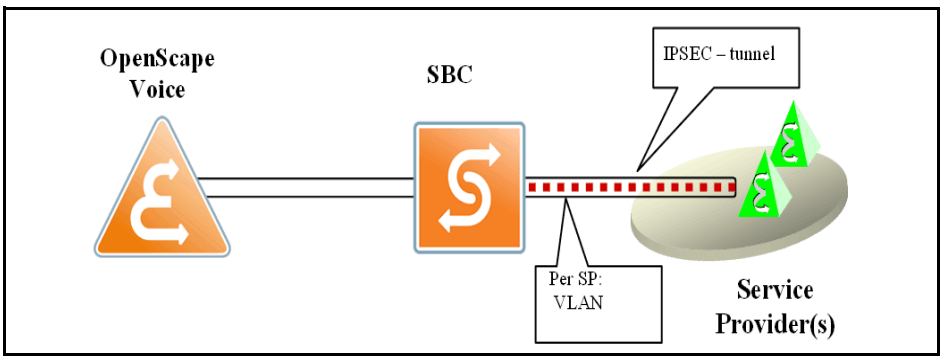
4.3.6 Signaling and Payload Encryption (SPE)

4.3.6.1 Signaling Encryption

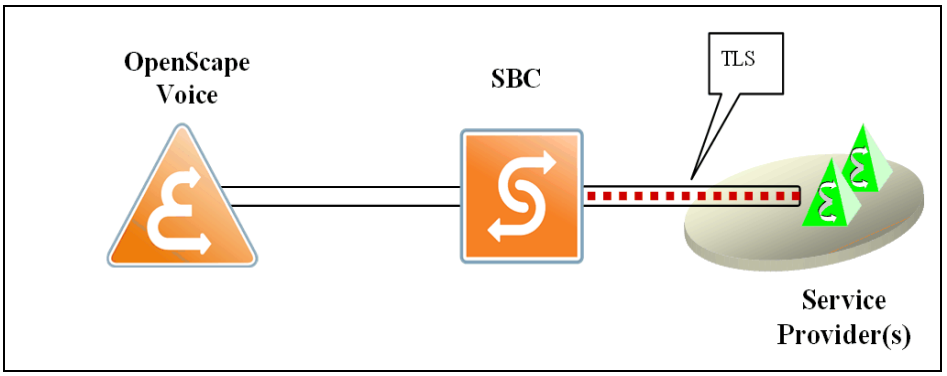
If SIP signaling security is required (SP is in a non-trusted domain), the SBC can secure the SIP signaling connections using IPSec or TLS on the external (public) side to/from the SP.

SIP signaling security between OpenScape Voice and the SBC is generally not required, but if necessary TLS may be used.

IPSec



TLS



The handling of the TLS origination and termination to/from the SP can be provided by the SBC.

If TLS is supported, both the SBC and the SP must have a valid certificate for the domain that they are responsible for. If multiple domains are supported, for each supported domain a corresponding certificate must be used.

A SBC should verify the SP's certificate for establishing the TLS session. This includes checking that:

- The certificate is not expired,
- The certificate is valid with respect to a stored root certificate
- The issuing certification authority is a trusted authority (from the OpenScape Voice perspective).
- The *subject* of the certificate matches the SP's domain.
- The status of the certificate should be checked using a suitable mechanism like CRL (RFC3280 [14]) or via OCSP (RFC2560 [5]),
- Additionally, all certificates in the certificate chain should be validated as well.

The certificate that is presented to the SP should be signed by a trusted third-party certification authority. However, self-signed certificates may be used in accordance with the SP.

The SBC should support TLS mutual authentication on SIP server connections. When OpenScape Voice is configured to use a single IP address per node in conjunction with TLS Server and Mutual Authentication, the SBC or any other SIP endpoint that communicates with OpenScape Voice via Mutual TLS, must utilize

a different non-standard port if using TLS Mutual Authentication. For this OpenScape Voice configuration, a default port of 5161 is used to support TLS Mutual Authentication.

Note: The ACME Packet SBC (Net-Net 4250 SD) only supports TLS for the external SIP signaling interfaces towards the SP; TLS is not supported on the internal SIP signaling interfaces towards the OpenScape Voice server. So, although OpenScape Voice does support TLS, it cannot currently be used for the link between the OpenScape Voice server and the SBC.

4.3.6.2 Payload Encryption

Securing Media Streams

The negotiation of the SDP for payload encryption is primarily an end-to-end function achieved by the two endpoints. For pure SIP scenarios, the OpenScape Voice server will pass the SDP transparently between the two end points. Having said that, OpenScape Voice has to identify calls as using payload encryption for various purposes and it does this by recognizing that at an m-line in the SDP answer contains the “SAVP” string (for example, “m=audio 62986 RTP/**SAVP** 0 4 18”).

SIP Service Provider in Conjunction with On-Net SRTP/SPE

- For SBC’s capable of interworking between Siemens Best Effort SRTP and a SIP Service Provider that is only RTP capable, the Best Effort SRTP support field in the Endpoint SIP options for the SBC endpoint in OpenScape Voice must be set to "MIKEY, SDES". The SBC must be configured to interwork the media session between SRTP for the inside network and RTP for the outside network interface with the SIP Service Provider.
- For SBC’s unable to terminate SRTP media sessions, i.e., only capable of operating in a media session “pass-thru” mode, the Best Effort SRTP attributes should be set to “Disabled”.
- Transport Protocol between SBC and OpenScape Voice must be set to TCP or TLS.

4.3.7 DTMF

There are two ways to transmit DTMF tones:

- Inband DTMF

  Inband transport of DTMF tones means that the DTMF tones are transmitted within the RTP stream that is generated by the client. This is only possible if the RTP stream is not compressed—for example, with the G.711 codec. Other codecs that perform a compression/decompression—for example, G.729—are not suitable.

  The OpenScape Voice system supports this mechanism.

- DTMF via RFC2833

  Transport of DTMF tones is achieved via Named Events using two RTP payload formats, named telephone-event and tone, and associated Internet media (MIME) types, audio/telephone-event and audio/tone. These payload formats use a dynamic payload type number (for example, payload type 98 or 101). These payload formats can be interpreted at a PSTN Gateway, or at an Application Server or an Interactive Response System. See RFC2833 [6].

  The OpenScape Voice system supports this mechanism.

4.3.8 FAX

There are two ways to transmit FAX data:

- Inband FAX

  The OpenScape Voice server supports inband transport (origination and termination) of fax or modem calls (for audio-based media) using the G.711 codec as a best effort. Other methods may be supported end-to-end between the gateways involved in the fax communication. In this scenario, the OpenScape Voice system supports transparently passing an SDP body.

- FAX via T.38

  The OpenScape Voice system is able to support T.38 FAX handling according to RFC 3362 between two participating gateways. The OpenScape Voice system supports transparently passing an SDP body. This is necessary in order to allow for end-to-end T.38 signaling.

  Details on T.38 fax handling can be found in the ITU-T document ITU-T T.38 [34] and RFC3362 [39].

4.3.9 Codecs

OpenScape Voice does not send/receive media streams itself, and therefore does not use the RTP/RTCP protocol. Although OpenScape Voice does not use RTP/RTCP, it may still need to recognize payload type information carried in the SDP for various purposes—for example, call admission control/bandwidth resource management. Payload types that OpenScape Voice does not recognize may still be used between SIP endpoints for audio and/or video sessions (passed transparently by OpenScape Voice), but interworking with endpoints using signaling protocols other than SIP may not be possible and other OpenScape Voice-based functionality may be limited.

OpenScape Voice recognizes the following payload types:

Note: Only the payload types marked with an asterisk (*) are recognized by OpenScape Voice Call Admission Control (Internal Resource Manager). Other network elements—for example, media servers, gateways, and so on—may not support all of the payload types. Refer to the third-party product documentation to determine which payload types they support.

---

audio/AAC-LC*	video/H264_L4
audio/AMR*	audio/telephone-event
audio/AMR-WB*	image/t38
audio/G721-24*	video/H261
audio/G721-32*	video/H263
audio/G721-48*	video/H263-L40
audio/G722*	video/CelB
audio/G723*	video/H263_L45
audio/G726-16*	video/H263-1998
audio/G726-24*	video/H263-2000
audio/G726-32*	video/H264
audio/G726-40*	video/H264_L1B

audio/G728*
audio/G729*
audio/ILBC*
audio/PCMA*
audio/PCMU*
video/MPEG2
video/MPEG4
video/MPEG4_P2_L0B
video/MPEG4_P2_L2
video/H264_L1_2
video/H264_L1_3
video/H264_L3
video/JPEG
video/MP2T
video/MPV
video/nv
CLEARMODE

4.3.10 Transport Protocol

The OpenScape Voice server supports the following transport protocols for the SIP trunking interface:

- UDP
- TCP
- TLS (security protocol which uses TCP as underlying transport protocol)

Established TCP and TLS connections should be reused in order to avoid repetitive TCP or TLS connection setups for each request and response.

See Section 4.3.6, “Signaling and Payload Encryption (SPE)” on securing connections between the OpenScape Voice server and Service Provider.

Note: UDP datagrams that exceed the size of the layer 2 maximum transmission unit (MTU), which for Ethernet is 1500 bytes, may or may not be received correctly. Although fragmentation and re-assembly at the IP layer can be used for long datagrams, packet loss or excessive delay can make this unreliable. RFC 3261 mandates that if a request is within 200 bytes of this maximum (i.e., 1300 bytes), it must be sent using a reliable transport, e.g., TCP. The additional 200 bytes allows the response to be slightly larger than the request. Switching between UDP and TCP on a per transaction basis, depending on the size of the request, is difficult and is not guaranteed to take account of oversize responses. Therefore UDP should not be used when oversize messages are a possibility. For example, oversize messages are likely when the following feature capabilities are used:
- Large number of session description protocol payload types or attributes
- Large header field parameters, or URI parameters
- IPv6 addresses

It is recommended to use TCP transport for the Service Provider interface. While OpenScape Voice does not enforce the RFC3261 mandate for UDP mentioned above, to minimize possible side effects, the default transport type in OpenScape Voice for SIP interfaces added to the configuration is TCP.

Note: OpenScape Voice can be configured with a local port for SIP signaling using UDP, TCP, TLS or MTLS. The default port for UDP and TCP is 5060, and for TLS or MTLS is 5061. When the OpenScape Voice IP addresses for TLS and MTLS are the same, then port 5161 must be used for MTLS.

4.3.11 IPv6

IPv6 support is not currently available for SIP Service Provider interfaces. Support for interworking between IPv6 and IPV4 networks for non-dual stack clients is only supported in OpenScape Voice via an SBC.

4.3.12 Quality of Service

The Differentiated Services Code Point (DSCP) value determines the drop probability for an IP packet. The DSCP value is the first six bits of the IP type of service (ToS) byte.

The OpenScape Voice system will mark IP packets with SIP signaling messages that are sent to the Service Provider with an appropriate value for VoIP SIP signaling. The OpenScape Voice default DSCP values should not need to be changed under normal circumstances. OpenScape Voice Technical Support should be contacted if the DSCP value has to be changed.

The recommended values for VoIP are:

TOS

Precedence Field = CRITICAL/ECP

TOS Field = Normal Service

DSCP

Class = Default PHB

Precedence = High

Both the above create a Type of Service octet value of 101000xx in the IP packet header

The TOS/DSCP value in IP packets with RTP media or RTCP data is controlled by the endpoint sending the media/data.

4.3.13 Monitoring Service Level Agreements

The SBC may generate per-call CDRs that include packet delay, jitter, packet loss, and such statistics. These parameters can be made available over a RADIUS interface; however, this is out of scope of this document. See ACME Packet documentation [ACME_RADIUS] for further details.

4.3.14 Emergency Calls

Emergency calls are normally routed via gateways that support transport of Location Identification Number (LIN) information and onward routing via Channel Associated Signalling (CAS) trunks to an E9-1-1 tandem switch.

If emergency calls are routed via SIP trunking to a Service Provider, the OpenScape Voice system may by configured to provide a Location Identification Number (LIN) in the From header (and P-Asserted-Identity header if present) of the SIP INVITE information.

The OpenScape Voice system may also be configured to include the LIN as multi-part MIME in the body of the SIP INVITE (instead of in the From / PAI headers) as shown in this example:

```
Content-Type: text/plain
Content-Disposition: render; handling=optional
LIN=4951199987910
```

Use of the phone-context parameter in the To: header (to represent the physical location from which the call originated) is not supported by OpenScape Voice.

4.3.15 SIP INVITE without SDP Offer (AKA Delayed SDP)

OpenScape Voice sends SIP INVITE requests that do not contain an SDP offer when certain 3PCC (and other) Enterprise services are used. The Service Provider is expected to respond to these 'offerless' INVITE's with an SDP offer in the 18x or 200 response in accordance with RFC3264 [11]. To accommodate Service Providers that do not comply with the RFC, OpenScape Voice provides a configuration option via the following endpoint attribute:

Do not send INVITE without SDP

When this attribute is enabled, OpenScape Voice will send the previously negotiated SDP in a reINVITE, or in the case of an initial INVITE a dummy SDP, in scenarios where OpenScape Voice would normally send an offer less INVITE. See OpenScape Voice FRN3290 feature description for details of other configuration parameters associated with this feature.

Note: Use of this configuration option has limitations, and is not a substitute for full RFC compliance on the part of the Service Provider.

4.3.16 SDP Size

The maximum SDP size supported by OpenScape Voice in V6 is 10 Kbytes.

5 Features

This section contains *normative* statements of a limited set of telephony features.

The goal of this section is to provide *normative* statements which are accompanied by *informative* descriptions for stakeholders like Product Management, Technical Sales personnel, and (Service Provider) partners that need to get an overview of our SIP Trunking feature signaling principles. The focus of this section is to describe the signaling messages that need to be exchanged in order to achieve a particular feature. For sake of simplicity, only straightforward cases are depicted.

The control of features that are distributed between OpenScape Voice and the Service Provider is outside the scope of this version of the specification. In many cases, there are different ways of signaling for accomplishing the same features. Feature interworking with Service Providers is still subject to further study and might undergo some changes in the signaling. Updated versions of this document will try to keep up with the developments on the interface to the various Service Providers.

5.1 Number Identification

5.1.1 Calling Line Identification Presentation (CLIP)

CLIP (Calling Line Identification Presentation) provides the called party with the identity of the calling party. The identity consists of an optional name and telephone number of the calling party.

Identity information to be included in *P-Asserted-Identity* header fields is inserted by the SSNE that is responsible for the calling party. Therefore, the SSNE should authenticate the calling party in order make sure that the correct identity information is included.

Note: It may also be possible that a Service Provider inserts identity information on behalf of the calling party. However, this is outside the scope of this document.

OpenScape Voice is able to send identity information to a Service Provider which provides the CLIP feature for the called party.

Likewise, OpenScape Voice is able to process identity information received from a Service Provider for presentation to an OpenScape Voice called party.

The calling identity information is communicated between the OpenScape Voice and Service Provider based upon the Enterprise "Trust Domain" relationship between the OpenScape Voice and the Service Provider. Reference Section 6.4.21 for a description of the Enterprise "Trust Domain" and application using the P-Asserted-Identity header field.

5.1.1.1 CLIP procedures by OpenScape Voice:

Sending requests and responses to a Service Provider:

The identity conveyed in the following fields may be used to identify an OpenScape Voice authentication number which may not always be the calling party. For example, external calls which arrive in the OpenScape Voice Provider due to OpenScape Voice features may be redirected back to the Service Provider. The authentication number is typically used to identify an OpenScape Voice Number to the Service Provider (reference *Section 6.4.22*).

The identity information is sent in one or more of the following header fields, each containing URI's according to the following criteria based upon the available identity information:

- Name and Number Available
  "Some Name" <sip:12345@10.0.0.100>
- Name and Number Unavailable
  <sip:10.0.0.100>
- Number Unavailable
  "Some Name" <sip:h8k1.siemens.com>
- Name Unavailable
  <sip:12345@10.0.0.100>

The authenticated number identity to be sent to the Service Provider can be chosen as an option based on the type of call. With this option, a different authenticated number identity may be used other than the default behavior which uses the external Caller-ID for subscriber originated calls or feature calls, or the default home DN for trunk originated calls.

- For an OpenScape Voice subscriber originated call or feature subscriber call, the subscriber account or home DN or the enterprise organization’s account
- For Service Provider originated calls the default home DN
- The enterprise organization’s account or default home DN for all calls.

1. *P-Asserted-Identity* header field (see Section 6.4.21, “P-Asserted-Identity”)

   This header field is used if the Service Provider is considered part of the Enterprise "Trust Domain". For such a relationship, the OpenScape Voice SIP Endpoint Profile's 'Privacy' support should be set to 'Full' or 'Full-Send'.

OpenScape Voice will include the P-Asserted-Identity header field in SIP INVITE requests containing a public identity. Normally, only public identities are sent to the Service Provider so if the calling party is a member of a user group with a private numbering plan then the callers private name and/or number will not be sent in the P-Asserted-Identity. As an option, depending on the originating caller, the header field may be used to identify an OpenScape Voice calling subscriber account or home DN, a feature subscriber account or home DN or the enterprise organization default home DN.

If the Service Provider is not considered part of the Enterprise "Trust Domain" or is unable to process the P-Asserted-Identity header field, then the OpenScape Voice SIP Endpoint Profile's 'Privacy' support may be set to 'Basic' or 'Full-Receive', in which case no P-Asserted-Identity header field will be sent.

2. *P-Preferred-Identity header field (see Section 6.4.22)*

   The same guidelines as P-Asserted-Identity above are followed, except that the P-Preferred-Identity header field is sent. This option is dependent on the OpenScape Voice SIP Endpoint Attribute 'Send P-Preferred-Identity rather than P-Asserted-Identity' setting (reference Section 7).

3. *From* Header field (see Section 6.4.17, “From”)

   The OpenScape Voice responsible for the calling party may remove the original identity information from the received From header field from the client and insert appropriate public identity information from the OpenScape Voice database. Usually, this header field contains the desired public PSTN identity of the subscriber.

Note: OpenScape Voice is able to provide an OpenScape Voice authentication number within the P-Asserted-Identity (or P-Preferred-Identity) or From header field for calls which are redirected or transferred to the Service Provider (reference "Send authentication number in P-Asserted-Identity header", "Send P-Preferred-Identity rather than P-Asserted-Identity" or "Send authentication number in From header", endpoint attributes in Section 6.4). The OpenScape Voice "Send authentication number in P-Asserted-Identity header" attribute overrides the OpenScape Voice SIP Endpoint Profile 'Privacy' support setting of 'Basic' or 'Full-Receive for the initial INVITE.

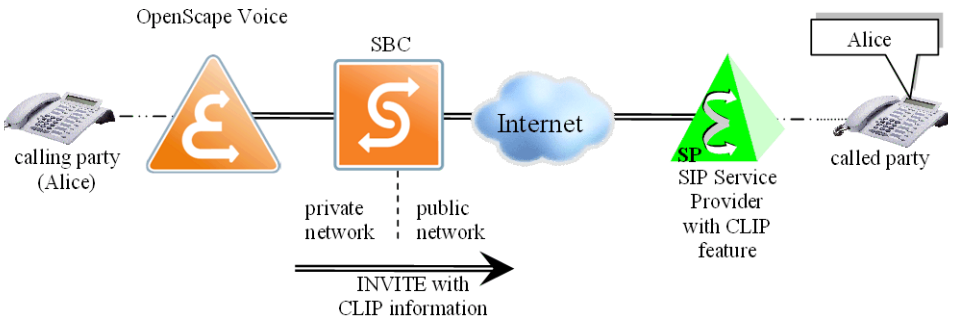


Figure 10 *Example: CLIP Information Exchange (Outgoing Call to Service Provider)*

	Header Field Values for CLIP
P-Asserted-Identity:	"Acme Rockets Sales" <sip:+15617221122@provider.com>
Privacy:	–
From:	"Acme Rockets Sales" <sip:+15617221122@provider.com>

Table 5.1 *Example: Header Fields used for Calling Line Identity Presentation information (Call to Service Provider)*

Note: The example in Table 5.1 shows example header fields that are sent to a Service Provider. The hyphen indicates that the corresponding header field is not present in the SIP request.

Receiving requests and responses from Service Provider:

The Enterprise system SHOULD be able to process a *P-Asserted-Identity* header field in received *INVITE* requests from the Service Provider (for example, for display update and call logging purposes). If no *P-Asserted-Identity* header field is present, identity information from the *From* header field may be used for these purposes.

Note: This corresponds to an incoming call (from the Service Provider to the Enterprise system), where the call originator provides calling line identity information consisting of the number and optionally a name which may be used for presentation to an OpenScape Voice SIP client.

The header fields used for processing calling identity information is dependent on the Enterprise "Trust Domain" relationship and is reflected in the OpenScape Voice SIP Endpoint Profile's 'Privacy' support.

If the OpenScape SIP Endpoint Profile's 'Privacy' support is set to 'Full', or 'Full-Receive', the Service Provider is expected to provide a P-Asserted-Identity header field as part of its "Trust Domain" relationship with OpenScape Voice.

If the OpenScape SIP Endpoint Profile's 'Privacy' support is set to 'Basic', or 'Full-Send', the Service Provider is expected to exclude sending a P-Asserted-Identity header field due to its limited Enterprise "Trust Domain" relationship with OpenScape Voice. OpenScape Voice will ignore the P-Asserted-Identity header field sent by the Service Provider and will use the identity in the From header field.

OpenScape Voice is able to process identity information for the name and number independently according to the Service Provider supplied header and fields and available URI content.

For example:
- Name Available, Number Unavailable
“Some Name" <sip:10.0.0.100>
or
"Some Name" <sip:unavailable@[valid-domain]>
- Name Unavailable, Number Available
<sip:12345@10.0.0.100>
- Number Available
sip:[valid-domain]
or
sip:unavailable@[valid-domain].

OpenScape Voice also supports processing a received *Remote-Party-ID* header field defined in draft-ietf-sip-privacy [43] and predecessor of the *P-Asserted-Identity* header field, for Calling Party Identification and for Service Providers that do not support the *P-Asserted-Identity* header. The support of the *Remote-Party-ID* header field is described in Section 6.4.31, “Remote-Party-ID” and is processed when received in an initial SIP INVITE request. When the SIP INVITE request is received with the display-name parameter set to *pending*, then OpenScape Voice shall also process a *Remote-Party-ID* header field received in a SIP INFO message containing the delayed Calling Name. The rpi-privacy parameter, described in Section 6.4.31, “Remote-Party-ID”, specifies whether calling identity information, i.e. name and number, can be presented or must be hidden from untrusted entities.

Note: OpenScape Voice shall not support sending the *Remote-Party-ID* header field in any message. When received in a SIP INVITE request, it shall be mapped to a *P-Asserted-Identity*, *P-Preferred-Identity* or *From* header field per conditions described under Sending requests and responses to a Service Provider:. The *Remote-Party-ID* header field received in a SIP INFO message containing the delayed Calling Name is mapped to a *P-Asserted-Identity* header field sent in a SIP UPDATE message.

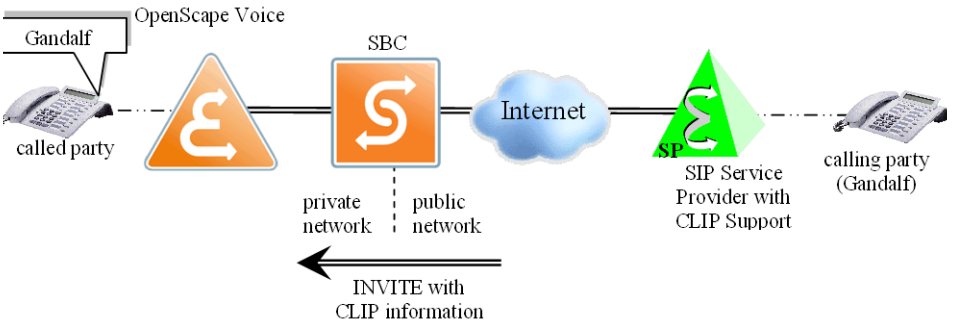


Figure 11 *Example: CLIP information exchange (incoming call from Service Provider)*

5.1.1.2 CLIP procedures by Service Providers:

Sending requests and responses to OpenScape Voice:

A Service Provider may send identity information in a *P-Asserted-Identity* header field and a *From* header field to the OpenScape Voice system. This corresponds to an incoming call (from the Service Provider to the OpenScape Voice system), where the call originator provides calling line identity information consisting of a number and optional name.

Note: f the Service Provider does not support the *P-Asserted-Identity* header field, they may send the *Remote-Party-ID* header field according to the guidelines described in Section 6.4.31, “Remote-Party-ID”.

Receiving requests and responses from OpenScape Voice:

A Service Provider may make use of the *P-Asserted-Identity* header field in received requests from an OpenScape Voice system.

5.1.2 Calling Line Identification Restriction (CLIR)

CLIR (Calling Line Identification Restriction) prevents the called party from receiving the identity of the calling party.

In order to support CLIR, the SSNE supporting the calling user must identify the identity suppression requirements within the INVITE request to restrict the identity presentation to the called user.

OpenScape Voice relies on the Enterprise "Trust Domain" relationship discussed in Section 5.1.1 to determine the calling identity suppression information to be sent or processed for restricting the calling identity presentation to the called user

OpenScape Voice:

Sending requests and responses to Service Provider:

If the OpenScape Voice SIP Endpoint Profile's 'Privacy' support is set to 'Full' or 'Full-Send' and the calling identity is restricted, OpenScape Voice will include a P-Asserted-Identity header field along with a 'Privacy:id' header field (or ’P-Preferred-Identity’ header field) within the SIP INVITE request (reference Section 5.1.1). The *From* header field will be populated according to the OpenScape SIP endpoint attribute 'Include Restricted Numbers in From Header' (reference - Section 7). The following are some examples:

- Name and Number Restricted; 'Include Restricted Numbers in From' enabled:

  From: "Anonymous" <sip:12345@10.0.0.100>
  Privacy:id, user
  P-Asserted-Identity: "Some Name" <sip:12345@10.0.0.100>

- Name and Number Restricted; 'Include Restricted Numbers in From' disabled

  From: <sip:anonymous@annonymous.invalid>
  Privacy:id
  P-Asserted-Identity: "Some Name" <sip:12345@10.0.0.100>

If the OpenScape Voice SIP Endpoint Profile's 'Privacy' support is set to 'Basic' or 'Full-Receive' and the calling identity is restricted, OpenScape Voice will not include a P-Asserted-Identity header field or Privacy:id header field in the INVITE. The From header field will however be populated according to the required identity restrictions according to the OpenScape SIP endpoint attribute 'Include Restricted Numbers in From Header' setting.

Some examples:

- Name Available, Number Restricted and “Include Restricted Numbers in From Header” is disabled

  From: "Some Name" <sip:anonymous@anonymous.invalid>

- Name Available, Number Restricted and “Include Restricted Numbers in From Header” is enabled

  From: “Anonymous” <sip:15619231470@10.0.0.100>
  Privacy: user

- Name Restricted, Number Allowed (independent of “Include Restricted Numbers in From Header” setting)

  From: <sip:12345@10.0.0.100>

- Name Restricted, Number Restricted and “Include Restricted Numbers in From Header” is disabled

  From: <sip:anonymous@anonymous.invalid>

- Name Restricted, Number Restricted and “Include Restricted Numbers in From Header” is enabled

  From: “Anonymous” <sip:15619231470@10.0.0.100>
  Privacy: user

Note: OpenScape Voice is able to provide an OpenScape Voice authentication number within the P-Asserted-Identity (or P-Preferred-Identity) or From header field for calls which are redirected or transferred to the Service Provider (reference "Send authentication number in P-Asserted-Identity header", "Send P-Preferred-Identity rather than P-Asserted-Identity" or "Send authentication number in From header", endpoint attributes in Section 7). The OpenScape Voice "Send authentication number in P-Asserted-Identity header" attribute overrides the OpenScape Voice SIP Endpoint Profile 'Privacy' support setting of 'Basic' or 'Full-Receive for the initial INVITE. The name and/or number restriction is applied according to the authentication number or name identity.

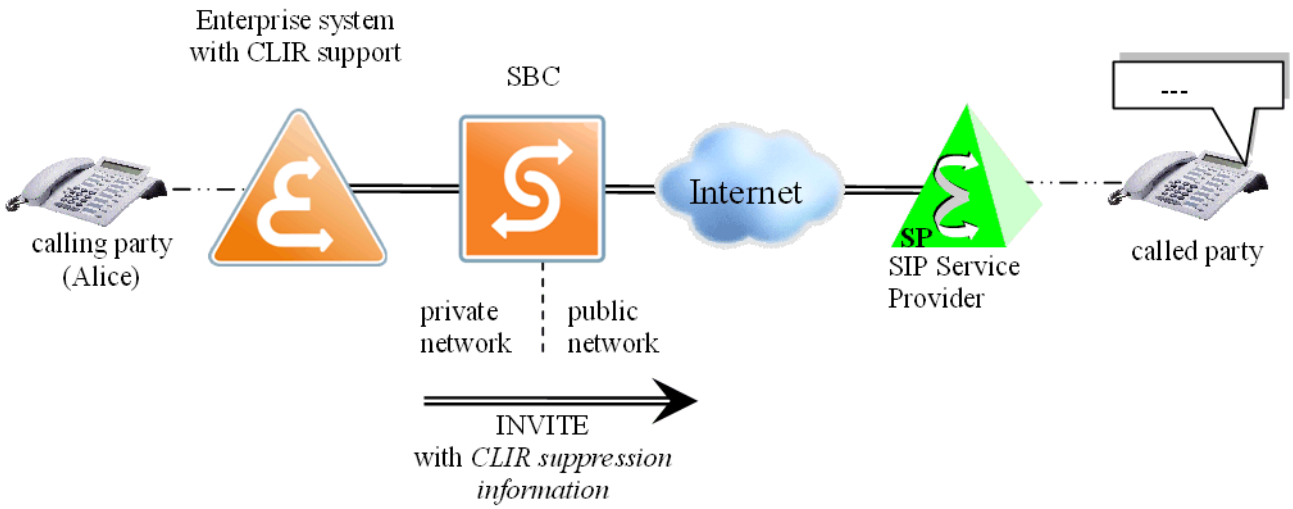


Figure 12 *Example: CLIR Suppression information (outgoing call to Service Provider)*

	Header Field Values for CLIR
P-Asserted-Identity:	“Acme Rockets Sales” <sip:+15617221122@provider.com>
Privacy:	id
From:	“anonymous” <sip:anonymous@anonymous.invalid>

Table 5.2 *Example: CLIR Suppression Information Header Fields (Sending Request from OpenScape Voice (Call to Service Provider)*

Receiving requests and responses from Service Provider:

The Enterprise system should be able to process a received Privacy header field values with id, user, and header as indicated in Section 6.4.23, “Privacy” as well as support for receiving an anonymous From header field (see Section 6.4.17, “From”).

If the OpenScape Voice SIP Endpoint Profile's 'Privacy' support is 'Full' or 'Full-Receive':

The Service Provider may identify to OpenScape Voice that the calling identity should be restricted from being delivered to an interface outside the Enterprise "Trust Domain" by including a Privacy header field with a value of 'user' or 'id' within the SIP INVITE request message.

If the OpenScape Voice SIP Endpoint Profile's 'Privacy' support is 'Basic' or 'Full-Send':

OpenScape Voice processes the From: header field to determine if the calling identity presentation is restricted. The following SIP URIs are indications are that the calling identity presentation is restricted.

- sip:anonymous@anonymous.invalid
- sip:anonymous@[valid-domain]

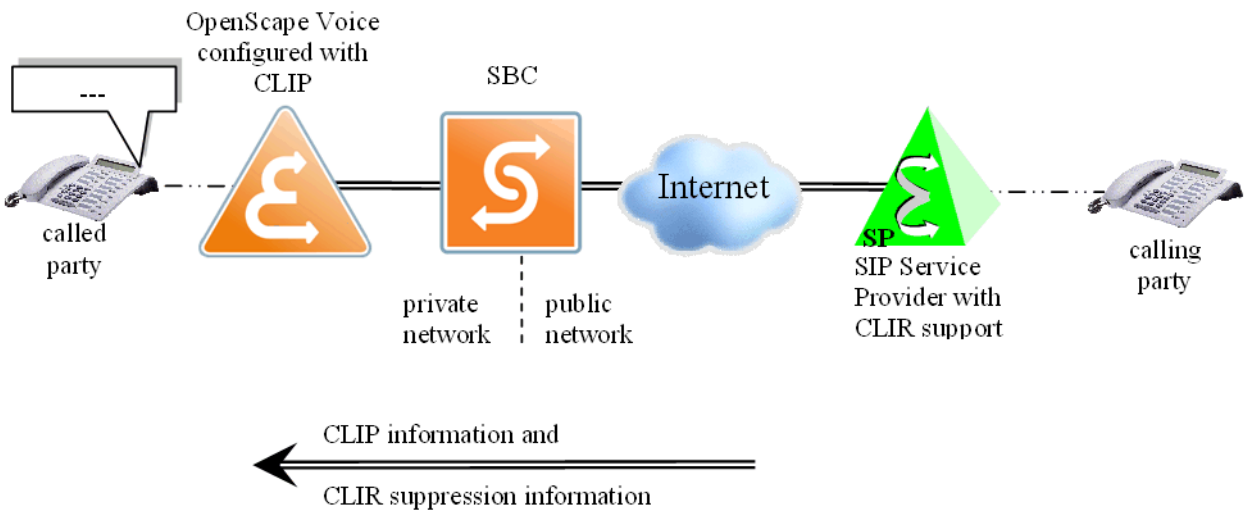


Figure 13 Example: Calling Line Identity Suppression (incoming call from Service Provider)

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may support sending a Privacy header field with the header field values with id, user, and header to the OpenScape Voice system according to RFC3323 [16] and RFC3325 [17].

Receiving requests and responses from OpenScape Voice:

A Service Provider may support receiving a Privacy header field with the header field values with id, user, and header to the OpenScape Voice system according to RFC3323 [16] and RFC3325 [17].

Note: This received identity information should not be conveyed to the called party. A Service Provider may make use of the received identity information for billing and for feature handling.

5.1.3 Connected Line Identification Presentation (COLP)

The COLP (Connected Line Identification Presentation) feature provides the calling party with the identity of the connected party. The identity consists of name (optional) and number of the connected party. To enable the feature, an identity of the called party consisting of a name (optional) and number are delivered by the called party SSNE when the call is answered. Similar features exist to identify the called party during call establishment before answer, however these procedures are not available to callers within the PSTN.

The connected identity information is communicated between the OpenScape Voice and Service Provider based upon the Enterprise "Trust Domain" relationship between the OpenScape Voice and the Service Provider. Reference Section 6.4.21 for a description of the Enterprise "Trust Domain" and its application to the P-Asserted-Identity header field. The delivery of this information requires establishment of an Enterprise "Trust Domain" between OpenScape Voice and the Service Provider. The called party's SSNE inserts identity information within the P-Asserted-Identity header (or P-Preferred-Identity header) field of responses which establish a SIP INVITE dialog . The SSNE for the calling party may use this information in order to display the called or connected party's identity.

OpenScape Voice:

Sending requests and responses to Service Provider:

For OpenScape Voice incoming calls (client with the COLP feature is located within the Service Provider's network), if the OpenScape Voice SIP Endpoint Profile's 'Privacy' support is 'Full' or 'Full-Send':

OpenScape Voice includes a P-Asserted-Identity header field (or P-Preferred-Identity header field) within the 200 OK response to dialog creating INVITE request, independent of the particular OpenScape Voice client that answered the call according to Section 6.4.21.

Note: OpenScape Voice may also send called identity information within a P-Asserted-Identity header field (or P-Preferred-Identity header field) during the establishment of the incoming call:
- 180 Ringing response identifying the alerting party,
or
- 183 Session Progress identifying the called party
Once the call is answered, if the identity of the connected user changes, OpenScape Voice will either:
- Perform a target refresh using the SIP UPDATE method if the SIP Service Provider included indications within the SIP INVITE that the SIP UPDATE method is supported and OpenScape Voice is aware that the Service Provider supports the procedures for performing a target refresh (reference "Supports SIP UPDATE Method for Display Purposes" in Section 7).
- Send a SIP re-INVITE if the SIP UPDATE method is not supported or the Service Provider does not support the target refresh procedures (reference "Supports SIP UPDATE Method for Display Purposes" in Section 7).

For OpenScape Voice incoming calls (client with COLP is at the Service Provider), if the OpenScape Voice SIP Endpoint Profile's 'Privacy' support is 'Basic' or 'Full-Receive':

No requirements.

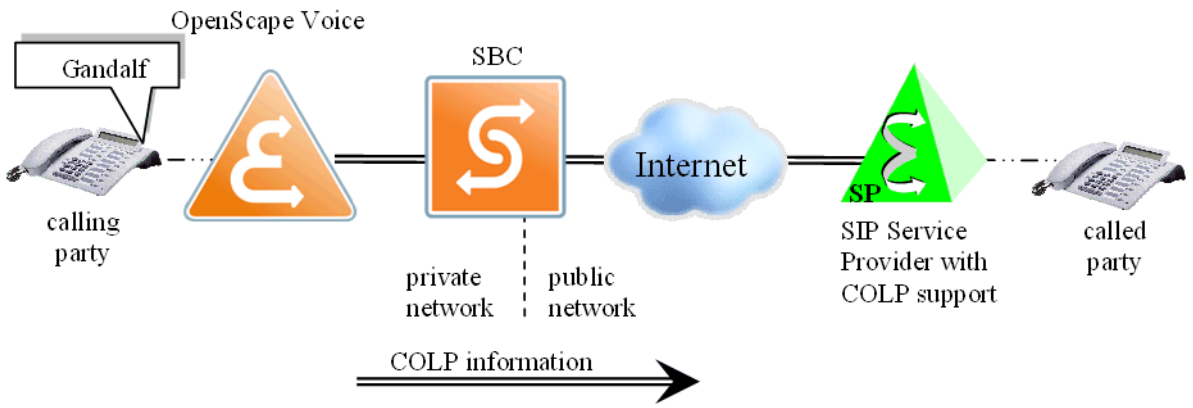


Figure 14 Example: COLP information (incoming call from Service Provider)

	Header Field Values in Responses to Initial *INVITE* Sent to Service Provider (With COLP Feature)
P-Asserted-Identity:	"Gandalf" <sip:+15617221122@another.com>
Privacy:	-
From:	Not relevant.

Table 5.3 Example: COLP information (Incoming Call from Service Provider)

Receiving requests and responses from Service Provider:

For OpenScape Voice outgoing calls to the Service Provider, if the OpenScape Voice SIP Endpoint Profile's 'Privacy' support is 'Full' or 'Full-Receive': OpenScape Voice processes a P-Asserted-Identity header field from the Service Provider only within 200 OK responses to dialog creating INVITE requests as a Called Identity.

Note: Once the call is answered, if the identity of the connected user changes, OpenScape Voice will either:
- Perform a target refresh using the SIP UPDATE method if the INVITE included indications that SIP UPDATE is supported and the Service Provider supports the procedures for performing a target refresh (reference "Supports SIP UPDATE Method for Display Purposes" in Section 7).
- "Sent a SIP reINVITE if SIP UPDATE is not supported or the Service Provider does not support the target refresh procedures (reference "Supports SIP UPDATE Method for Display Purposes" in Section 7).

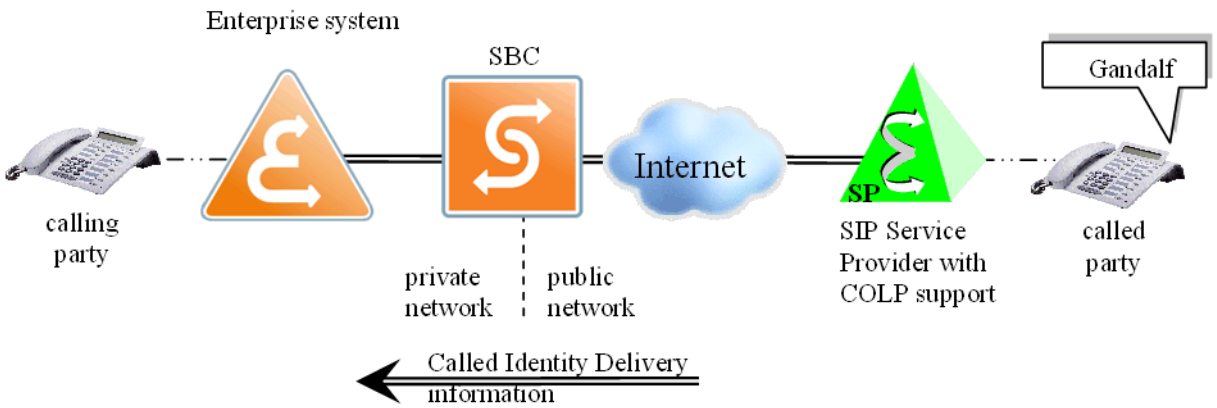


Figure 15 Example: COLP information (Outgoing Call to Service Provider)

For outgoing calls to the Service Provider, if the OpenScape Voice SIP Endpoint Profile's 'Privacy' support is set to 'Basic' or 'Full-Send':

No requirements.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may support sending the identity information of the called party in a P-Asserted-Identity header field in 200 responses to dialog creating INVITE requests.

Receiving requests and responses from OpenScape Voice:

A Service Provider may support processing received identity information of the called party in a P-Asserted-Identity header field in 18x provisional or 200 responses to dialog creating INVITE requests.

5.1.4 Connected Line Identification Restriction (COLR)

The COLR (Connected Line Identification Restriction) prevents the called party from divulging identity information to the calling party.

In order to support COLR, an Enterprise "Trust Domain" must be established between OpenScape Voice and the Service Provider and SNNE should be able to send a *P-Asserted-Identity* header field as well as a *Privacy* header field in responses to another SSNE.

An SSNE providing the COLP or equivalent feature should be able to process a received *P-Asserted-Identity* header field as well as a *Privacy* header field in responses from another SSNE.

OpenScape Voice:

Sending requests and responses to Service Provider:

For OpenScape Voice incoming calls (client with the COLP feature is located within the Service Provider's network), if the OpenScape Voice SIP Endpoint Profile's 'Privacy' support is 'Full' or 'Full-Send':

OpenScape Voice sends a P-Asserted-Identity header field together with a Privacy header field with value of 'id' in 200 OK responses to dialog creating INVITE requests from the Service Provider, if the particular OpenScape Voice client has their Name and or Number Presentation Status active.

Note: OpenScape Voice may send Called identity information during the establishment of the call with 18x provisional responses in addition to the 200 OK response to an initial INVITE.

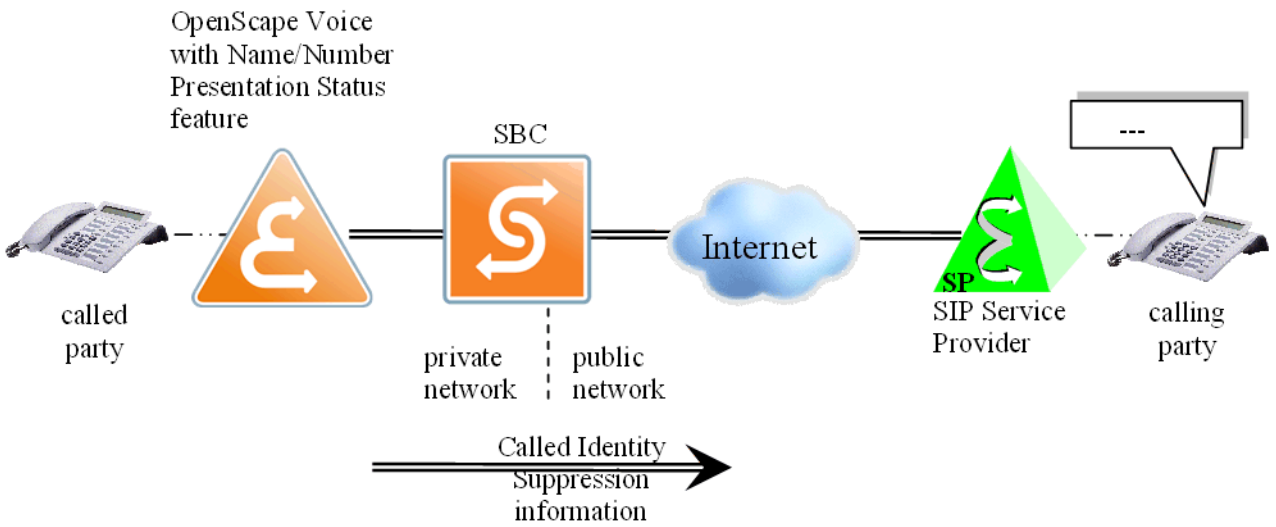


Figure 16 Called Identity Suppression (incoming call from Service Provider)

	Responses to Initial *INVITE* Sent to Service Provider (OSV user with Name/Number Presentation Status feature)
P-Asserted-Identity:	`"Alice" <sip:+49897221122@provider.com>` `Alternatively: not present`
Privacy:	`Id` `Alternatively: not present`
From:	`Not relevant.`

Table 5.4 Example: Called Identitiy Suppression header fields (In Responses) (Incoming Call from Service Provider)

If the OpenScape Voice SIP Endpoint Profile's 'Privacy' support is 'Basic' or 'Full-Receive':

No requirements.

Receiving requests and responses from Service Provider:

If the OpenScape Voice SIP Endpoint Profile's 'Privacy' support is 'Full' or 'Full-Receive':

For outgoing calls, OpenScape Voice processes a received P-Asserted-Identity header field as well as a Privacy header field in 200 responses to dialog creating INVITE requests.

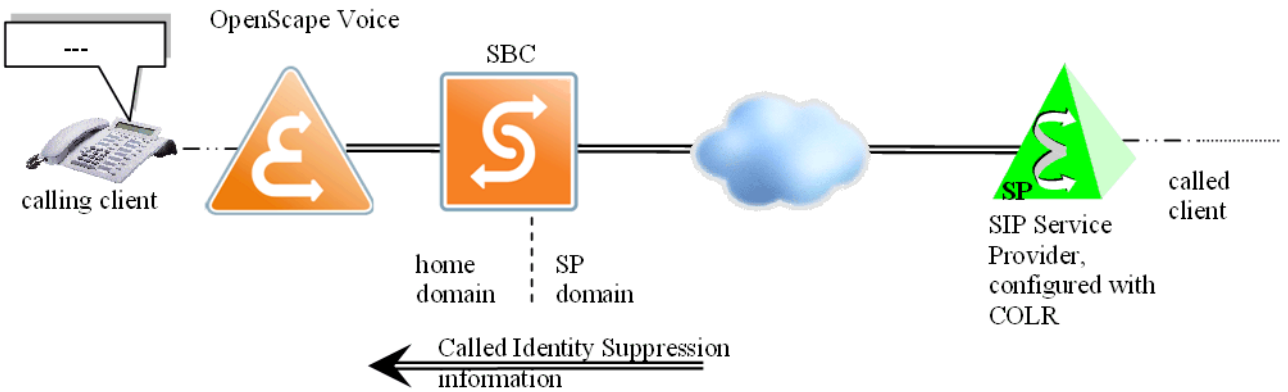


Figure 17 Example: Called Identity Suppression (outgoing call to Service Provider)

	Header Field Values for COLR (In Responses)
P-Asserted-Identity:	`"Gandalf" <sip:+15617221122@another.com>`
Privacy:	`id`
From:	`Not relevant.`

Table 5.5 Example: Called Identity Suppression header fields (In Responses)

If the OpenScape Voice SIP Endpoint Profile's 'Privacy' support is 'Basic' or 'Full-Send':

No requirements

Service Provider:

Sending requests and responses to OpenScape Voice:

Note: This includes sending the identity information of the called party in a *P-Asserted-Identity* header field together with a *Privacy* header field in 200 responses to dialog creating *INVITE* requests, if the particular client at the Service Provider has COLR active.

Receiving requests and responses from OpenScape Voice:

Note: This includes processing received identity information of the called party in a *P-Asserted-Identity* header field together with a *Privacy* header field in 200 responses to dialog creating *INVITE* requests. This identity information

should not be conveyed to the calling party. A Service Provider may make use of the received identity information for reverse charge billing and for feature handling.

5.2 Call Hold, Retrieve, and Alternate

An established call may be put on hold, for example, so that the holding party is able to place another call. Meanwhile the held party may receive Music on Hold (MOH). This music on hold may be provided by either the holding party, by a media server on behalf of the holding party, or locally by the held party.

Alternating is a combination of Call Hold and Call Retrieve. Prerequisite for Alternating is a held call and another (secondary) call that is established after the first call is placed on hold. By executing Alternate, the secondary call is placed on hold and the first call is retrieved. This way, the user can toggle between two parties by placing the other party on hold each time the Alternate feature is invoked.

An SSNE, acting as a B2BUA, should be able to place an established call on hold and to retrieve a held call.

An SSNE, acting as a B2BUA, should be able to place an established call on hold and the held party may also place the holding party on hold.

An SSNE, acting as a B2BUA, may be able to alternate between an active call and a held call.

Figure 18 and Figure 19 show example hold scenarios. The Media Server shown below may be included in the OpenScape Voice server. It is not necessarily a separate Media Server host. It is shown as a separate entity only for sake of generality.

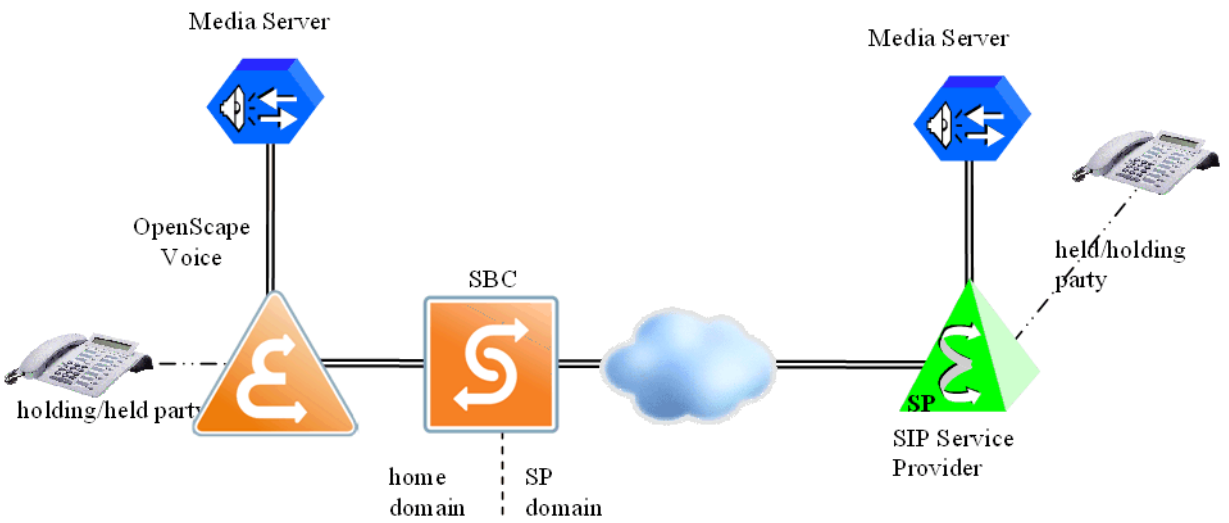


Figure 18 Example: Call Hold between OpenScape Voice and Service Provider

Prerequisites:

The assumption for the following description is that a two-party call has been established. One of the participating parties invokes Call Hold. Some time later the holding party retrieves the held party.

There may be either a Media Server within the OpenScape Voice server, or at the Service Provider, or both. It is out of the scope of this specification how the location of the Media Server(s) is made known to the B2BUAs. This may be done for example via configuration.

Figure 19 shows an example call flow between holding party, held party, and media server. No distinction is made, whether the participating network elements belong to the Service Provider or to the OpenScape Voice holding party and to the held party are not shown.

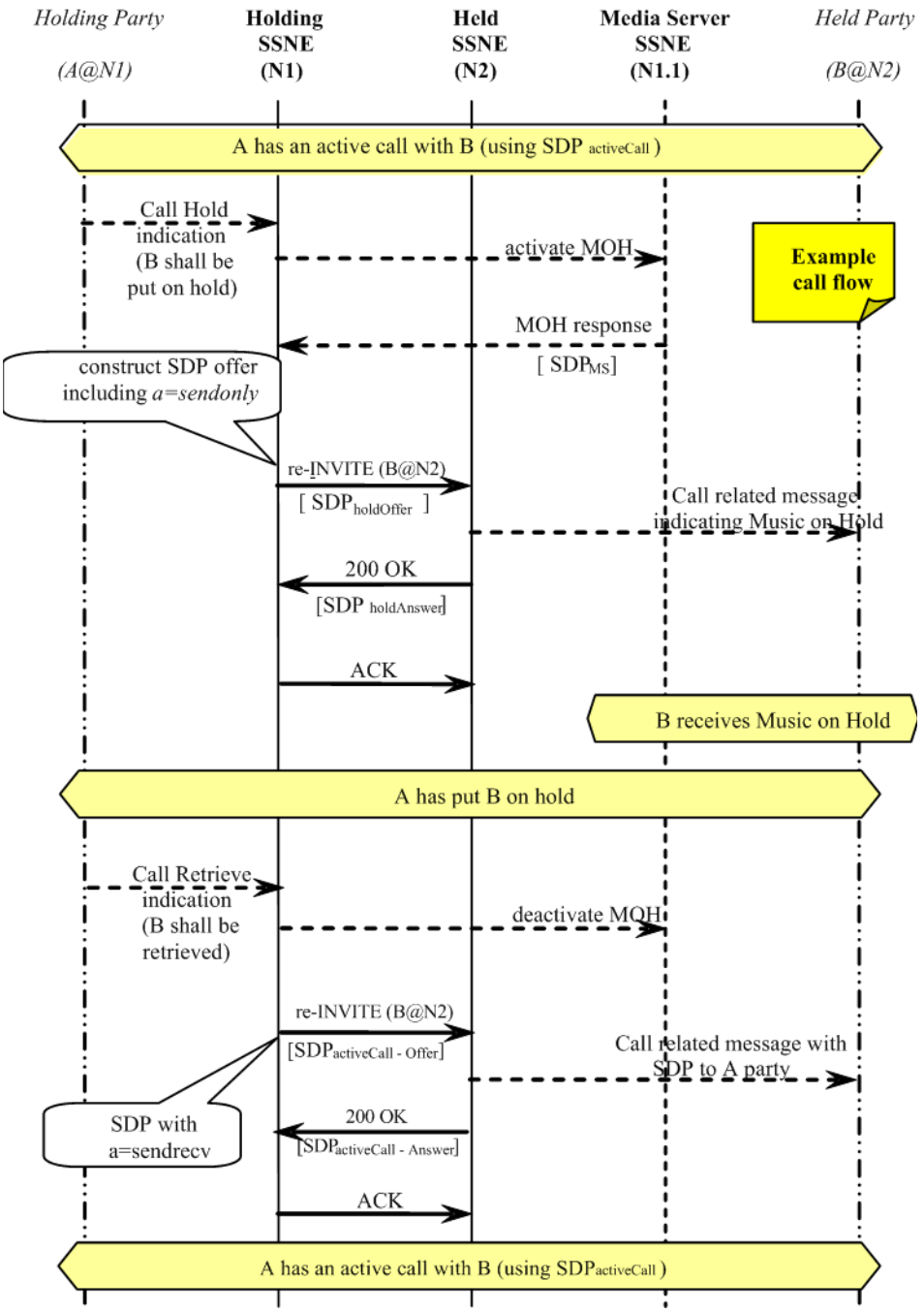


Figure 19 Example: Call Hold and Call Retrieve Call Flows (with Media Server)

Note: Typically, the protocol that is used in order to control a Media Server is MGCP. Some SSNEs hide the MGCP specifics from the participating SIP entities.

OpenScape Voice:

Sending requests and responses to Service Provider:

Note: Call Hold
This includes that on a user request to put an active call on hold, the holding SSNE sends a *re-INVITE* request to the held client with an SDP offer. This SDP offer contains the attribute line a=inactive or a=sendonly. The OpenScape Voice system also supports the deprecated method of setting the IP address in c= line to 0.0.0.0, this option can be enabled/disabled via OpenScape Voice configuration).
An example *re-INVITE* request that is sent to the held party is depicted below.

Request URI:	see Section 6.4.1, “Request URI”, URI of the held client
From header field:	see Section 6.4.17, “From”, *From tag* from the existing dialog
To header field:	see Section 6.4.41, “To”, *To tag* from the existing dialog
Call-ID header field:	Call-ID from the existing dialog
SIP Message Body:	SDP offer with either *a=inactive* or *a=sendonly*

The holding SSNE will place the attribute line *a=inactive* in the SDP offer, when no Music on Hold can be provided from a Media Server.

```
: v=0
  o=<username> <session id> <version> IN IP4 <address>
  s=-
  t=0 0
  c=IN IP4 <address>
  m=audio <port number> RTP/AVP 0
  a=rtpmap:0 PCMU/8000
  a=inactive
```

The holding SSNE will place the attribute line *a=sendonly* in the SDP offer, when Music on Hold can be provided from a Media Server.

```
: v=0
  o=<username> <session id> <version> IN IP4 <address>
  s=-
  t=0 0
  c=IN IP4 <Media Server address>
  m=audio <Media Server port number> RTP/AVP 0
  a=rtpmap:0 PCMU/8000
  a=sendonly
```

Note: Call Retrieve
This includes that on a user request to retrieve a held call, the holding SSNE sends a *re-INVITE* request to the held client with an SDP offer. This SDP offer contains the attribute line *a=sendrecv*.
An example *re-INVITE* request that is sent to the held party is depicted below.

Request URI:	see Section 6.4.1, “Request URI”, URI of the held client
From header field:	see Section 6.4.17, “From”, *From tag* from the existing dialog
To header field:	see Section 6.4.41, “To”, *To tag* from the existing dialog
Call-ID header field:	Call-ID from the existing dialog
SIP Message Body:	SDP offer with *a=sendrecv*

The holding SSNE will place the attribute line *a=sendrecv* in the SDP offer, in order to re-establish the held call.

```
v=0
o=<username> <session id> <version> IN IP4 <address>
s=-
t=0 0
c=IN IP4 <holding client address>
m=audio <holding client port number> RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=sendrecv
```

Receiving requests and responses from Service Provider:

Note: Call Hold
This includes processing a received *re-INVITE* request that is sent from a Service Provider to a client. This *re-INVITE* request contains an SDP offer with the attribute line *a=inactive* or *a=sendonly*, which instructs the client to hold the currently active call. An SSNE should pass any received SDP body unchanged to the destination of the *re-INVITE* request.

Note: Call Retrieve
This includes processing a received *re-INVITE* request that is sent from a Service Provider to a client. This *re-INVITE* request contains an SDP offer with the attribute line *a=sendrecv*, which instructs the client to resume the held call. An SSNE should pass any received SDP body unchanged to the destination of the *re-INVITE* request.

Service Provider:

Sending requests and responses to OpenScape Voice:

Note: Call Hold
This includes that a Service Provider sends a *re-INVITE* request on an established dialog with an SDP body that contains either the attribute line *a=inactive* or *a=sendonly*. The OpenScape Voice system also accepts the deprecated method of setting the IP address in c= line to 0.0.0.0.

Note: Call Retrieve
This includes that a Service Provider sends a *re-INVITE* request on an established dialog with an SDP body that contains the attribute line *a=sendrecv*.

Receiving requests and responses from OpenScape Voice:

Note: Call Hold
This includes that a client to be held behind a Service Provider is able to process a received *re-INVITE* request that is sent to a client with an SDP offer that contains either the media attribute *a=inactive* or *a=sendonly*. A Service Provider may pass received SDP body transparently to the destination of the *re-INVITE* request or it may insert its own Media Server address in the SDP body.

Note: Call Retrieve
This includes that a held client behind a Service Provider is able to process a received *re-INVITE* request that is sent to a held client with an SDP offer that contains a media attribute with *a=sendrecv*. A Service Provider should pass received SDP body transparently to the destination of the *re-INVITE* request.

5.3 Call Transfer

Call transfer is a call rearrangement of an existing call in which one party is replaced with another party. Initially, the transferor is in an active call with the transferee. Then the transferor initiates a call transfer to the transfer target. Finally the transfer target gets connected to the transferee.

Transferor, transferee, and transfer target may be within the Enterprise system or behind the Service Provider.

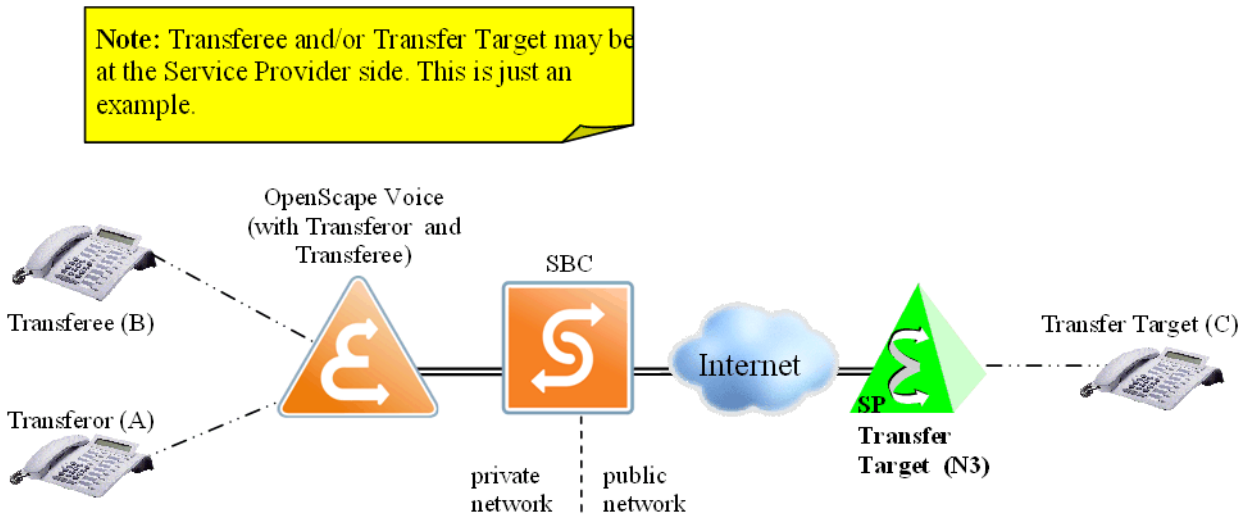


Figure 20 Call Transfer – Between Enterprise and Service Provider

Figure 20 depicts an example call transfer scenario with two call transfer participants within the OpenScape Voice system and one party behind the Service Provider. Any other combination of call transfer participants within the OpenScape Voice system or behind a Service Provider is possible.

Note: There are several mechanisms available in order to achieve call transfer. This document only outlines call transfer using REFER and re-INVITE requests. Other mechanisms include sending INVITE requests with a Replaces header field. These mechanisms are not described in this document and might be added in future versions of this document.

5.3.1 Attended Call Transfer

The assumption for the following description is that a two-party call has been established between the transferor (A) and the transferee (B) on dialog_1. Then the transferee is put on hold. Afterwards, the transferor calls the transfer target (C) on dialog_2. The transferor executes the call transfer after answer so that the held transferee is connected to the transfer target on dialog_3.

Both call legs to the transferor are finally released. The transferee and the transfer target remain connected until one of them hangs up.

- **Transferor behavior**

If Attended Call Transfer is supported, the OpenScape Voice system should be able to perform the role of a transferor by converting a received call transfer indication (for example via SIP REFER request) into a series of *re-INVITE* requests using third party call control techniques as described below.

OpenScape Voice:

Sending requests and responses to Service Provider:

- If transferee is at Service Provider:

  The OpenScape Voice system should support sending a *re-INVITE* request on the existing dialog (dialog_1) with no SDP to the transferee. This *re-INVITE* request SHOULD contain a *P-Asserted-Identity* header field that indicates the transfer target. This allows the transferee to update its phone display with the identity of the transfer target.

  An example *re-INVITE* request that is sent to the transferee (which is behind the Service Provider) is depicted below:

Request URI:	see Section 6.4.1, “Request URI”, contact URI of the transferee
From header field:	see Section 6.4.17, “From”, *From tag* from the existing dialog (dialog_1)
To header field:	see Section 6.4.41, “To”, *To tag* from the existing dialog (dialog_1)
Call-ID header field:	*Call-ID* from the existing dialog between transferor (within the OpenScape Voice system) and transferee (behind the Service Provider) (dialog_1)
P-Asserted-Identity header field:	see Section 6.4.21, “P-Asserted-Identity”, contains the identity of the transfer target
SIP Message Body:	None

- If transfer target is at Service Provider:

  The OpenScape Voice system should support sending a *re-INVITE* request on the existing dialog (dialog_2) with the SDP from the transferee (or from the OpenScape Voice B2BUA if it terminates media) to the transfer target. This *re-INVITE* request SHOULD contain a *P-Asserted-Identity* header field that indicates the transferee as well as a *Referred-By* header field that indicates that a call transfer has been performed by the transferor. This allows the transfer target to update its phone display with the identity of the transferee.

  An example *re-INVITE* request that is sent to the transfer target (which is behind the Service Provider) is depicted below.

Request URI:	see Section 6.4.1, “Request URI”, contact URI of the transfer target
From header field:	see Section 6.4.17, “From”, *From tag* from the existing dialog (dialog_2)
To header field:	see Section 6.4.41, “To”, *To tag* from the existing dialog (dialog_2)
Call-ID header field:	*Call-ID* from the existing dialog between transferor and transfer target (dialog_2)

P-Asserted-Identity header field:	see Section 6.4.21, “P-Asserted-Identity”, contains the identity of the transferee
Referred-By header field:	see Section 6.4.30, “Referred-By”, indicates the transferor, may contain additional session related information (session cookie)
SIP Message Body:	SDP from the transferee

Receiving requests and responses from Service Provider:

The OpenScape Voice system should support *re-INVITE* requests with and without SDP in order to support call transfers which are originated outside the OpenScape Voice system.

Note: OpenScape Voice provides a configuration option to accept a SIP *REFER* request from the Service Provider as a call transfer request (the default operation of OpenScape Voice is to not accept SIP *REFER* requests from a Service Provider). Provisioning at OpenScape Voice is necessary to accept a SIP *REFER* request from a Service Provider.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may send *re-INVITE* requests to the OpenScape Voice system with and without SDP. A Service Provider may send a REFER request to the OpenScape Voice system to initiate a call transfer if the OpenScape Voice system has been configured to accept REFER requests from the Service provider.

Receiving requests and responses from OpenScape Voice:

No requirements.

- **Transfer target behavior**

  The OpenScape Voice system should be able to perform the role of a transfer target as described below:

  OpenScape Voice:

  Sending requests and responses to Service Provider:

  The OpenScape Voice system should respond to received *re-INVITE* requests containing SDP according to RFC3264 [11]. Furthermore, sending a *P-Asserted-Identity* header field in responses may be supported (see Section 6.4.21, “P-Asserted-Identity”) in order to allow updating the transferee client display. Refer to Figure 21 on page 63 for an example call flow.

  Receiving requests and responses from Service Provider:

The OpenScape Voice system should support processing of received *re-INVITE* requests with SDP. Furthermore, it may support a received *Referred-By* header field as well as a received *P-Asserted-Identity* header field in received *re-INVITE* requests.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should be able to respond to received *re-INVITE* requests with SDP.

Receiving requests and responses from OpenScape Voice:

A Service Provider should support processing of received *re-INVITE* requests with SDP.

- **Transferee behavior**

  The OpenScape Voice system should be able to perform the role of a transferee as described below:

  OpenScape Voice:

  Sending requests and responses to Service Provider:

  The OpenScape Voice system should respond to received *re-INVITE* requests without SDP according to RFC3264 [11]. Furthermore, sending a *P-Asserted-Identity* header field in responses may be supported (see Section 6.4.21, “P-Asserted-Identity”) in order to allow updating the transferee client display. Refer to Figure 21 below for an example call flow.

  Receiving requests and responses from Service Provider:

  The OpenScape Voice system should support processing of received *re-INVITE* requests without SDP. Furthermore, it may support a received *P-Asserted-Identity* header field in received *re-INVITE* requests.

  Service Provider:

  Sending requests and responses to OpenScape Voice:

  A Service Provider should be able to respond to received *re-INVITE* requests without SDP.

  Receiving requests and responses from OpenScape Voice:

  A Service Provider should support processing of received *re-INVITE* requests without SDP.

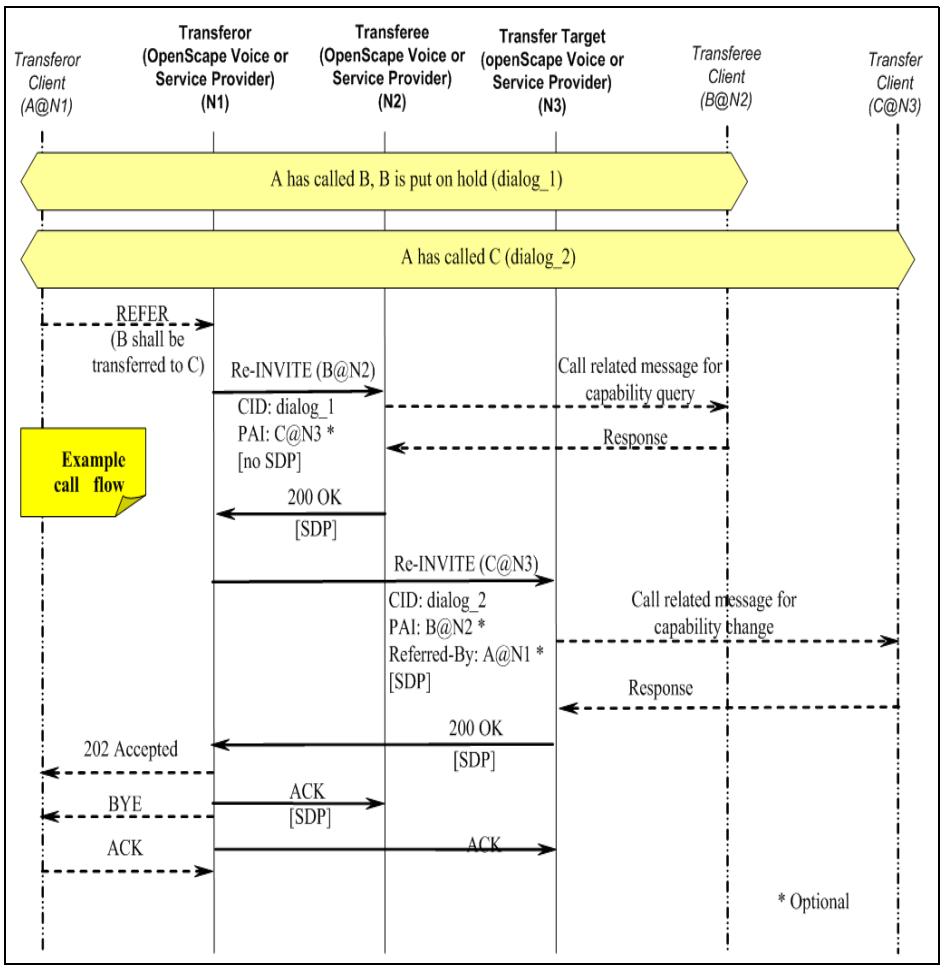


Figure 21 Example Call Flow - Attended Call Transfer

5.3.2 Blind Call Transfer

- **Transferor behavior**

  If Blind Call Transfer is supported, the OpenScape Voice system should be able to perform the role of a transferor by converting a received call transfer indication (for example, SIP REFER request) into a series of *INVITE/re-INVITE* requests using third party call control techniques as described below.

  OpenScape Voice:

  Sending requests and responses to Service Provider:

  - If transfer target is at Service Provider:

The OpenScape Voice system should support sending a new *INVITE* request (thereby creating dialog_2) with no SDP to the transfer target. This *INVITE* request SHOULD contain a *P-Asserted-Identity* header field that indicates the transferee and may contain a *Referred-By* header field that indicates that a call transfer has been performed by the transferor. This allows the transfer target to update its phone display with the identity of the transferee.

An example *INVITE* request that is sent to the transfer target (which is behind the Service Provider) is depicted below:

Request URI:	see Section 6.4.1, “Request URI”, contact URI of the transfer target
From header field:	see Section 6.4.17, “From”, new *From tag*
To header field:	see Section 6.4.41, “To”
Call-ID header field:	*New Call-ID*
P-Asserted-Identity header field:	see Section 6.4.21, “P-Asserted-Identity”, optional, contains the identity of the transferee
Referred-By header field:	see Section 6.4.30, “Referred-By”, optional, indicates the transferor, may contain additional session related information (session cookie)
SIP Message Body:	None (unless the OpenScape Voice B2BUA terminates media, see below)

Note: An exception to this is when the OpenScape Voice B2BUA terminates media streams. In this case the INVITE request from above already contains an SDP offer.

Note: OpenScape Voice is able to provide an OSV Authentication User Identity in place of an external transferee or transferor identity if the transfer target is behind the Service Provider. Additionally, the transferor identity may be sent within a Diversion header field if the Service Provider is unable to accept a Referred-By header field. Reference Section 5.1.1, Section 6.4.14, Section 6.4.17, Section 6.4.21, Section 6.4.32 and "Send Authentication Number in …" attributes in Section 7.

- If transferee is at Service Provider:

  The OpenScape Voice system should support sending a *re-INVITE* request on the existing dialog (dialog_1) with the received SDP (from the transfer target) to the transferee. This *re-INVITE* request SHOULD contain a *P-Asserted-Identity* header field that indicates the transfer target. This allows the transferee to update its phone display with the identity of the transfer target.

An example *re-INVITE* request that is sent to the transferee (which is behind the Service Provider) is depicted below:

Request URI:	see Section 6.4.1, “Request URI”, contact URI of the transferee
From header field:	see Section 6.4.17, “From”, *From tag* from the existing dialog (dialog_1)
To header field:	see Section 6.4.41, “To”, *To tag* from the existing dialog (dialog_1)
Call-ID header field:	*Call-ID* from the existing dialog between transferor (within the OpenScape Voice system) and transferee (behind the Service Provider) (dialog_1)
P-Asserted-Identity header field:	see Section 6.4.21, “P-Asserted-Identity”, contains the identity of the transfer target
SIP Message Body:	SDP from transfer target

Receiving requests and responses from Service Provider:

The OpenScape Voice system should support *re-INVITE* requests with and without SDP in order to support call transfers which are originated outside the OpenScape Voice system.

Note: OpenScape Voice provides a configuration option to accept a SIP *REFER* request from the Service Provider as a call transfer request (the default operation of OpenScape Voice is to not accept SIP *REFER* requests from a Service Provider). Provisioning at OpenScape Voice is necessary to accept a SIP *REFER* request from a Service Provider.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may send *re-INVITE* requests to the OpenScape Voice system with and without SDP. A Service Provider may send a REFER request to the OpenScape Voice system to initiate a call transfer if the OpenScape Voice system has been configured to accept REFER requests from the Service Provider.

Receiving requests and responses from OpenScape Voice:

No requirements.

- **Transfer Target behavior**

  The OpenScape Voice system should be able to perform the role of a transfer target as described below:

  OpenScape Voice:

  Sending requests and responses to Service Provider:

The OpenScape Voice system should respond to received *INVITE* requests containing no SDP according to RFC3264 [11]. Furthermore, sending a *P-Asserted-Identity* header field in responses may be supported (see Section 6.4.21, “P-Asserted-Identity”) in order to allow updating the transferee client display.

Receiving requests and responses from Service Provider:

The OpenScape Voice system should support processing of received *re-INVITE* requests with no SDP. Furthermore, it may support a received *Referred-By* header field (by copying it to corresponding subsequent requests) as well as a received *P-Asserted-Identity* header field in received *INVITE* requests.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should be able to respond to received *INVITE* requests with no SDP.

Receiving requests and responses from OpenScape Voice:

A Service Provider should support processing of received *INVITE* requests with no SDP.

- **Transferee behavior**

  The OpenScape Voice system should be able to perform the role of a transferee as described below:

  OpenScape Voice:

  Sending requests and responses to Service Provider:

  The OpenScape Voice system should respond to received *re-INVITE* requests with SDP according to RFC3264 [11]. Furthermore, sending a *P-Asserted-Identity* header field in responses may be supported (see Section 6.4.21, “P-Asserted-Identity”) in order to allow updating the transferee client display.

  Receiving requests and responses from Service Provider:

  The OpenScape Voice system should support processing of received *re-INVITE* requests with SDP. Furthermore, it may support a received *P-Asserted-Identity* header field in received *re-INVITE* requests.

  Service Provider:

  Sending requests and responses to OpenScape Voice:

  A Service Provider should be able to respond to received *re-INVITE* requests with SDP.

  Receiving requests and responses from OpenScape Voice:

  A Service Provider should support processing of received *re-INVITE* requests with SDP.

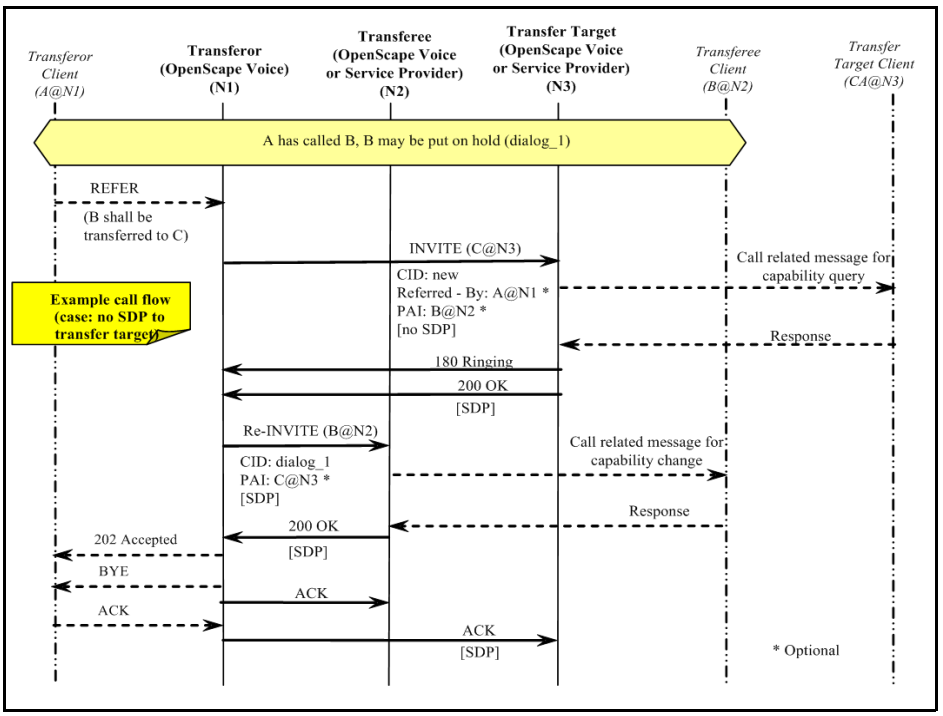


Figure 22 Example Call Flow - Blind Call Transfer

5.3.3 Semi-Attended Call Transfer

The assumption for the following description is that a call has been established between the transferor (A) and the transferee (B) on dialog_1. Then the transferee may be put on hold. Afterwards, the transferor calls the transfer target (C) on dialog_2. As soon as the transfer target starts ringing (that is the second call is not yet fully established), the user A is disconnected. At this point user A doesn't know yet, whether this call will succeed—for example, the offered call is never answered or even rejected. Furthermore, this call might even undergo forking.

- **Transferor behavior**

  If Semi-Attended Call Transfer is supported, the OpenScape Voice system should be able to perform the role of a transferor by converting a received call transfer indication (for example, SIP REFER request) into a series of *INVITE* and *UPDATE* requests using third party call control techniques as described below.

  OpenScape Voice:

  Sending requests and responses to Service Provider:

  - If transferee is at Service Provider:

The OpenScape Voice system should support placing the existing dialog to the transferee on hold (refer to Section 5.2, “Call Hold, Retrieve, and Alternate”, on page 52).

- If transfer target is at Service Provider:

  The OpenScape Voice system should support sending an *INVITE* request, thereby creating an early dialog (dialog_2). This *INVITE* request SHOULD contain a *P-Asserted-Identity* header field that indicates the transferee. This allows the transfer target to update its phone display with the identity of the transferee.

  As soon as the first *180 Ringing* or *182 Queued* response is received, the transferor user may be disconnected, but the dialog1 SHOULD still be maintained. This is necessary in case the call to the transfer target fails. As the call to the transfer target is still in an early state, it may still undergo forking, be rejected or simply not answered.

  The OpenScape Voice system may send an UPDATE request containing a *P-Asserted-Identity* header field with the identity of the transferee to the transfer target in order to allow for display updates and call logging.

Receiving requests and responses from Service Provider:

The OpenScape Voice system should support *INVITE* and *re-INVITE* requests with and without SDP in order to support call transfers which are originated outside the OpenScape Voice system.

Note: OpenScape Voice provides a configuration option to accept a SIP *REFER* request from the Service Provider as a call transfer request (the default operation of OpenScape Voice is to not accept SIP *REFER* requests from a Service Provider). Provisioning at OpenScape Voice is necessary to accept a SIP *REFER* request from a Service Provider.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may send *re-INVITE* requests to the OpenScape Voice system with and without SDP. A Service Provider may send a REFER request to the OpenScape Voice system to initiate a call transfer if the OpenScape Voice system has been configured to accept REFER requests from the Service Provider.

Receiving requests and responses from OpenScape Voice:

No requirements.

- **Transfer target behavior**

  The OpenScape Voice system should be able to perform the role of a transfer target as described in Section 5.3.1, “Attended Call Transfer”.

- **Transferee behavior**

  The OpenScape Voice system should be able to perform the role of a transferee as described in Section 5.3.1, “Attended Call Transfer”.

5.3.4 Call Transfer Handoff

OpenScape Voice provides a 'Transfer Handoff' feature that can be enabled on via an endpoint attribute.

The 'Transfer Handoff' feature allows OpenScape Voice to detect a Transfer request originated by a SIP subscriber. OpenScape Voice would then handover the transfer request to the SIP Service Provider and proxy all relevant/related communication between the SIP Service Provider and the SIP based Transferor for the life of that session.

The 'Transfer Handoff' feature will only be activated if both the OpenScape Voice subscriber and SIP Service Provider endpoint are configured with the 'Transfer Handoff' attribute enabled.

With this mechanism in place, all communication between the SIP subscriber and the SIP Service Provider will be 'proxy'ed' by OpenScape Voice and for Transfer requests; the transfer feature will NOT be active within OpenScape Voice in this case.

5.4 Call Pickup

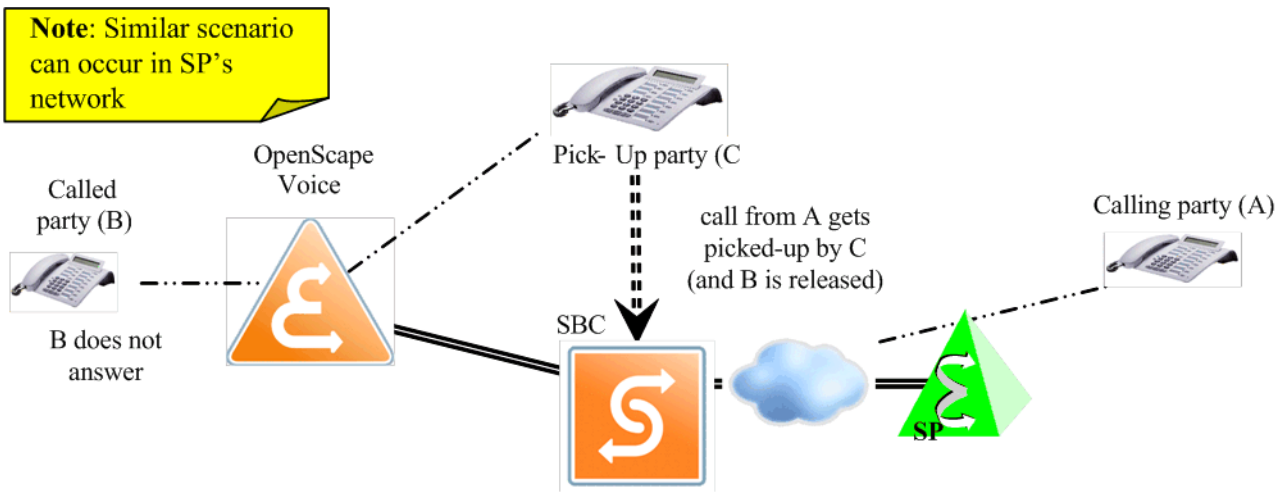


Figure 23 Call Pickup in OpenScape Voice

Note: OpenScape Voice provides several implementations of call pickup based on the capabilities of the endpoints and the method of feature activation. This document only outlines (based on informative descriptions) call pickup using basic call requests and responses within a single dialog for each party. Other mechanisms include sending *INVITE* requests with a *Replaces* header field. These mechanisms are not described in this document as they are not available for pickup of calls from a Service Provider.

Party A calls Party B, who is a subscriber within the OpenScape Voice domain, via the Service Providers network. While party B is being alerted another OpenScape Voice subscriber picks up the call from party C by, for example, dialing a feature access code. Party A is connected to Party C and the session to Party B is terminated.

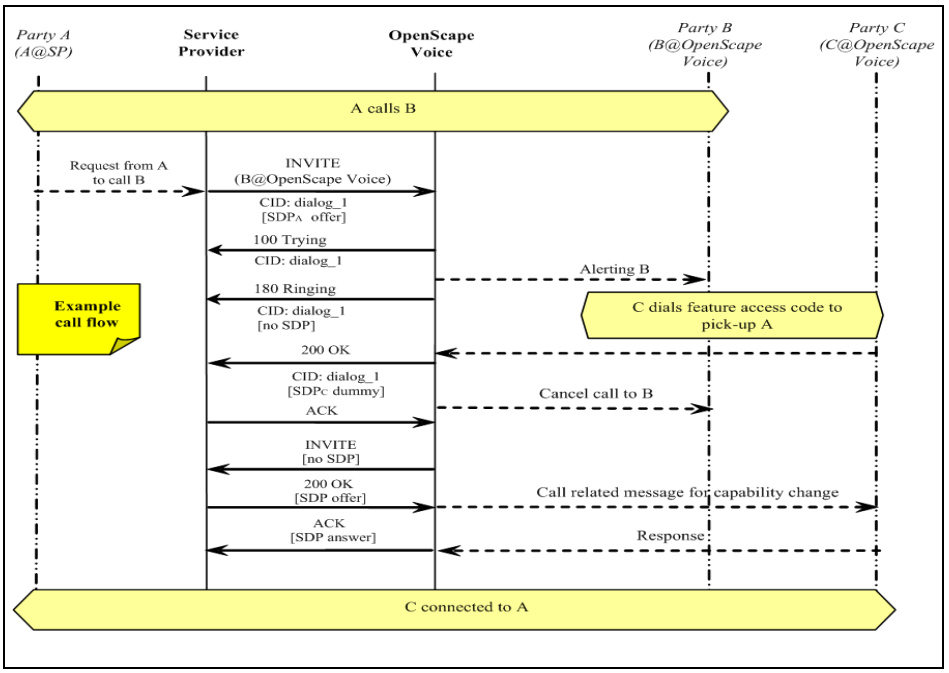


Figure 24 Example Call Flow - Call Pickup

5.5 Call Diversion

Call diversion is the change of the destination of a call. There is a wide range of call diversion types available. Examples are Call Diversion Unconditional, Call Diversion on No Reply, Call Diversion on Busy, Call Diversion on Not Logged-In redirection by One Number Service, and so on.

In this document, only Call Diversion Unconditional is described in detail, although all the redirection scenarios in the previous paragraph will result in a SIP Diversion header being sent to the Service Provider.

OpenScape Voice provides some configuration options to accommodate Service Providers that are unable to receive a SIP Diversion header field. See Section 6.4.14.

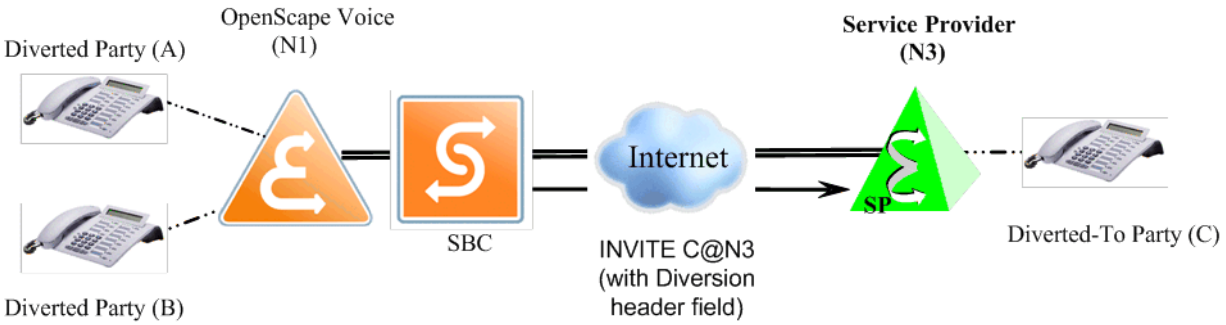


Figure 25 Example: Call Diversion scenario (Diverted-To at Service Provider)

Figure 25 depicts a call diversion scenario where the Diversion destination is at the Service Provider side.

Description:

The calling party A@N1 calls the diverting party B@N2. This call gets diverted to C@N3, for example, due to a received indication from the client or due to a configured call diversion within the Enterprise system, by sending a new *INVITE* request to the diverted-to destination at the Service Provider side. This new *INVITE* request may contain a *Diversion* header field which indicates that this call is a diverted call.

- **Enterprise diverts call to Service Provider:**

  The Enterprise system MUST be able to divert a call to a Service Provider.

  Enterprise:

  Sending requests and responses to Service Provider:

  The Enterprise system MUST be able to send an *INVITE* request which contains a *Diversion* header field with the URI of the diverting party as well as the diversion reason (see Section 6.4.14, “Diversion”). Furthermore, sending a *P-Asserted-Identity* header field with the identity of the calling party SHOULD be supported in order to allow updating the client display. Refer to Figure 26 below for an example call flow.

  An example *INVITE* request that is sent to the diversion destination at the Service Provider is depicted below:

Request URI:	see Section 6.4.1, “Request URI”, URI of the diversion destination
From header field:	see Section 6.4.17, “From”
To header field:	see Section 6.4.41, “To”
Diversion header field:	see Section 6.4.14, “Diversion”, URI of diverting party and the diversion reason, e.g. `Diversion: "Alice" <+49897221122@provider.com>; reason=user-busy`
P-Asserted-Identity header field:	see Section 6.4.21, “P-Asserted-Identity”, optional, contains the identity of the calling party
SIP Message Body:	SDP offer

Note: Currently, OpenScape Voice normally sends a SIP Diversion header field when OpenScape Voice Call Forwarding or ONS deflection services are used. OpenScape Voice allows the identity of the forwarding subscriber to be send in both the From and P-Asserted-Identity (or P-Preferred-Identity) header-fields for SIP Service Providers that do not support the Diversion header-field. Reference "Send redirecting number rather than calling number for redirected calls" and "send authentication number in P-Asserted-Identity header" and "send authentication number in From header" in Section 7.

For external calls which are call forwarded, diverted or blind call transferred to the SIP Service Provider, OpenScape Voice is able to provide an OSV Authentication User Identity in place of the external caller or diverting identity. Additionally, the transferor identity may be sent within a Diversion header field if the Service Provider is unable to accept a Referred-By header field. Reference Section 5.1.1, Section 6.4.14, Section 6.4.17, Section 6.4.21, Section 6.4.32, and "Send Authentication Number in …" attributes in Section 7.

Receiving requests and responses from Service Provider:

No requirements.

Service Provider:

Sending requests and responses to Enterprise:

No requirements.

Receiving requests and responses from Enterprise:

The Service provider SHOULD be able to process a received *INVITE* request containing a *Diversion* header field.

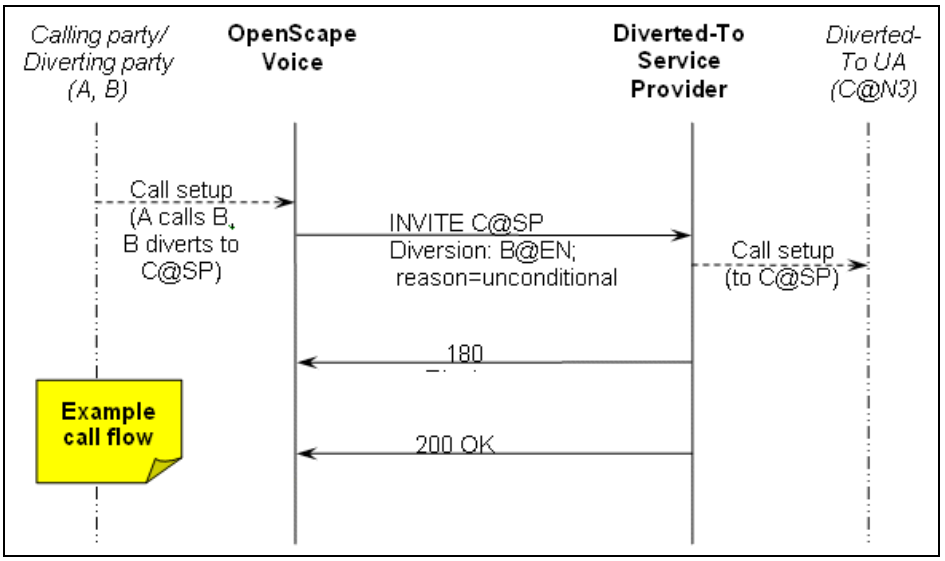


Figure 26 Example Call Flow – Call Diversion

- **Service Provider diverts call to Enterprise:**

  The Service Provider MAY support diverting calls to the Enterprise system or MAY pass diverted calls to the Enterprise system.

Note: Currently no support for actively diverting calls to the Enterprise system using the Diversion header field is available from any Service Provider. Therefore, for the Enterprise system this diverted call is just like a new incoming call.

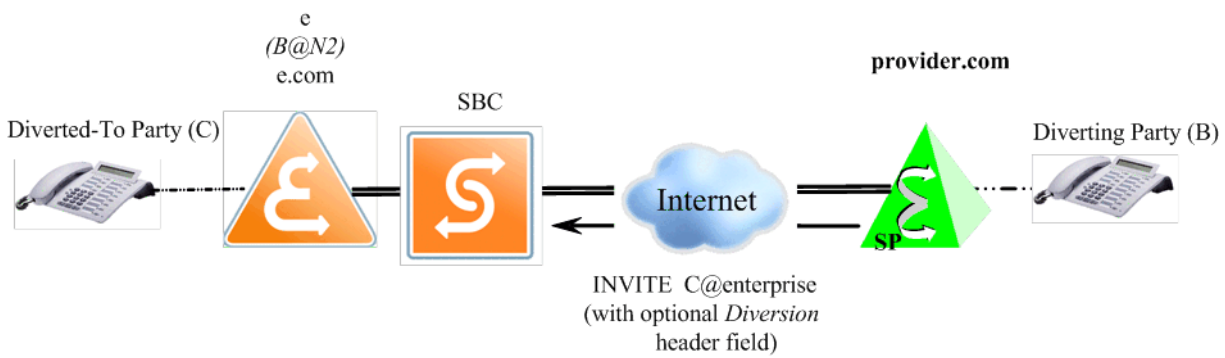


Figure 27 Example Call Diversion Scenario (Diverting Party at Service Provider)

Figure 27 depicts a call diversion scenario where the diverting party destination is at the Service Provider side.

5.5.1 Configuration Options

The following endpoint attributes may be configured for SIP Trunking interfaces:

- Send forwarding number rather than calling number for forwarded calls

  When this option is enabled, OpenScape Voice will replace the calling party number in the SIP From header (and P-Asserted-Identity / P-Preferred-Identity headers) with the diverting party number.

- Do not send Diversion header

  When this option is enabled, OpenScape Voice will not send SIP Diversion headers.

5.6 Message Waiting Indication

Message Waiting Indication (MWI) is an indication that is rendered on the phone, to inform the user that a message is waiting. This indication involves typically a display indication, an acoustic indication, or a lamp on the phone (see Figure 28).

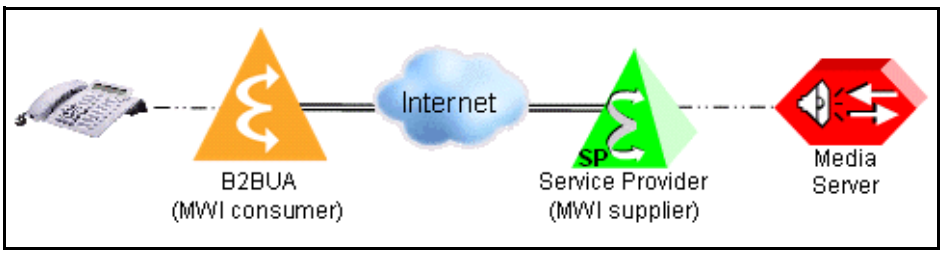


Figure 28 Example: Message Waiting Indication

- **MWI Supplier:**

  An SSNE, acting as a supplier for message waiting notifications, is usually connected to a Media Server and provides notifications to a subscriber about stored voice messages for this subscriber.

  An MWI supplier may be within the OpenScape Voice system or at a Service Provider.

  OpenScape Voice or Service Provider:

  Sending requests and responses:

  If a SSNE is acting as a MWI supplier for subscribers then the SSNE should support the *message-summary* event package (see Section 6.6.1, “Message-Summary”).

  In case the client needs to be notified about a received message (for example when the message count has changed), the SSNE should send a *NOTIFY* request towards the subscriber including a *message-summary*

event including the following header fields: a *Contact* header field with the URI of the Media Server, an *Event* header field with a value of *message-summary*, a *Subscription-State* header field with a value of *active*, and the *Content-Type* header field with a value of *application/simple-message-summary*. Details on the event package can be found in RFC3842 [26].

:

```
NOTIFY sip:1122@10.22.33.44:5060 SIP/2.0
To: sip:1122@10.22.33.44:5060;tag=2222
From: Xpression <sip:3399@10.22.33.44>;tag=1111
Event: message-summary
Subscription-State: active
Content-Type: application/simple-message-summary

Messages-Waiting: yes\n
Voice-Message: 1/0\n
\n
```

Receiving requests and responses from SSNE:

Sending SUBSCRIBE requests for MWI notification is not supported, that is the SSNE will send unsolicited NOTIFY requests as a MWI Supplier.

- **MWI Consumer:**

An SSNE, acting as a consumer for message waiting notifications, is usually connected to a client that provides a display or a lamp in order to indicate to the user that messages have been stored which can be retrieved by the user.

OpenScape Voice or Service Provider:

Sending requests and responses to SSNE:

The MWI Consumer expects the MWI supplier to support the message-summary event package with implicit subscriptions; that is, MWI Consumer does not send SUBSCRIBE requests to the MWI Supplier.

Receiving requests and responses from SSNE:

An SSNE should support processing a received *NOTIFY* request containing a *message-summary* event, if it has an implicit agreement with the MWI supplier that this event is understood.

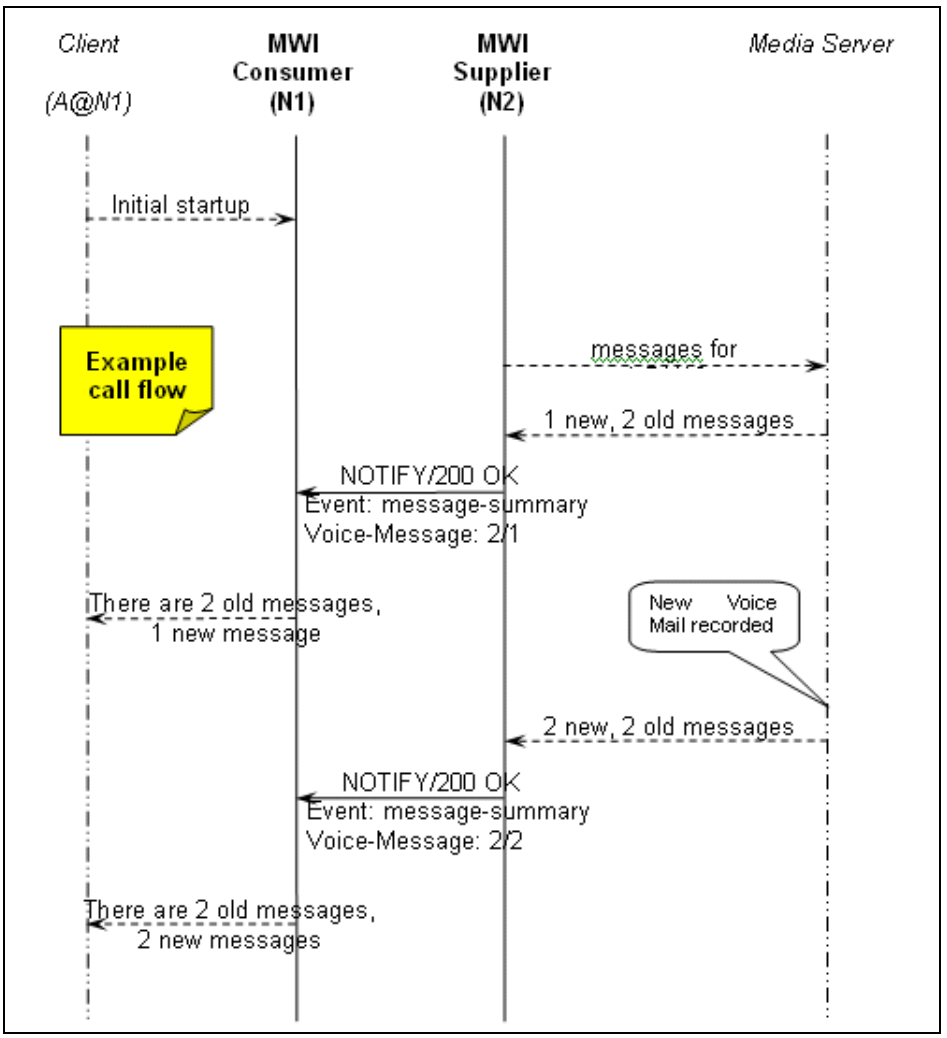


Figure 29 Example Call Flow—Message Waiting Indication

5.7 Call Completion (CCBS/CCNR)

The Call Completion to Busy Subscriber (CCBS) and Call Completion on No Reply (CCNR) features allow a calling subscriber to be automatically connected to a busy or no reply called subscriber when that subscriber becomes available. The OpenScape Voice implementation is based on the ETSI TISPAN recommendation [TISPAN_CCBS] and uses the “ccbs” and “ccnr” event packages. The following example message flows illustrate use of CCBS and CCNR between Call Completion (CC) Servers, in this case OpenScape Voice and a Service Provider.

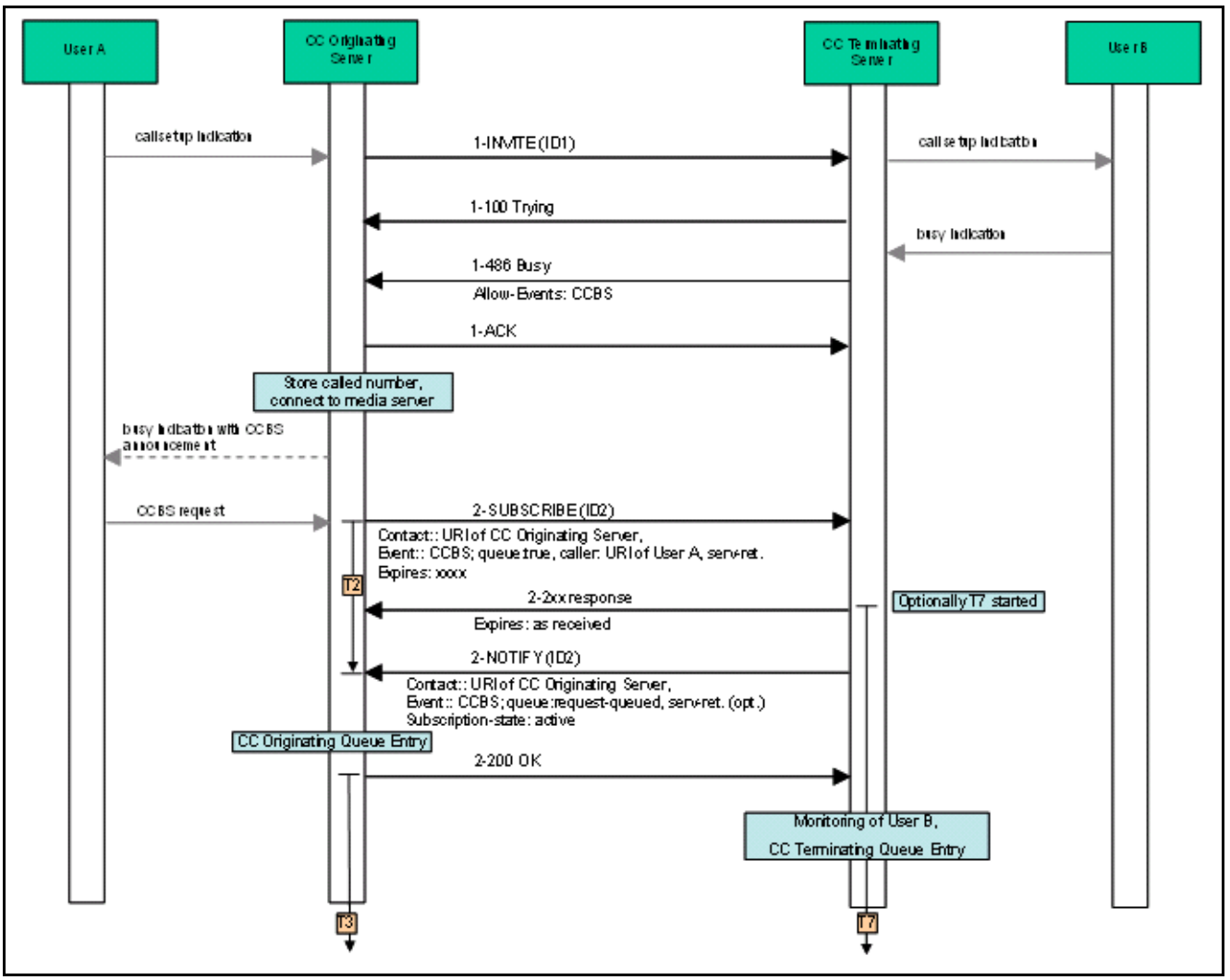


Figure 30 CCBS Available Indication

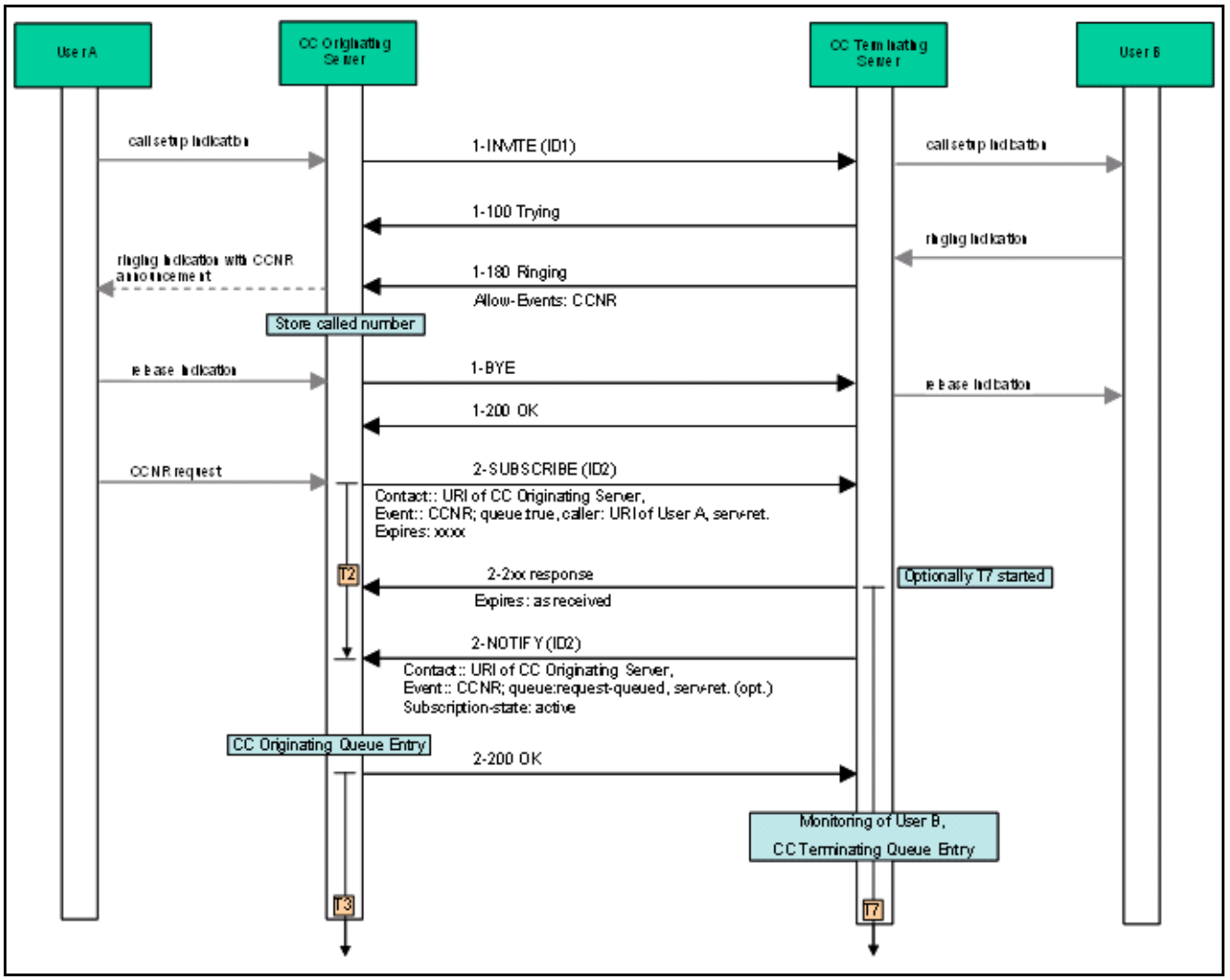


Figure 31 CCNR Available Indication

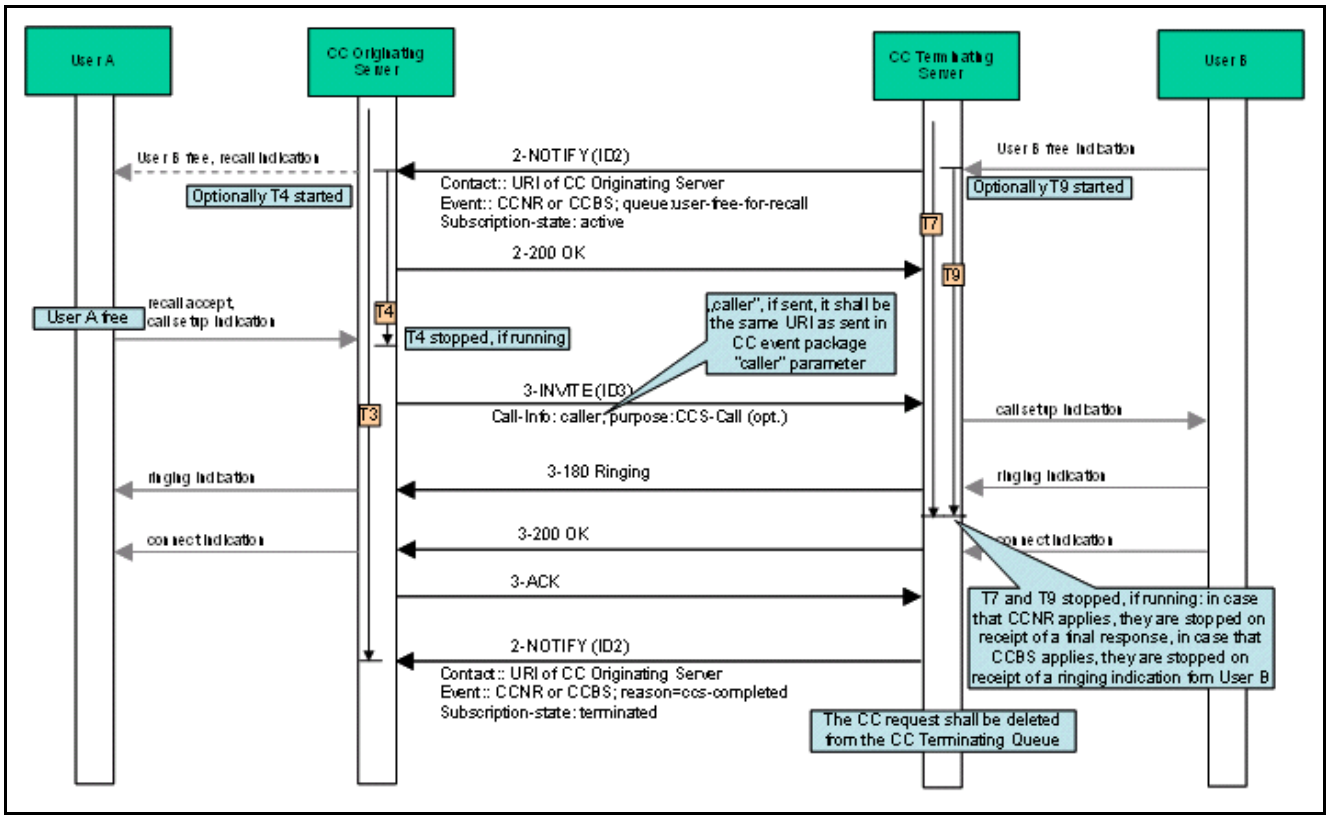


Figure 32 CC Execution, Both, User B and User A are Free

5.8 Third-Party Call Control (3PCC)

The OpenScape Voice solution includes applications that make use of 3PCC procedures to generate and manipulate calls. These 3PCC generated calls may be calls routed via a SIP Service Provider. In order to support 3PCC, the SIP Service Provider must support the procedures described in RFC3725 [40]. In particular, the Service Provider must be able to support at least Flow I of RFC 3725 (in fact, accept a SIP INVITE request that does not include an SDP offer and be able to support the SDP offer/answer exchange via the SIP 200 OK and ACK messages).

5.9 Automatic Collect Call Blocking (ACCB)

OpenScape Voice has the following SIP signaling capabilities that may be used to provide automatic collect call blocking when this feature is supported by the PSTN (e.g. Brasil):

- Sending SIP INFO response with Content-Type: application/broadsoft and a message body containing the text event flashhook. This indicates to the SP that the called subscriber is not allowed to receive collect calls.
- Receiving X-Siemens-Call-Type header field with collect-call token. The SP may use this to indicate to OpenScape Voice that this is a collect call.
- Sending a SIP 403 response with Warning: 399 <OSCV IP address> "Automatic Collect Call Blocking". This indicates that the call was rejected as the called subscriber is not allowed to receive collect calls.

See Section 7 for configuration details.

6 Building Blocks and Protocol Compliance

This section contains *normative* statements about SIP signaling building blocks like SIP methods, header fields, event packages, and so on, which are relevant in trunking scenarios.

This SIP trunking specification does not require new extensions to SIP because the capability to interconnect provider networks is already provided by the SIP RFC3261 [8] and SIP extension RFCs (see Section 1.2.1, “Normative References”). It rather describes procedures and best practice methods using available SIP mechanisms towards the Service Provider.

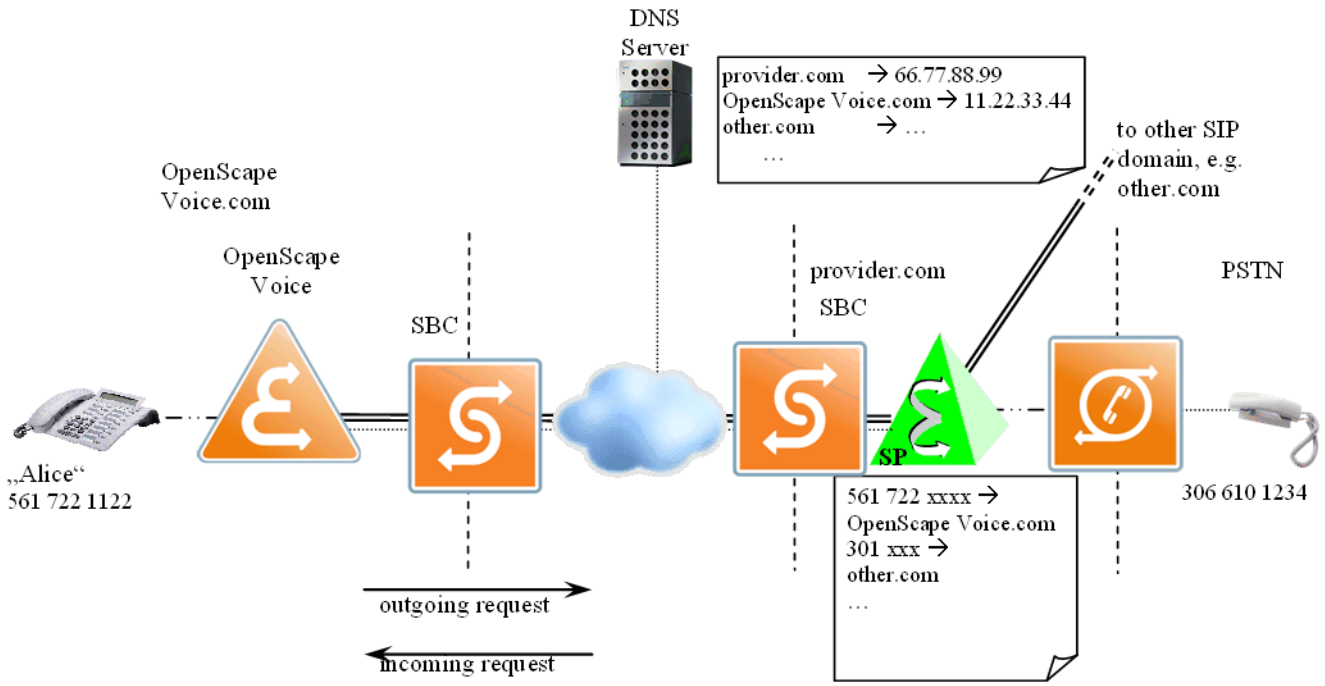


Figure 33 Example OpenScape Voice - Service Provider Configuration

Figure 33 shows an example OpenScape Voice—Service Provider configuration including example telephone numbers for reference purposes only. All examples are informative only and not normative.

The box next to the DNS server illustrates the mapping from domain names to IP addresses with example names and IP addresses that are used throughout this document. The green pyramid represents a Service Provider that serves the domain “provider.com”. The Service Provider handles all telephone numbers starting with 561 722 on behalf of the OpenScape Voice system “OpenScape_Voice.com”. Calls that are directed to other domains—for example, “other.com”—are routed to the respective domain. Calls that are directed to the PSTN are handled by the Service Provider’s TDM gateway—for example, 301 xxxx numbers are normal PSTN numbers.

6.1 SIP Forum Recommendations – OpenScape Voice Compliance Matrix

Table 6.1 describes the OpenScape Voice compliance with the SIP Forum IP PBX/Service Provider Interoperability recommendations (SIP Forum [33]).

Legend

--- section contains no normative statements

n/a not applicable to an IP PBX

C Compliant

PC Partially compliant

NC Not compliant

Clause	Title	Compliant?	Remarks
1	Introduction	---	
2	Conventions and terminology	---	
3	Reference Architecture	---	
4	Definitions	---	
5	Key Assumptions and Limitations of Scope	C	
6	Standards Support	C	
7	Locating SIP Servers	---	
7.1	Enterprise Requirements	PC	See Section 4.3.1, “Locating SIP Servers”
7.2	Service Provider Requirements	n/a	
8	Signaling Security	PC	See Section 4.3.6, “Signaling and Payload Encryption (SPE)”
9	Firewall and NAT Traversal	C	See Section 4.3.4, “NAT Traversal”
10	Authentication and Accounting	---	
10.1	Authentication of the Enterprise by the Service Provider	PC	See clauses 10.1.1 and 10.1.2 below
10.1.1	Option 1: Authentication using TLS Credentials	PC	See Section 4.3.6, “Signaling and Payload Encryption (SPE)”
10.1.2	Option 2: Digest Access Authentication	C	See Section 4.3.3, “Authentication”
10.2	Authentication of the Service Provider by the Enterprise	PC	See Section 4.3.6, “Signaling and Payload Encryption (SPE)”
11	Enterprise PSTN Identities	C	See Section 5.1, “Number Identification”
12	Enterprise URI Formatting and Addressing Rules	C	
12.1	‘From:’ Field	PC	See clauses 12.1.1 and 12.1.2 below
12.1.1	Option 1: Utilizing the ‘From:’ and ‘P-Asserted-Identity:’ SIP Header Fields	PC	See Section 5.1, “Number Identification”
12.1.2	Option 2: Utilizing the ‘From:’ SIP Header Field only	PC	See Section 5.1, “Number Identification”

Table 6.1 SIP Forum Compliance Matrix (Sheet 1 of 2)

Clause	Title	Compliant?	Remarks
12.2	'To:' Field – PSTN Destinations	C	See Section 6.2.1, "URI Schemas"
12.2.1	Option 1: SIP URI	C	See Section 6.2.1, "URI Schemas"
12.2.2	Option 2: tel: URL	C	See Section 6.2.1, "URI Schemas"
12.3	'To:' Field – Emergency Services Destinations	NC	*phone-context* parameter not supported
12.4	'To:' Field -- Other Destinations	C	
12.5	Request-URI	C	
13	Service Provider URI Formatting and Addressing Rules	n/a	
13.1	'From:' Field	n/a	
13.2	'To:' Field	n/a	
13.3	Request-URI	n/a	
14	Quality of Service Considerations	C	
15	Media Attributes and Minimum Requirements	---	
15.1	Media Capability Negotiation	C	OpenScape Voice does not originate or terminate media, but in all other respects it is compliant with this clause.
15.2	Codec Support and Media Transport	C	OpenScape Voice does not originate or terminate media, but in all other respects it is compliant with this clause.
15.3	Transport of DTMF Tones	C	OpenScape Voice does not originate or terminate media, but in all other respects it is compliant with this clause.
15.4	Echo Cancellation	C	OpenScape Voice does not originate or terminate media, but in all other respects it is compliant with this clause.
15.5	Fax and Modem Calls	C	OpenScape Voice does not originate or terminate media, but in all other respects it is compliant with this clause.
16	PSTN Interactions	---	
16.1	Call Progress Tones	C	OpenScape Voice does not originate or terminate media, but in all other respects it is compliant with this clause.
16.2	Early Media	C	OpenScape Voice does not originate or terminate media, but in all other respects it is compliant with this clause.
17	References	---	
18	Contributors and Contact Information	---	
19	Full Copyright Statement	---	

Table 6.1 SIP Forum Compliance Matrix (Sheet 2 of 2)

6.2 General

6.2.1 URI Schemas

The following URI schemas should be supported:

- SIP (for incoming and outgoing requests)

The following URI schemas may be supported:

- SIPS (for incoming and outgoing requests)
- TEL (for incoming and outgoing requests, see RFC3966 [29])

Size limitations:

- Display Name - max. 39 characters
- User Part - max. 128 characters
- Host Part - IPV4 address or FQDN
- URI Parameters - max. 128 characters

6.3 SIP Methods

The following section describes SIP methods from RFC3261 [8] and SIP extension RFCs (see Section 1.2.1, “Normative References”) that are used on the OpenScape Voice – Service Provider interface. Individual header fields are only mentioned where specific considerations in the context of the SIP method apply. Other fields in those SIP methods—for example Call-ID, CSeq, or Content-Length—are skipped.

6.3.1 ACK

OpenScape Voice and the Service Provider should support sending and receiving the *ACK* request according to RFC3261 [8].

6.3.2 BYE

OpenScape Voice and the Service Provider should support sending and receiving the *BYE* request according to RFC3261 [8].

6.3.3 CANCEL

OpenScape Voice and the Service Provider should support sending and receiving the *CANCEL* request according to RFC3261 [8].

6.3.4 INFO

The OpenScape Voice may transparently pass SIP INFO requests.

The OpenScape Voice may send SIP INFO requests that include the following SIP header fields and message body to indicate in a SIP 200 OK response in order to indicate that the called party is not allowed to receive reverse charge (aka collect) calls.

```
Content-Type: application/broadsoft; version=1.0
Content-Length: 17
event flashhook
```

OpenScape Voice shall support receiving a SIP INFO message with a Remote-Party-ID header field containing a delayed Calling Name.

6.3.5 INVITE

The *INVITE* method is defined in RFC3261 [8].

OpenScape Voice:

Sending requests and responses to Service Provider:

An SSNE should support sending new *INVITE* and *re-INVITE* requests according to RFC3261 [8] to the Service Provider as follows:

Request URI:	see Section 6.4.1, “Request URI”, URI of the destination
From header field:	see Section 6.4.17, “From”
To header field:	see Section 6.4.41, “To”, with or without the *to tag*, depending on whether it is a dialog creating *INVITE* request or whether a *re-INVITE* request within the context of an existing dialog.
P-Asserted-Identity header field:	see Section 6.4.21, “P-Asserted-Identity”, optional
Privacy header field:	see Section 6.4.23, “Privacy”, optional

SIP Message Body:	Without SIP message body, with SDP offer, or with any other SIP message body. SDP offer/answer processing should be according to RFC3264 [11]. In case any other SIP message body is provided, special handling applies according to the content type.

OpenScape Voice supports sending those requests with and without SDP body.

Receiving requests and responses from Service Provider:

OpenScape Voice supports processing an *INVITE* request according to RFC3261 [8].

OpenScape Voice shall support receiving a *Remote-Party-ID* header field in an initial *INVITE* request, to use the identity provided as the calling party's identity. Refer to Section 6.4.31, "Remote-Party-ID".

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending an *INVITE* request to the OpenScape Voice system.

Receiving requests and responses from OpenScape Voice:

A Service Provider should support receiving an *INVITE* request from the OpenScape Voice system.

Note: This includes a reINVITE with unchanged SDP used as a session refresh, for example SIP Session Timing (RFC4028 [30]).

6.3.6 NOTIFY

The *NOTIFY* method is defined in RFC3265 [12].

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending a *NOTIFY* request according to RFC3265 [12] in order to support higher-level features which require sending *NOTIFY* requests to a Service Provider.

Note: NOTIFY requests should only be sent if there is an active subscription for a particular event package. However, in some cases the sender and receiver of a NOTIFY request may have an implicit knowledge about this event package, and may exchange NOTIFY requests even without explicit subscription. Those NOTIFY requests must only be sent if the sender of the request can assume that the receiver is able to process it.

OpenScape Voice should support sending the *NOTIFY* request to the Service Provider as follows:

Request URI:	see Section 6.4.1, “Request URI”, URI of the destination
From header field:	see Section 6.4.17, “From”
To header field:	see Section 6.4.41, “To”, with or without the *to tag*, depending on whether a dialog has been created
Event header field:	see Section 6.4.15, “Event”, event packages are described in Section 6.6, “SIP Event Packages”
Subscription-State header field:	see Section 6.4.39, “Subscription-State”
Content-Type header field:	see Section 6.4.12, “Content-Type”
Contact header field:	see Section 6.4.9, “Contact”, optional
SIP Message Body:	SIP message body is according to the signaled event. See Section 6.6, “SIP Event Packages”.

Receiving requests and responses from Service Provider:

The OpenScape Voice server, acting as a B2BUA, is able to process a received *NOTIFY* request for a supported event package.

Note: OpenScape Voice may receive a NOTIFY request because it has subscribed to it, or it may receive this request due to an implicit subscription, that is without prior SUBSCRIBE request. This implicit subscription may have been created by configuration or some other means.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending a *NOTIFY* request to the OpenScape Voice system, if it has to provide support for features that require sending *NOTIFY* requests.

A Service Provider should support transmitting a received *NOTIFY* request to the OpenScape Voice system, if received from another domain.

Receiving requests and responses from OpenScape Voice:

A Service Provider may be able to process a received *NOTIFY* request for a supported event package.

A Service Provider should support transmitting a received *NOTIFY* request from the OpenScape Voice system to the destination.

6.3.7 OPTIONS

The *OPTIONS* method is defined in RFC3261 [8].

When receiving an OPTIONS request, OpenScape Voice treats this as just a 'ping' and sends the response without checking headers such as 'Supported', etc. SIP Session Timing procedures [section 4.3.5] can also be used as a session keep alive mechanism.

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending the *OPTIONS* request to the Service Provider, according to RFC3261 [8], as part of an auditing mechanism. When a target endpoint fails to respond to an INVITE request, the endpoint is put into an operational blocked state while SIP OPTIONS requests are sent by OpenScape Voice. As soon as the target endpoint responds to the OPTIONS request, it is put back into an operational state and OpenScape Voice discontinues the audit for the endpoint (i.e., OPTIONS requests are not sent under normal operating conditions).

Note: Support for OPTIONS within OpenScape Voice is limited to sending OPTIONS requests as an audit mechanism or as a heartbeat mechanism between a network elements. OpenScape Voice does not currently use OPTIONS to discover UA capabilities.

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process *OPTIONS* requests received from the Service Provider, according to RFC3261 [8].

Note: OpenScape Voice may not provide capability information in the response to the OPTIONS request. OpenScape Voice is limited to responding to OPTIONS requests as an audit mechanism or as a heartbeat mechanism between a network elements.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may support sending an *OPTIONS* request to OpenScape Voice.

Receiving requests and responses from OpenScape Voice:

A Service Provider should respond to *OPTIONS* requests received from OpenScape Voice.

6.3.8 PRACK

Reliable Provisional Responses, including the *PRACK* method, are defined in RFC3262 [9]. A PRACK request is used to confirm that a reliable provisional response was received.

OpenScape Voice provides limited support of PRACK on a half-call basis, and only if enabled on a per-SIP network-network interface basis (refer to Endpoint Attribute *PRACK Enabled* in Chapter 7, “Configuration options for SIP Service Provider interoperability”). It does not provide end-to-end PRACK behavior - OpenScape Voice as a B2BUA supports all requirements for PRACK as a SIP UAC or a SIP UAS, i.e., PRACK interworking preformed on each interface independently.

Note: This approach deviates from RFC3262 [9] goal of ensuring reliable provisional response handling end-to-end, however it does satisfy many of the OpenScape Voice application scenarios.

It is highly recommended that a reliable transport type (TCP or TLS) is used between OpenScape Voice and the Service Provider (as SIP requests/responses may exceed the maximum size that can safely be sent via UDP). When a reliable transport type is used, all responses are reliable and therefore use of PRACK is unnecessary.

6.3.9 REFER

The *REFER* request indicates that the receiver should contact another client using the contact information from the *Refer-To* header field.

The *REFER* method is defined in RFC3515 [19].

OpenScape Voice:

Sending requests and responses to Service Provider:

So far there is no requirement for OpenScape Voice, acting as a B2BUA, to send a *REFER* request to a Service Provider, because OpenScape Voice translates a *REFER* request from a subscriber corresponding *INVITE* requests. See Section 5.3, “Call Transfer”, where the *REFER* request is used for Call Transfer.

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a received *REFER* request if OpenScape Voice is configured to accept Call Transfer (*REFER*) requests from the Service Provider for Blind Call Transfer scenarios. For other call transfer scenarios which involve a call establishment by the call transferor to the transfer-target, the REFER request Refer-To header field

(reference section 6.4.30) should include a Replaces header field (reference section 6.4.33) parameter. If the Replaces header field parameter references a dialog unknown to OpenScape Voice, the REFER will be rejected with a 420 Bad Extension response. For this type of call transfer to work, all call transfer call legs must be handled by OpenScape Voice to support these call transfer scenarios.

If OpenScape Voice is not configured to accept *REFER* requests from the Service Provider, OpenScape Voice should reject a received *REFER* request from a Service Provider with a *403 "Forbidden"* response

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may send a *REFER* request to OpenScape Voice if OpenScape Voice is configured to accept *REFER* requests from the Service Provider; otherwise, a Service Provider should not send *REFER* requests to the OpenScape Voice system.

Receiving requests and responses from OpenScape Voice:

There is no requirement for a Service Provider, acting as a B2BUA, to process received *REFER* requests. The SP may reject a received *REFER* request from OpenScape Voice with a *403 “Forbidden”* response.

6.3.10 REGISTER

The *REGISTER* method is defined in RFC3261 [8].

OpenScape Voice:

Sending requests and responses to Service Provider:

The OpenScape Voice server should not send *REGISTER* requests to the Service Provider.

Refer to Section 4.3.2, “Registration” for registration concepts.

Receiving requests and responses from Service Provider:

There is no requirement for OpenScape Voice, acting as a B2BUA, to process received *REGISTER* requests from a Service Provider. OpenScape Voice may reject a received *REGISTER* request from an SP with a *403 “Forbidden”* response.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should not send *REGISTER* requests to OpenScape Voice.

Receiving requests and responses from OpenScape Voice:

There is no requirement for a Service Provider, acting as a B2BUA, to process received *REGISTER* requests from OpenScape Voice. The SP may reject a received *REGISTER* request from OpenScape Voice with a *403 "Forbidden"* response.

Refer to Section 4.3.2, "Registration" for registration concepts.

6.3.11 SUBSCRIBE

The *SUBSCRIBE* method is defined in RFC3265 [12].

OpenScape Voice:

Sending requests and responses to Service Provider:

The OpenScape Voice system supports sending the *SUBSCRIBE* request according to RFC3265 [12] in order to support higher-level features, if at least one event package is implemented that requires subscription.

The OpenScape Voice system supports sending the *SUBSCRIBE* request to the Service Provider as follows:

Request URI:	see Section 6.4.1, "Request URI", URI of the destination
From header field:	see Section 6.4.17, "From"
To header field:	see Section 6.4.41, "To", with or without the *to tag*, depending on whether a dialog has been created
Event header field:	see Section 6.4.15, "Event", event packages are described in Section 6.6, "SIP Event Packages"
Expires header field:	see Section 6.4.16, "Expires"
Accept header field:	see Section 6.4.2, "Accept", indicates the supported SIP message body type
Allow header field:	see Section 6.4.4, "Allow", must be *NOTIFY*
Contact header field:	see Section 6.4.9, "Contact", optional
SIP Message Body:	SIP message body is according to the signaled event. See Section 6.6, "SIP Event Packages".

Receiving requests and responses from Service Provider:

The OpenScape Voice system is able to process a received *SUBSCRIBE* request for a particular event package, if it has implemented this event package.

If the OpenScape Voice system does not understand the received event package, it will reject the *SUBSCRIBE* request with a *489 "Bad Event"* response.

If the OpenScape Voice system is not configured to accept the received event package, it will reject the *SUBSCRIBE* request with a *403 "Forbidden"* response.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending a *SUBSCRIBE* request to the OpenScape Voice system, if it has to provide support for features that require subscriptions.

Receiving requests and responses from OpenScape Voice:

A SP should process a received *SUBSCRIBE* request for a supported event package.

6.3.12 UPDATE

The *UPDATE* method is defined in RFC3311 [15]. OpenScape Voice does not support use of the UPDATE method (except in the special case of sending an UPDATE request to update phone displays after e.g. a call transfer as described in Section 5.3.3, "Semi-Attended Call Transfer", or when receiving a delayed Calling Name as described in Section 5.1.1, "Calling Line Identification Presentation (CLIP)").

Once the call is answered (i.e. once the SIP dialog is established), the identity of either the calling party or the connected party MAY change. This happens, for instance, if the call is transferred.

In these scenarios, the updated identity SHALL be sent in an UPDATE request provided that:

- The Service Provider has indicated support for the method in the '*Allow*' header field of the INVITE request or response message
- An Enterprise "Trust Domain" relationship has been established which allows sending a *P-Asserted-Identity* header field (or *P-Preferred-identity*)
- The Service Provider supports the display update procedures as reflected in the OpenScape SIP Endpoint attribute "*Supports SIP UPDATE Method for Display Purposes*"

6.3.13 MESSAGE

The *MESSAGE* method is defined in RFC3428.

OpenScape Voice does not support the *MESSAGE* method on NNI interfaces and will not include the *MESSAGE* method in Allow: headers.

A Service Provider should not send *MESSAGE* requests to OpenScape Voice.

6.3.14 Unknown Methods

An SSNE, acting as a proxy, should be able to pass through unknown SIP methods transparently to the next SSNE, unless the *Proxy-Require* header field is specified. In this case, the proxy should reject the request according to RFC3261 [8].

Note: Use of OpenScape Voice as a SIP Proxy is outside the scope of this document. OpenScape Voice normally operates as a B2BUA and will therefore reject unknown SIP methods.

6.4 Header Fields

Details on the header field in this document can be found in RFC3261 [8] and related RFCs. These are referenced when appropriate.

Many header fields contain URIs. Refer to Section 6.2.1, “URI Schemas” for allowed URI formats.

Usage of a header field is according to the corresponding RFC that defines it, unless otherwise specified in this document or any other referenced document. Header fields that are defined in other RFCs and that are used by OpenScape Voice are included in this document.

The following statement applies to all subsequent sections, unless otherwise stated:

An SSNE, acting as a proxy, should support passing a received request or response containing a header field listed below transparently to another SSNE, unless otherwise stated.

Note: Use of OpenScape Voice as a SIP Proxy is outside the scope of this document. OpenScape Voice normally operates as a B2BUA and will therefore not necessarily pass header fields transparently.

6.4.1 Request URI

OpenScape Voice:

Sending requests and responses to Service Provider:

When sending a request outside the context of an existing dialog, OpenScape Voice will include in the host part of the *request URI* an FQDN that the Service Provider can accept or the IP address of the Service Provider.

Note: Some Service Providers may accept only their own FQDN. Some Service Providers might require their own IP address.

If OpenScape Voice is aware (via OpenScape Voice provisioning) that the domain concerned requires a particular format (for example an international E.164 number) in the userinfo part of the *request URI*, it will supply the correct format.

The URI parameter *user=phone* will be included in sip: (or sips:) *request URI's* and the userinfo part will be a telephone number (with any separators removed).

OpenScape Voice may also be provisioned to send tel: URI's (in Global Number Format or in Local Number Format), the phone-context parameter for tel: URI's is not currently supported.

Note: Some requests—for example, SUBSCRIBE requests—do not necessarily require a telephone number in the userinfo part. In those requests, the userinfo part may, for example, contain access codes, alphanumeric characters such as used in email addresses, or a number that points to a presence service

---

✎: `INVITE sip:+15613387654@OpenScape_Voice.com;user=phone SIP/2.0`

✎: `INVITE sip:5613387654@OpenScape_Voice.com;user=phone SIP/2.0`

✎: `INVITE tel:+15613387654 SIP/2.0`

✎: `INVITE tel:5613387654 SIP/2.0`

Receiving requests and responses from Service Provider:

OpenScape Voice is able to accept either an FQDN or its IP address in the host part of the request URI of a request outside the context of an existing dialog.

OpenScape Voice assumes that the request is for its own domain and takes no further action on the host part of the URI.

OpenScape Voice can be provisioned to accept the URI userinfo part as:

- sip/sips URI's in GNF
- sip/sips URI's in local number format
- tel URI's in GNF

- tel URI's in local number format

If there is no "user=phone" parameter included with a sip/sips URI then OpenScape Voice will still treat the userinfo part as an E.164 phone number if only the characters 0-9, A-F,8,# are present.

✎: `INVITE sip:+15617221122@OpenScape_Voice.com;user=phone SIP/2.0`

✎: `INVITE sip:5617221122@OpenScape_Voice.com;user=phone SIP/2.0`

✎: `INVITE tel:+15617221122 SIP/2.0`

✎: `INVITE tel:5617221122 SIP/2.0`

Service Provider:

Sending requests and responses to OpenScape Voice:

For a request outside the context of an existing dialog, the Service Provider must send in the host part of the request URI either an FQDN for which OpenScape Voice is authoritative or the IP address of the OpenScape Voice server. As part of a local policy agreement with OpenScape Voice, the Service Provider may send the userinfo part in any of the formats described above in the OpenScape Voice sections. The default mode of operation is sip URI with userinfo as E.164 number in GNF and user=phone parameter included.

Receiving requests and responses from OpenScape Voice:

When receiving a request outside the context of an existing dialog, if the host part of the request URI identifies a domain for which the Service Provider is authoritative, the Service Provider should be able to accept E.164 numbers in GNF as the userinfo part. As part of a local policy agreement with OpenScape Voice, the Service Provider may receive the userinfo part in any of the formats described above in the OpenScape Voice sections. If the Service Provider is not authoritative for that domain but is prepared to route the request towards that domain, it must accept any value in the userinfo part.

6.4.2 Accept

For details refer to RFC3261 [8].

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice will send *INVITE*, and *SUBSCRIBE* requests containing an *Accept* header field according to RFC3261 [8], if support for SIP message body formats other than *application/sdp* is available. Furthermore, it sends the *Accept* header field in *2xx* responses as well as in *415 "Unsupported Media Type"* responses.

: `Accept: application/dialog-info+xml`

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a received request containing an *Accept* header field. This means, that the OpenScape Voice will send only SIP bodies of the type *application/sdp* or the types that were indicated in a received *Accept* header field.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending requests containing an *Accept* header field according to RFC3261 [8], if support for SIP message body formats other than *application/sdp* is available. Furthermore, it should support sending the *Accept* header field in *2xx* responses as well as in *415 "Unsupported Media Type"* responses.

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to process a received *INVITE*, and *SUBSCRIBE* request containing an *Accept* header field according to RFC3261 [8]. Furthermore, it should be able to process the *Accept* header field in *2xx* responses as well as in *415 "Unsupported Media Type"* responses.

6.4.3 Alert-Info

For details refer to RFC3261 [8].

The Alert-Info header is only used in SIP signaling to OpenScape Voice subscribers, it is never sent to or received from a Service Provider.

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice will never send an *Alert-Info* header field to a Service Provider.

Receiving requests and responses from Service Provider:

OpenScape Voice will not pass on an *Alert-Info* header received from a Service provider.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should not send an *Alert-Info* header to OpenScape Voice.

Receiving requests and responses from OpenScape Voice:

A Service Provider should not receive an *Alert-Info* header from OpenScape Voice, if one is received it may be ignored.

6.4.4 Allow

For details refer to RFC3261 [8].

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending *INVITE* requests containing an *Allow* header field according to RFC3261 [8].

: `Allow: INVITE,ACK,CANCEL,BYE,REFER,NOTIFY`

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a received *INVITE* request containing an *Allow* header field.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending *INVITE* requests containing an *Allow* header field according to RFC3261 [8].

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to accept a received *INVITE* request containing an *Allow* header field according to RFC3261 [8].

6.4.5 Allow-Events

The *Allow-Events* header field indicates the event packages supported by the sender of the request or response.

For details refer to RFC3265 [12].

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending an *Allow-Events* header field according to RFC3265 [12] in 486 and 180 SIP responses as part of the CCBS/CCNR feature.

: `Allow-Events: ccbs`
: `Allow-Events: ccnr`

Supported events are described in Section 6.6, “SIP Event Packages”

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process received 486 and 180 SIP responses containing an *Allow-Events* header field.

Note: This header field is useful in determining what event packages are implemented and hence, what features are supported.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may support sending SIP 486 and 180 responses containing an *Allow-Events* header field according to RFC3265 [12], if at least one event package is supported.

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to accept received SIP 486 and 180 responses containing an *Allow-Events* header field according to RFC3265 [12].

6.4.6 Authentication-Info

OpenScape Voice:

OpenScape Voice can support sending and receiving an *Authentication-Info* header field in *2xx* responses according to RFC3261 [8].

```
: Authentication-Info:
nextnonce="e77511be36e123e063196c019b6f9582"
```

Service Provider:

A Service Provider should support sending and receiving an *Authentication-Info* header field in *2xx* responses according to RFC3261 [8].

6.4.7 Authorization

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice can support sending the *Authorization* header field in requests to the Service Provider. See Section 4.3.3, “Authentication” for authentication procedures.

```
: Authorization: Digest
            response="64b20e760fca0650fd276704f3735675",
            username="alice",realm="siemens.com",
            nonce="e77511be36e123e063196c019b6f9582"
```

Receiving requests and responses from a Service Provider:

OpenScape Voice is able to process a received *Authorization* header field in requests from OpenScape Voice, if digest authentication between Service Provider and OpenScape Voice is requested.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service provider should support sending the *Authorization* header field in requests to the OpenScape Voice. See Section 4.3.3, “Authentication” for authentication procedures.

```
Authorization: Digest
            response="64b20e760fca0650fd276704f3735675",
            username="bob",realm="provider.com",
            nonce="e77511be36e123e063196c019b6f9583"
```

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to process a received *Authorization* header field in requests from OpenScape Voice, if digest authentication between Service Provider and OpenScape Voice is requested.

6.4.8 Call-ID

OpenScape Voice as well as a Service Provider should support sending and receiving a *Call-ID* header field according to RFC3261 [8].

6.4.9 Contact

The *Contact* header field provides a URI that can be used to contact the client for subsequent requests.

Refer to RFC3261 [8] for details.

Note: OpenScape Voice imposes the following size limits on components of a contact URI:
userinfo – 32 characters (will increase to 128 in a future release)
hostport – 64 characters
uri-parameters – 128 characters

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice will insert its own *Contact* header field in requests and responses to the Service Provider. OpenScape Voice will insert a URI in the *Contact* header field that is routeable to OpenScape Voice.

: `Contact: <sip:+15617221122@siemens.com;transport=udp;maddr=10.77.38.102>`

Receiving requests and responses from Service Provider:

OpenScape Voice will store the received *Contact* URI, as it is a B2BUA.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending the *Contact* header field in requests and responses to the OpenScape Voice system. A Service Provider should insert a URI in the *Contact* header field that is routeable to the Service Provider.

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to process a received *Contact* header field in requests and responses from the OpenScape Voice system.

6.4.10 Content-Disposition

Refer to RFC3261 [8] for details.

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice will not send a Content-Disposition header to the Service provider. The Service Provider should assume the default disposition for the message body, that is *session; handling=required*.

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a received *Content-Disposition* header field according to RFC3261 [8]. The header field value *session* will be processed. Other header field values may be processed.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may support sending the *Content-Disposition* header field to the OpenScape Voice system. If the Service Provider does not send the *Content-Disposition* header field, OpenScape Voice will assume the default disposition for the message body— that is, *session; handling=required*.

Receiving requests and responses from OpenScape Voice:

OpenScape Voice will not send a *Content-Disposition* header field to the Service Provider. The Service Provider should assume the default disposition for the message body, that is *session; handling=required*.

6.4.11 Content-Length

OpenScape Voice as well as a Service Provider should support sending and receiving a *Content-Length* header field according to RFC3261 [8].

```
Content-Type: application/sdp
c=IN IP4 10.152.231.252
m=audio 29100 RTP/AVP 8
a=rtpmap:8 PCMA/8000
```

6.4.12 Content-Type

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending the *Content-Type* header field in requests to the Service Provider, according to RFC3261 [8].

```
Content-Type: application/sdp
```

Receiving requests and responses from Service Provider:

OpenScape Voice should be able to process a received *Content-Type* header field.

If a received *Content-Type* header field value is not supported or not understood, the request will be rejected with a *415 "Unsupported Media Type"* response.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending the *Content-Type* header field in requests and responses to OpenScape Voice.

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to process a received *Content-Type* header field in requests and responses from OpenScape Voice, unless the request has to be routed to another destination.

6.4.13 CSeq

OpenScape Voice as well as a Service Provider should support sending and receiving a *CSeq* header field according to RFC3261 [8].

```
CSeq: 1234 INVITE
```

6.4.14 Diversion

The *Diversion* header field is an optional header field that indicates re-direction of a call. The definition of this header can be found in reference [Diversion].

The *Diversion* header field value contains the URI of the re-directing party. The *reason* parameter indicates the re-direction reason, for example call diversion unconditional, call diversion on busy, or call diversion on no answer.

Note: Usage of the *Diversion* header field is particularly useful in conjunction with the *P-Asserted-Identity* header field. Both header fields provide the complete set of information in case of call diversion, that is URI and name of calling and diverting parties.

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending *INVITE* requests including up to two *Diversion* header fields in case of call diversion with the top-most Diversion header field identifying the last redirecting party. If the diverting party's identity presentation is allowed, the *Diversion* header field contains the party's external identity URI, a privacy parameter with value="off", and one of the following reason parameters: *user-busy, no-answer, unconditional*, or *deflection*. The *Diversion* header field sent by OpenScape Voice may include the counter and limit parameters.

If the diverting party's identity presentation is restricted then the content of the diversion header field is dependent on the OpenScape Voice Enterprise "Trust Domain" relationship with the Service Provider (reference section 7).

– If the OpenScape Endpoint Profile's '*Privacy*' support is '*Full*' or '*Full-Send*', the Diversion header URI is populated with the diverting party's identity along with a privacy parameter with value of "full".

– If the OpenScape Endpoint Profile's '*Privacy*' support is '*Basic*' or '*Full-Receive*', the diversion header URI is anonymized.

A *Diversion* header field may contain the external display name of the diverting client.

: `Diversion: "Alice" <sip:+15617221122@siemens.com>; reason="no-answer";counter=5`

: `Diversion: "Bob" <sip:+15617221122@siemens.com>; reason="unconditional"`

OpenScape Voice is able to send an authentication number within the *Diversion* header field which may not necessarily identity the call forwarding or diverting party. The authentication number can also be included in the *From*, *P-Asserted-Identity* header fields, or any combination. Another benefit

is the ability to send the authentication number in alternative header fields whenever the Service Provider is unable to accept or process the header field normally used to convey an identity of a feature user, i.e., in this case the *Diversion* header field (reference "*Send authentication number in xxx header*" and "*Do not send Diversion header*" endpoint attributes in section 7).

The URI parameter user=phone will be included in the sip: URI except when the URI is anonymized. The insertion of the user=phone parameter may be disabled (reference section 7 Rtp parameters).

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a received *INVITE* request with up to two *Diversion* header fields. OpenScape Voice is able to recognize the following reason parameters: *user-busy*, *no-answer*, or *unconditional*. If the reason parameter is not present or the value is other than *user-busy*, *no-answer*, *unconditional, or deflection*, then OpenScape Voice will default to a *reason* parameter value of *unknown* (which will be processed by OpenScape Voice in the same way as a value of *unconditional*).

If the OpenScape Endpoint Profile's '*Privacy*' support is '*Full*' or '*Full-Receive*', the Service Provider may identify that a diverting party's identity presentation must be restricted by including a privacy parameter with a value of "full" if both name and number are restricted, "name" if only the name is restricted, or "uri" if only the number is restricted.

✎: `Diversion: "Gandalf" <sip:+1567306610@provider.com>; reason="no-answer"`

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may support sending *INVITE* requests that contain a *Diversion* header field.

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to process a received *INVITE* request that contains a *Diversion* header field.

6.4.15 Event

Refer to RFC3265 [12] for details. Supported events are described in Section 6.6, "SIP Event Packages"

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending the *Event* header field in *SUBSCRIBE* and in *NOTIFY* requests, if at least one event package is implemented. See Section 6.6, "SIP Event Packages".

✎: `Event: ccbs`

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process an *Event* header field in a received *SUBSCRIBE* or *NOTIFY* request, if the specified event package is implemented. See Section 6.6, “SIP Event Packages”.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending the *Event* header field in *SUBSCRIBE* and *NOTIFY* messages to OpenScape Voice, if at least one event package is implemented.

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to process a received *Event* header field in *SUBSCRIBE* or *NOTIFY* messages from OpenScape Voice, if at least one event package is implemented.

6.4.16 Expires

The *Expires* header field in *SUBSCRIBE* requests specifies how long the subscription is valid.

Refer to RFC3261 [8] and RFC3265 [12] for details.

Note: For ccbs/ccnr events the Expires header is populated with the maximum value that can be held in the *Expires* Header (or a value greater than the maximum time that the ccbs/ccnr application allows a request is remain active). Since the ccbs/ccnr application timers control the length of the activation duration, it is not necessary to perform the re-subscription function.

OpenScape Voice:

Sending requests and responses to Service Provider:

If at least one event package is implemented, OpenScape Voice supports sending the *Expires* header field in *SUBSCRIBE* requests as well as in *2xx* responses to *SUBSCRIBE* requests. See Section 6.6, “SIP Event Packages”.

✎: `Expires: 3600`

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process an *Expires* header field in a received *SUBSCRIBE* request and in a received *2xx* response from a *SUBSCRIBE* request.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending the *Expires* header field in *SUBSCRIBE* requests and in *2xx* responses to a *SUSBSCRIBE* request, if at least one event package is implemented.

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to process a received *Expires* header field in *SUBSCRIBE* requests from OpenScape Voice, if the corresponding event package is supported.

6.4.17 From

The *From* header field, the *P-Asserted-Identity* header field (Section 6.4.21, “P-Asserted-Identity”) and the *Privacy* header field (see Section 6.4.23, “Privacy”) are important for conveying identities between OpenScape Voice, Service Providers, and the PSTN.

Note: The *From* header field should be populated with the desired public identity of the calling party. If a *P-Asserted-Identity* (or *P-Preferred-Identity*) header field (see section 6.4.21) is present in the SIP request it identifies that an Enterprise "Trust Domain" relationship exists. In this case, the *P-Asserted-Identity* should contain the private identity of the calling party. In case privacy is requested, the *From* header field may be anonymized or may identify a public identity depending on the setting of the OpenScape Voice SIP Endpoint attribute (reference "*Include Restricted Numbers in From Header*", section 7). Regardless of the setting, the *P-Asserted-Identity* header field should contain the public identity, and the *Privacy* header field (see section 6.4.23) should be present with a value reflecting the desired identity privacy.
The URI parameter user=phone will be included in the sip: URI except when the URI is anonymized. The insertion of the user=phone parameter may be disabled (reference section 7 Rtp parameters).

6.4.17.1 From header field procedures byOpenScape Voice:

Sending requests to Service Provider:

The *From* header field URI is constructed according to the rules specified in Section 6.4.1, “Request URI”.

The *From* header field may also contain the display name of the calling party, if available.

✎: From: “Acme Rocket Sales” <sip:+15617221122@enterprise.com>;tag=1923837465

✎: From: “Acme Rocket Sales” <sip:+15617221122@123.12.23.45>;tag=1923837465

Note: OpenScape Voicee provides the following endpoint attribute to force the OpenScape Voice domain name (rather than an IP address) to be sent as the host part of the From header URI:

Send domain name in From and P-Preferred-Identity headers

There are two exceptions to this: if the Service Provider requires some other format or if privacy applies (see Section 5.1.2, “Calling Line Identification Restriction (CLIR)”).

If privacy was requested (either from the user or because the client or the system is configured to establish private calls), the *From* header will be anonymized, as described in RFC3261 [8].

Name and Number Restricted:

✎: From: “anonymous” <sip:anonymous@anonymous.invalid>;tag=1923837465

Number Restricted:

✎: From: "Some Name" <sip:anonymous@anonymous.invalid>;tag=1923837465

Name Restricted:

✎: From: <sip:+15617221122@123.12.23.45>;tag=1923837465

Note: The OpenScape Voice Rtp configuration parameter *Srx/Sip/useAnonymousFrom* used to indicate that the number in the *From* header should not be anonymized is being removed for OpenScape Voice V5.

The Rtp parameter is being replaced by a new OpenScape Voice SIP endpoint attribute "*Include Restricted Numbers in From header*" (reference section 7) which may be used to indicate that the number in the *From* header should not be anonymized if the SIP Endpoint Profile's '*Privacy*' support is set to '*Full*' or '*Full-Send*'.

If the SIP Trunking Endpoint Profile's Privacy Support is '*Basic*' or '*Full-Receive*' and the SIP endpoint attribute "*Include Restricted Numbers in From Header*" is enabled, OpenScape Voice does not anonymize the *From* header field URI but the display-name is set to "*anonymous*" for the initial INVITE request sent to the Service Provider.

Examples for header fields in the SIP INVITE to the SIP Trunking Endpoint when the calling party identity (Name and Number) is restricted:

- "*Include Restricted Numbers in From Header*" is NOT set
  - Privacy Support = Basic (or Full-Receive)

    ```
    From: <sip:anonymous@anonymous.invalid>
    <NO P-Asserted-Identity or Privacy header-field>
    ```

  - Privacy Support = Full (or Full-Send)

    ```
    From: <sip:anonymous@anonymous.invalid>
    P-Asserted-Identity: "Rodrigo Pastro"
    <sip:15619231470@10.0.0.100>
    Privacy: id
    ```

- "*Include Restricted Numbers in From Header*" is set
  - Privacy Support = Basic (or Full-Receive)

    ```
    From: "Anonymous"
    <sip:15619231470@10.0.0.100>;tag=snl_J9IFm9h881
    Privacy: user
    <NO P-Asserted-Identity header-field>
    ```

  - Privacy Support = Full (or Full-Send) and "*Include Restricted Numbers in From Header*" is set

    ```
    From: "Rodrigo Pastro" <sip:15619231470@anonymous.invalid>
    P-Asserted-Identity: "Rodrigo Pastro"
    <sip:15619231470@10.0.0.100>
    Privacy: id
    ```

Note: This capability is provided to allow interoperability with some Service Providers (e.g. Arcor) and Gateways that are not fully RFC3325 [17] compliant. It is expected that this SIP endpoint attribute configuration parameter and SIP Endpoint '*Privacy*' Profile will become obsolete when all Service Providers and gateways become RFC3325 [17] compliant. OpenScape Voice is able to send the identity of the OpenScape party that has performed a call forwarding, deflection or call transfer within the *From* header field in the event that the Service Provider is unable to accept a Diversion header field, in the case of a diversion, or *Referred-By* header field in the case of a call transfer (reference "*Do not send Diversion header*", "*Allow Sending of Insecure Referred-By Header*", "*Send redirecting Number rather than calling number for redirected calls*" and "*Send authentication number in xxx field*" SIP endpoint attributes in section 7).

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a *From* header from a Service Provider if it complies with the rules described above for sending to a Service Provider. The leading 60 characters in the URI field of the *From* header are used to look up the endpoint.

If the SIP Endpoint Profile's Privacy Policy is 'Basic' or 'Send-Full', OpenScape Voice will honor the privacy if signaled in the *From* header by use of display name anonymous (with or without double quotes).

6.4.17.2 From header field procedures by a Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should follow the rules described above for sending to a SP.

Receiving requests and responses from OpenScape Voice:

The Service Provider should honor the privacy if signaled in the header by use of display name *anonymous*.

6.4.18 Max-Forwards

OpenScape Voice and the Service Provider should support sending and receiving the *Max-Forwards* header field, according to RFC3261 [8]. Both OpenScape Voice and Service Provider should check, that the header field value has not reached the value 0. If this is the case, an SSNE should reject the request with a *483 "Too May Hops"* response.

: `Max-Forwards: 70`

6.4.19 Min-Expires

Not Applicable – SIP REGISTER requests are not sent on this interface (see Section 4.3.2, "Registration"); therefore, this header is not required.

6.4.20 Min-SE

RFC4028 [30] defines a mechanism for periodic refreshes of SIP sessions through a *re-INVITE* or *UPDATE* request.

According to RFC4028 [30], the *MIN-SE* header field indicates the minimum allowed lifetime of a SIP session.

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending *INVITE* requests containing the *Min-SE* header field to the Service Provider, according to RFC4028 [30]. Furthermore, it supports sending the *Min-SE* header field in *422 "Session Interval Too Small"* responses.

✎:
```
Supported: timer
Min-SE: 90
```

Note: The *Supported* or *Required* header field with the header field value with timer will be specified when the *Min-SE* and *Session-Expires* header fields are intended to be used.

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a *Min-SE* header field in a received *INVITE* request or in a received *422 "Session Interval Too Small"* response.

OpenScape Voice supports re-using a *Min-SE* header field value from a received *422 "Session Interval Too Small"* response for re-sending a new *INVITE* request, as specified above.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may support sending *INVITE* requests containing the *Min-SE* header field to OpenScape Voice.

Receiving requests and responses from OpenScape Voice:

A Service Provider may support receiving a *Min-SE* header field in a received *INVITE* request.

6.4.21 P-Asserted-Identity

The *P-Asserted-Identity* header field is used to convey the identity of authenticated users within a network and between trusted networks. This header field is particularly useful for conveying display information, it may be the basis for billing, and it allows providing certain telephony features on a per-user basis. This is only possible because it provides identity information based on a previous client authentication.

Note: The application of the *P-Asserted-Identity* header field relies on establishing an Enterprise "Trust Domain" relationship defined in RFC3325 [17], between OpenScape Voice and the Service Provider.

The relationship identifies how the identity information will be communicated and managed in either a bidirectional or unidirectional manner and is used to determine the proper provisioning of the OpenScape Voice SIP Endpoint Profile's '*Privacy*' support (reference section 7):

- If the relationship is bidirectional, the OpenScape Voice SIP Endpoint Profile's '*Privacy*' support should be set to 'Full'.
- If OpenScape Voice considers the Service Provider to be within the Enterprise "Trust Domain" but the Service Provider does not, or the Service Provider is unable to support the requirements for identifying an Enterprise "Trust Domain" to OpenScape Voice, the OpenScape Voice SIP Endpoint Profile's '*Privacy*' support of '*Full-Send*' should be used.
- If the Service Provider considers the OpenScape Voice to be within the Enterprise "Trust Domain" but OpenScape Voice does not have the same view, the OpenScape Voice Endpoint Profile's '*Privacy*' support of '*Full-Receive*' should be used.
- If neither the Service Provider or OpenScape Voice considers the peer to be within the Enterprise "Trust Domain" or the Service Provider is unable to support the Enterprise "Trust Domain" requirements, the OpenScape Voice SIP Endpoint Profile's '*Privacy*' support of '*Basic*' should be used.

For purposes of this specification, it is recommended that the Service Provider be considered part of the Enterprise "Trust Domain" for OpenScape Voice and the Service Provider consider OpenScape Voice to be in the same "Trust Domain", the OpenScape Voice SIP Endpoint Profile '*Privacy*' support '*Full*' should be used

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending the *P-Asserted-Identity* header field in requests and responses to the Service Provider.

Note: Sending the *P-Asserted-Identity* header field is specified by the OpenScape Voice SIP Endpoint Profile 'Privacy' support of 'Full' or 'Full-Send'. The setting depends on the Enterprise "Trust Domain" relationship with the Service Provider.

The userinfo part of the URI should be globally unique, that is in case a telephone number is available, it will either be an E.164 number in GNF or any other format that is accepted by the Service Provider (controlled by configurable options in the OpenScape Voice). A display name may be provided if available.

The URI parameter user=phone will be included in the sip: URI. The insertion of the user=phone parameter may be disabled (reference section 7 Rtp parameters).

:
```
P-Asserted-Identity: "Alice"
<sip:+49897221122@provider.com>
```

Note: The *From* header field should be populated with the desired public PSTN identity of the calling party, if a *P-Asserted-Identity* header field is present in the SIP request. In case privacy is requested, the *From* header field (see Section 6.4.17, “From”) should be anonymized, the *P-Asserted-Identity* header field should contain the callers identity, and the *Privacy* header field (see Section 6.4.23, “Privacy”) should be present with the value id. The reason behind this is that a Service Provider must have a means to perform billing and services.

Note: As an option, OpenScape Voice supports sending a private identity in the *P-Asserted-Identity* header field to a Service Provider. By default, this header field will contain the callers public identity (generally the same as the identity in the *From* header unless the *From* header is anonymized). See the SIP endpoint attributes “Use SIP Endpoint Default Home DN as Authentication Number”, “Use Subscriber Home DN as Authentication Number“ along with the “Send authentication number in …” attribute options in Chapter 7, “Configuration options for SIP Service Provider interoperability” which identify how an authenticated identity is selected and can then be sent in one or more identity header fields within the SIP INVITE.

Note: An Endpoint Attribute "Send Authentication Number in P-Asserted-Identity header" is available, see section 7 for details.

OpenScape Voice may be configured to send a P-Preferred-Identity header field rather than a P-Asserted-header field, see Section 6.4.22, “P-Preferred-Identity” below (reference "*Send P-Preferred-Identity rather than P-Asserted-Identity*" endpoint attribute in section 7).

OpenScape Voice is able to provide an OpenScape Voice authentication number within the *P-Asserted-Identity* (or *P-Preferred-Identity*) header field for calls which are redirected or transferred to the Service Provider (reference "*Send authentication number in P-Asserted-Identity header*" endpoint attribute in section 7). For example;

- If a call is redirected due to call deflection or call forwarding the *P-Asserted-identity* header may be used to identify the diverting user or another authentication number in place of the *Diversion* header.
- If a call is transferred to the Service Provider *P-Asserted-identity* header may be used to identify the transferring user or another authentication number in place of the Referred-By header.

  OpenScape Voice will send a *P-Asserted-Identity* header field to a SIP Service Provider which has Privacy Support set to 'Basic' or 'Full-Receive', provided the endpoint has the "*Send authentication number in P-Asserted-Identity*" attribute enabled. For these scenarios, the OpenScape Voice system will only include the *P-Asserted-Identity* header field in the initial SIP INVITE request.

  For basic calls from a SIP subscriber to the Service Provider, authentication is typically performed using the calling party number provided in the *From* or *P-Asserted-Identity* header field.

  However, for calls that are redirected or transferred to the Service Provider, the calling party number may not belong in that SP. For these scenarios, OpenScape Voice is able to send an authenticated number associated with the redirecting or transferring subscriber. The "*Send authentication number in xxx header*" attributes are used in these scenarios to indicate in which SIP header-field(s) the OpenScape Voice includes the number of the redirecting or transferring subscriber which will be used for authentication. OpenScape Voice allows the authentication number to be present in the *From*, *Diversion*, or *P-Asserted-Identity* header fields which may be influenced by the Service Provider's inability to accept and process a *Diversion* or *Referred-By* header field (reference "*Do not send Diversion header*", "*Allow Sending of Insecure Referred-By Header*", "*Send redirecting Number rather than calling number for redirected calls*" and "*Send authentication number in xxx field*" attributes in section 7).

  Receiving requests and responses from Service Provider:

OpenScape Voice is able to accept a *P-Asserted-Identity* header field from a SP. The *P-Asserted-Identity* may be passed to trusted subscribers if the *Privacy* header field value is “*id*”.

Note: Accepting a *P-Asserted-Identity* header field is a configurable option depending on the Enterprise "Trust Domain" relationship with the Service Provider. The header is processed within OpenScape Voice if the SIP Endpoint Profile's '*Privacy*' support is '*Full*' or '*Full-Receive*'.

Note: If more than one P-Asserted-Identity header is present in a message, only the first is taken into account.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may send a *P-Asserted-Identity* header field in requests and responses to OpenScape Voice, provided that the Service Provider and OpenScape Voice have a mutual agreement and the appropriate trust relationship. This might be useful for providing display names and call logging possibilities.

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to process a received *P-Asserted-Identity* header field in received requests and responses from an OpenScape Voice system, provided that the Service Provider and OpenScape Voice have a mutual agreement and the appropriate trust relationship.

6.4.22 P-Preferred-Identity

The *P-Preferred-Identity* header field is an optional header field that may be used at the client interface for indicating a preference of a particular identity in case several identities are available—for example, home, mobile, business, and so on.

Some Service Providers might require that this header field is used instead of the *P-Asserted-Identity* header field in order to convey identity information from the OpenScape Voice system (reference "*Send P-Preferred-Identity instead of P-Asserted-Identity*" SIP endpoint attribute in section 7 for details).

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice provides endpoint attributes to select between sending a *P-Asserted-Identity* or *P-Preferred-Identity* header field to SIP Trunks as follows:

Sending the header field depends on the Enterprise "Trust Domain relationship between the Service Provider and OpenScape Voice reflected in the OpenScape Voice SIP Endpoint Profile 'Privacy' Support. If the support is 'Full' or 'Full-Send', a P-Asserted-Identity or P-Preferred-Identity header field will be sent depending on the setting of the next attribute.

- Send P-Preferred-Identity rather than *P-Asserted-Identity*:
  If enabled, a *P-Preferred-Identity* header field will be sent rather than a *P-Asserted-Identity* header field.

Note: OpenScape Voice provides the following endpoint attribute to force the OpenScape Voice domain name (rather than an IP address) to be sent as the host part of the *P-Preferred-Identity* header URI:
- *Send domain name in From and P-Preferred-Identity headers*

The URI parameter user=phone will be included in the sip: URI. The insertion of the user=phone parameter may be disabled (reference section 7 Rtp parameters).

Receiving requests and responses from OpenScape Voice:

This header is not currently supported by OpenScape Voice and will be ignored by OpenScape Voice.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should not send the *P-Preferred-Identity* header field.

Receiving requests and responses from OpenScape Voice:

A SP may receive this header from OpenScape Voice if OpenScape Voice is configured to send a *P-Preferred-Identity* header field rather than a *P-Asserted-Identity* header field as described above.

6.4.23 Privacy

The *Privacy* header field is used to indicate that the identity of a person shall be withheld during the entire duration of a call. There are various header fields defined in RFC3323 [16] and RFC3325 [17] which require different behavior concerning handling of information in SIP requests and responses, see below.

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending the *Privacy* header field according to RFC3325 [17].

Sending the header field depends on the Enterprise "Trust Domain relationship between the Service Provider and OpenScape Voice reflected in the OpenScape Voice SIP Endpoint Profile '*Privacy*' Support. If the support is '*Full*' or '*Full-Send*', OpenScape Voice sends the *Privacy* header field with value '*id*' if the identity provided in the request must not leave the trust domain. This may require the Service Provider perform some actions to obscure identities or restrict presentation of identities contained in the request that are sent to untrusted interfaces.

If the SIP Trunking Endpoint Profile's Privacy Support is set to *Basic* (or *Full-Receive*) and the SIP endpoint has the "*Include Restricted Numbers in From Header*" attribute, when the calling party identity is restricted OpenScape Voice does not anonymize the *From* URI. Instead, the *From* header field includes a display name field set to "*Anonymous*" along with a "*Privacy: user*" header field in the message.

✎: `Privacy: id`

Receiving requests and responses from Service Provider:

OpenScape Voice supports receiving the *Privacy* header field values with *id*, *user*, *header* and *none* according to RFC3323 [16] and RFC3325 [17] whenever the service provider establishes an Enterprise "Trust Domain" relationship with OpenScape Voice, reflected by the OpenScape SIP Endpoint Profile's '*Privacy*' support of '*Full*' or '*Full-Receive*'.

✎: `Privacy: id`

In case a *Privacy* header field value with *id* is received, OpenScape Voice will send the received request or response including the *P-Asserted-Identity* header field only to trusted SSNEs. In case the destination SSNE is not trusted, OpenScape Voice will remove the *P-Asserted-Identity* header field before sending the request or response.

In case a *Privacy* header field value with *header* is received, OpenScape Voice will not add any header fields that might divulge identity information to the received request or response before it is routed to the next hop. Furthermore, it should rewrite every *Via, Record-Route* and *Contact* header field and store them for the entire duration of the session, so that the response can be constructed again to the sender of the request or response.

In case a *Privacy* header field value with *user* is received, OpenScape Voice will remove any header fields that have been added by the client, including the *Subject*, *Call-Info*, *Organization*, *User-Agent*, *Reply-To* and *In-Reply-To* before the request or response is routed to the next hop. The removed header fields should be stored for the entire duration of the session, so that the response can be constructed again to the sender of the request or response.

OpenScape Voice will not pass received identity information to a client whenever a *Privacy* header field was received with a value of *id*, *user*, or *header* (unless there are special local policies in place to treat the client as a trusted entity).

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending the *Privacy* header field value with *id* to the OpenScape Voice system, according to RFC3325 [17].

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to process a received *Privacy* header field value with *id* from the OpenScape Voice system, according to RFC3325 [17].

6.4.24 Proxy-Authenticate

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice will not send a *Proxy-Authenticate* header field to a Service Provider.

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a received *Proxy-Authenticate* header field in a *407 "Proxy Authentication Required"* response, if it is directed to the OpenScape Voice.

Note: Generally, OpenScape Voice expects a WWW-Authenticate header in a 401 "Unauthorized" response from the SP.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may send the *Proxy-Authenticate* header field in a *407 "Proxy Authentication Required"* response.

Receiving requests and responses from OpenScape Voice:

OpenScape Voice will not send a *Proxy-Authenticate* header field to a Service Provider.

6.4.25 Proxy-Authorization

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice is able to send a *Proxy-Authorization* header field to a Service Provider.

:
```
Proxy-Authorization: Digest username="5613383680",
          realm="siemens.com",nonce="4442bc9d7",
          uri="sip:49897221234@OpenScape_Voice.com",
          response="fcf587748",algorithm=MD5
```

Receiving requests and responses from Service Provider:

OpenScape Voice does not send a 407 response to the SP, therefore a `Proxy-Authorization` header is not expected in requests from a SP.

Service Provider:

Sending requests and responses to OpenScape Voice:

OpenScape Voice does not send a 407 response to the SP, therefore a `Proxy-Authorization` header is not expected in requests from a SP.

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to process a received *Proxy-Authorization* header field in SIP requests from OpenScape Voice if the SP sent a 407 response to the OpenScape Voice.

6.4.26 Proxy-Require

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice will not send this header to a SP.

Receiving requests and responses from Service Provider:

OpenScape Voice only looks for “100rel” and “timer” tags in this header if it is received from a SP.

Service Provider:

Sending requests and responses to OpenScape Voice:

If a SP sends this header to OpenScape Voice then only the “100rel” and “timer” tags in the header will be recognized by the OpenScape Voice.

Receiving requests and responses from OpenScape Voice:

OpenScape Voice will not send this header to a SP.

6.4.27 RAck

Reliable provisional responses are defined in RFC3262 [9]. Support for reliable provisional responses is indicated by the Supported or Required header field containing the value 100rel. The RAck header field indicates the sequence number of a provisional response in a PRACK request and is taken from a previously received RSeq header field (see Section 6.4.37, “Server”).

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending a *RAck* header field in a provisional response to a Service Provider, if the Service Provider has indicated support for reliable provisional responses according to RFC3262 [9].

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a received *RAck* header field in reliable provisional responses.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending a *RAck* header field in a provisional response to the OpenScape Voice system if the Service Provider has indicated support for reliable provisional responses according to RFC3262 [9].

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to process a received *RAck* header field in a provisional response from the OpenScape Voice system if reliable provisional responses are supported

6.4.28 Record-Route

A Service Provider should support sending and receiving a *Record-Route* header field according to RFC3261 [8].

```
: Record-Route:  <sip:serv2.siemens.com:5060;lr>
  Record-Route:  <sip:serv1.siemens.com:21020;lr>
```

Note: As a B2BUA, OpenScape Voice does not generate Record-Route headers, but is capable of receiving and passing these headers in responses.

6.4.29 Refer-To

The SIP *REFER* method, including the *Refer-To* header field, is defined in RFC3515 [19]. The *REFER* request indicates that the receiver should contact another client using the contact information from the *Refer-To* header field.

OpenScape Voice does not support sending a *SIP REFER* to the Service Provider.

OpenScape is able to accept a *SIP REFER* from a Service Provider for specific call transfer scenarios (Section 6.3.9, “REFER”).

6.4.30 Referred-By

The *Referred-By* mechanism is defined in RFC3892 [28]. The *Referred-By* header field provides information about the party that initiated a particular call feature—for example, a call transfer.

OpenScape Voice:

OpenScape Voice may pass a *Referred-By* header field to the Service Provider if received from the transferring UA.

OpenScape Voice provides a configuration option, via the following endpoint attribute, to control sending of this header field:

Allow sending of insecure Referred-By header

If this attribute is enabled, a *Referred-By* header field, excluding the Content-Id (cid) parameter, will be sent provided the transferring user's identity presentation is not restricted, in which case the identity in the header field is anonymized.

OpenScape Voice is able to send an authentication number which may not necessarily identity the call transfer party (transferor) within the Referred-By header field. The authentication number can also be included in the *From*, *P-Asserted-Identity* or *Diversion* header fields, or any combination. Another benefit is the ability to send the authentication number in alternative header fields whenever the Service Provider is unable to accept or process the header field normally used to convey the identity of a feature user, i.e., in this

case the *Referred-By* header field (reference "*Send authentication number in xxx header*" and "*Allow Sending of Insecure Referred-By Header*" SIP endpoint attributes in section 7).

Note: The URI parameter user=phone will be included in the sip: URI unless the URI is anonymized. The insertion of the user=phone parameter may be disabled (reference section 7 Rtp parameters).

OpenScape Voice ignores this header if received from a Service Provider.

Service Provider:

A Service Provider may support sending and receiving the *Referred-By* header field.

6.4.31 Remote-Party-ID

The Remote-Party-ID (RPID) header-field was defined as part of draft-ietf-sip-privacy [43], but it has been replaced by the P-Asserted-Identity (PAI) header-field which is defined in RFC3325 [17]. Nonetheless, OpenScape Voice supports the Remote-Party-ID header-field to inter-operate with Service Providers or Gateways that still use this header to transport caller ID information.

OpenScape Voice supports the Remote-Party-ID header field according to the following ABNF syntax:

```
Remote-Party-ID    = "Remote-Party-ID" HCOLON rpid *(COMMA rpid)
rpid               =  [display-name] LAQUOT addr-spec RAQUOT

                                          *(SEMI rpi-token)
rpi-token          = rpi-screen / rpi-pty-type /

                    rpi-id-type / rpi-privacy / other-rpi-token
rpi-screen         = "screen" EQUAL ("no" / "yes")
rpi-pty-type       = "party" EQUAL ("calling" / "called" / token)
rpi-id-type        = "id-type" EQUAL ("subscriber" / "user" /

                                           "term"  / token)
rpi-privacy        = "privacy" EQUAL

                     (rpi-priv-element

                      /(LDQUOT rpi-priv-element

                         *(COMMA rpi-priv-element) RDQUOT)

                      )
rpi-priv-element   = ("full" / "name" / "uri" / "off" / token)

                                      ["-" ( "network" / token )]
other-rpi-token    = ["-"] token [EQUAL (token / quoted-string)]
```

The "display-name" in Remote-Party-ID is a text string that identifies the name of the party. The "addr-spec" contains information identifying the party either in clear-text or encrypted form. In the latter case, the addr-spec contains a SIP-URI or a SIPS-URI where the "userinfo" part of the "addr-spec" typically contains the

encrypted party information, whereas the "hostport" identifies the entity that can decrypt the information. Furthermore, an "other-user" value of "private" will then be present to indicate that the "addr-spec" is non-intelligible.

Note: OpenScape Voice shall ignore the Remote-Party-ID header-field in case the "addr-spec" has an “other-user” value of “private” (e.g. sip:xxxxxxxxx@10.190.128.139;user=private).

OpenScape Voice shall only use the Remote-Party-ID header-field for the “calling” party’s identity.

Note: OpenScape Voice shall ignore the Remote-Party-ID field when the rpi-pty-type parameter is included and it is not set to “calling”.

The rpi-privacy parameter describes whether the identity information must be hidden from untrusted entities. There MAY be multiple rpi-privacy parameters in a Remote-Party-ID. If privacy is requested, it MUST be one or more of "full", "uri", or "name". The value "full" means that both the "display-name" and the "addr-spec" MUST be hidden. The values "name" and "uri" mean that the "display-name" or the "addr-spec" MUST be hidden respectively. The value "off" indicates that lack of privacy is explicitly requested, and MUST be the only value if present. The values may be postfixed with a string indicating that the privacy request was made by an entity other than the party itself. Postfixing with the value "-network" indicates that intermediaries ("the network") have requested that the information be hidden, despite the user not making such a request.

Note: OpenScape Voice shall ignore the following parameters:
- rpi-screen
- rpi-id-type

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice shall not send a *Remote-Party-ID* header field to a Service Provider.

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a received *Remote-Party-ID* header field in a SIP *INVITE* or *INFO* request, according to draft-ietf-sip-privacy [43], with the exceptions noted above.

Note: The presence of the display-name set to *pending* in a calling Remote-Party-ID header of an INVITE denotes that the display-name is to follow in an INFO message.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may send the *Remote-Party-ID* header field in a SIP *INVITE* or *INFO* request.

Receiving requests and responses from OpenScape Voice:

OpenScape Voice shall not send a *Remote-Party-ID* header field to a Service Provider.

6.4.32 Replaces

The *Replaces* header field is defined in RFC3891 [27]. The *Replaces* header field is used to replace an existing SIP dialog with a new SIP dialog. This mechanism may be particularly useful for higher level features.

This header is not supported by OpenScape Voice for the SP interface. The OpenScape Voice will not send this header to the SP. The OpenScape Voice will not include the *replaces* tag in *Supported* headers sent to the SP, therefore the SP should not send a *Replaces* header to the OpenScape Voice.

6.4.33 Require

OpenScape Voice and a Service Provider should support sending and receiving the *Require* header field, according to RFC3261 [8]. If the OpenScape Voice or a Service Provider received an option tag in a *Require* header field that is not supported, it should respond with a *420 "Bad Extension"* response including an *Unsupported* header field.

✎: `Require: timer, 100rel, replaces, foo`

Note: If a specified option tag is not understood, the SSNE responds with:

✎: `SIP/2.0 420 Bad Extension`

...

Unsupported: foo

A list of supported option tags can be found in Section 6.4.40, "Supported".

6.4.34 Retry-After

The Retry-After header field in error responses indicates the number of seconds after which the client may retry sending the same request.

OpenScape Voice:

OpenScape Voice supports sending and receiving the *Retry-After* header field in error responses according to RFC3261 [8] with the following qualifications. If a 5xx with retry-after is received, OpenScape Voice reports an error on that transaction (e.g. drops the call if sending an initial INVITE or fails media renegotiation if sending a mid-session INVITE, i.e., reINVITE).

Service Provider:

A Service Provider may support sending and receiving the *Retry-After* header field in error responses according to RFC3261 [8].

6.4.35 Route

The *Route* header field is used to force routing for a request through a list of proxies. This list may have been obtained from a received *Record-Route* header field from an edge proxy (see Section 6.4.28, “Record-Route”).

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending a *Route* header field in SIP requests to a Service Provider if a *Record-Route* header has been received from the SP.

✎:
```
Route: <sip:serv1.siemens.com>,
       <sip:serv2.siemens.com>
```

Receiving requests and responses from Service Provider:

OpenScape Voice, acting as a B2BUA, does not expect to receive this header and will ignore it if received.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may support sending a *Route* header field in requests to OpenScape Voice, although this should never be necessary as OpenScape Voice will never send a *Record-Route* header to the SP.

Receiving requests and responses from OpenScape Voice:

A Service Provider may be able to process a received *Route* header field in received requests.

6.4.36 RSeq

Reliable provisional responses are defined in RFC3262 [9]. Support for reliable provisional responses is indicated by the *Supported* or *Required* header field containing the value *100rel*. The *RSeq* header field specifies a sequence number in a provisional response to an *INVITE* request. This header field value is used in conjunction with the *RAck* header field (see Section 6.4.27, “RAck”).

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending a RSeq header field in a provisional response to a Service Provider, if the Service Provider has indicated support for reliable provisional responses according to RFC3262 [9].

: `RSeq: 5556`

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a received *RSeq* header field in reliable provisional responses, if reliable provisional responses are supported.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending a *RSeq* header field in a provisional response to the OpenScape Voice system if the Service Provider has indicated support for reliable provisional responses according to RFC3262 [9].

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to process a received *RSeq* header field in a provisional response from the OpenScape Voice system if reliable provisional responses are supported.

6.4.37 Server

OpenScape Voice may send a *Server* header to a Service Provider. A SP may send a *Server* header to OpenScape Voice.

6.4.38 Session-Expires

RFC4028 [30] defines a mechanism for periodic refreshes of SIP sessions through a *re-INVITE* or *UPDATE* request. According to RFC4028 [30], the *Session-Expires* header field indicates the duration of a SIP session after which a session must be terminated, unless a session refresh via *re-INVITE* or *UPDATE* requests is performed.

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending *INVITE* requests containing the *Session-Expires* header field to the Service Provider, according to RFC4028 [30]. OpenScape Voice also supports sending the *Session-Expires* header field in *2xx* responses to *INVITE* requests.

✎: `Session-Expires: 7200;refresher=uas`

Note: The *Supported* or *Required* header field with the header field value with *timer* should be specified when usage of the Min-SE or Session-Expires header field is made.

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a *Session-Expires* header field in a received *INVITE* request or in a received *2xx* response.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider may support sending *INVITE* requests or *2xx* responses containing the *Session-Expires* header field to OpenScape Voice.

Receiving requests and responses from OpenScape Voice:

A Service Provider may support receiving a *Session-Expires* header field in a received *INVITE* request or *2xx* response.

6.4.39 Subscription-State

The *Subscription-State* header field indicates the state of a subscription—that is, a subscription may be *active*, *pending* or *terminated*.

For details refer to RFC3265 [12].

Note: OpenScape Voice does not support use of the *pending* state.

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending a *Subscription-State* header field according to RFC3265 [12] in *NOTIFY* requests, if the *SUBSCRIBE*/*NOTIFY* mechanism is supported and if at least one event package is supported by both Service Provider and OpenScape Voice.

✎: `Subscription-State: active`

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a received *NOTIFY* request containing a *Subscription-State* header field, if at least one event package is supported.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending a *Subscription-State* header field according to RFC3265 [12] in *NOTIFY* requests if at least one event package is supported.

A Service Provider should support passing a received *Subscription-State* header field transparently to OpenScape Voice, even if this header field is not supported at the Service Provider.

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to accept a received *NOTIFY* request containing a *Subscription-State* header field according to RFC3265 [12], if at least one event package is supported.

A Service Provider should support passing a received *Subscription-State* header field transparently to the destination, even if this header field is not supported at the Service Provider.

6.4.40 Supported

The *Supported* header field indicates the capabilities that the originator of the request has implemented.

The following options are supported by OpenScape Voice for the SIP Service Provider interface and are defined in the corresponding RFCs:

- 100rel (see RFC3262 [9])
- timer (see RFC4028 [30])
- replaces (see RFC3891 [27])
- early-session (see RFC3959 [42]
- Precondition (see RFC3312 [41])

Note: OpenScape Voice does not support use of the *replaces* or *Precondition* options for the Service Provider interface.

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending the *Supported* header field to the Service Provider, if at least one option is supported (see above).

: `Supported: timer, 100rel`

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process the *Supported* header field from the Service Provider, according to RFC3261 [8].

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending the *Supported* header field if at least one option is supported.

Receiving requests and responses from OpenScape Voice:

A Service provider should be able to accept the *Supported* header field from OpenScape Voice.

6.4.41 To

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending any supported URI scheme (as specified in Section 6.2.1, “URI Schemas”) in the *To* header field of a request outside the context of an existing dialog.

Note: For responses, OpenScape Voice is constrained to support whatever URI scheme was in the request. For mid-dialog requests, OpenScape Voice is constrained to support whatever URI was in the dialog-forming request. For example, if OpenScape Voice received an INVITE request in which the *From* header field URI was not in accordance with Section 6.4.1, “Request URI” and if OpenScape Voice sends a mid-dialog request, the To header field URI is constrained to be the same.

The URI parameter user=phone will be included in the sip: URI except when the URI is anonymized. The insertion of the user=phone parameter may be disabled (reference section 7 Rtp parameters).

: `To: <sip:+15613386610@provider.com;user=phone>`

Receiving requests and responses from Service Provider:

OpenScape Voice is able to accept any supported URI scheme (see Section 6.2.1, “URI Schemas”) in the *To* header field.

No constraints are put on the contents of the *To* header field.

Note: The *To* header field in received SIP requests may be different from the request URI due to call diversion, call transfer, and other features.

Service Provider:

Sending requests and responses to OpenScape Voice:

No constraints are put on the contents of the *To* header field.

Receiving requests and responses from OpenScape Voice:

For a request outside the context of an existing dialog, the Service Provider should be able to accept any URI scheme in the *To* header field.

6.4.42 Unsupported

An SSNE may support sending and receiving this header field.

6.4.43 User-Agent

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice will not send a *User-Agent* header field to the Service Provider.

Receiving requests and responses from Service Provider:

OpenScape Voice will accept any value in the *User-Agent* header field according to RFC3261 [8].

: `User-Agent: superPhone 1.0`

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider, acting as a proxy, should support passing a received *User-Agent* header field transparently to the OpenScape Voice system.

Receiving requests and responses from OpenScape Voice:

OpenScape Voice will not send a *User-Agent* header field to the Service Provider.

6.4.44 Via

The *Via* header fields are used to indicate the path taken by a SIP request from the sender of the request to the destination through one or more intermediate SSNEs and Service Provider equipment (see Section 6.4.28, “Record-Route”). The subsequent responses should be routed according to the header field value of the *Via* header fields.

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice supports sending a *Via* header field in SIP requests and responses to a Service Provider.

```
Via: SIP/2.0/UDP 10.22.22.44:5060;branch=z9hG4bK_111
Via: SIP/2.0/UDP 10.22.22.100:5060;branch=z9hG4bK_222
```

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a received *Via* header field in received requests and responses according to RFC3261 [8].

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending a *Via* header field in requests and responses to the OpenScape Voice system.

Receiving requests and responses from OpenScape Voice:

A Service Provider should be able to process a received *Via* header field in received requests and responses.

6.4.45 Warning

OpenScape Voice:

OpenScape Voice may include a *Warning:* header with a warning code of *399* in some SIP response messages. The intent of the *Warning* header is to facilitate the debugging of complex scenarios, there is no need for any device to take any special action based on this header field (for example, *Warning: 399*).

<OpenScape Voice> "No License").

Service Provider:

A Service Provider should support sending the Warning header field to the OpenScape Voice system.

6.4.46 WWW-Authenticate

OpenScape Voice:

Sending requests to Service Provider:

OpenScape Voice can support sending the *WWW-Authenticate* header field in *401 "Unauthorized"* responses.

✎: `WWW-Authenticate: Digest realm="siemens.com", nonce="e77511be36e123e063196c019b6f9582", stale=false, algorithm="MD5", qop="auth"`

Note: Digest Authentication is a OpenScape Voice configuration option.

Receiving requests and responses from Service Provider:

OpenScape Voice, acting as a B2BUA, is able to process a received *WWW-Authenticate* header field in *401 "Unauthorized"* responses.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider should support sending the *WWW-Authenticate* header field in *401 "Unauthorized"* responses to OpenScape Voice.

Receiving requests and responses from OpenScape Voice:

A Service Provider should able to process a received *WWW-Authenticate* header field in *401 "Unauthorized"* responses.

6.4.47 X-Siemens-Call-Type

The private SIP header field X-Siemens-Call-Type may be used in a SIP INVITE request to indicate that the call is a reverse charge (aka collect) call e.g.

```
X-Siemens-Call-Type: collect-call
```

OpenScape Voice:

If OpenScape Voice receives this header field containing the collect-call token the call will be rejected if the called subscriber is not allowed to receive collect calls. The call will be rejected with a SIP 403 "`Forbidden`" response including a SIP Warning header field:

```
Warning: 399 <OSCV IP address> "Automatic Collect Call Blocking"
```

Service Provider:

A Service provider may include a *X-Siemens-Call_Type* header field with the *collect-call* token in a *SIP INVITE* request if the Service Provider is aware that this is a collect call.

6.4.48 X-Siemens-CDR

The X-Siemens-CDR header field is defined as follows:

```
X-Siemens-CDR = "X-Siemens-CDR" HCOLON id-set
id-set =  idtoken 0*4(COMMA idtoken)
idtoken = gidgen | gidseq | tidgen | tidseq | chargenum
gidgen = "gid-gn" EQUAL <string>
gidseq = "gid-seq" EQUAL <integer>
tidgen = "tid-gn" EQUAL  <string>
tidseq = "tid-seq" EQUAL <integer>
chargenum = "charge" EQUAL <string>
```

Example: X-Siemens-CDR: charge=5619234764

Note: The *gidgen*, *gidseq*, *tidgen*, and *tidseq* parameters have been defined for PBX networking and are outside the scope of this document.

OpenScape Voice:

If OpenScape Voice receives a *SIP INVITE* or *REFER* request containing the *X-Siemens-CDR* header field with the *charge* parameter then charge number will be stored as the billing number in the CDR. In addition the number plan, rate area, and code/toll restriction services associated with this charge number will also be used to process the call.

Note: This functionality is enabled/disabled by an OpenScape Voice endpoint attribute.

Service Provider:

A Service Provider may include a *X-Siemens-CDR* header field with the *charge* token in a *SIP INVITE* or *REFER* request.

6.4.49 Processing of Unknown Header Fields

All unknown header fields should be processed according to RFC3261 [8].

6.5 SIP Response Codes

Within Table 6.2 the following legend is used to indicate compliance with use of the associated SIP Response Code as defined in the associated reference:

Y	YES - response code must be sent or processed in accordance with associated reference.
N	NO - response code can not/should not be sent, and/or can not be processed if received.
N/A	NOT APPLICABLE - to this type of network element and/or interface.
P	PARTIAL - response code may be sent/received but processing is not fully compliant with the associated reference.
O	OPTIONAL – support for the response code is not necessary.

SIP Response Code	Reference	SP		OpenScape Voice		Comment
		Send	Recv	Send	Recv	
100 Trying	[RFC 3261] 21.1.1	Y	Y	Y	Y	
180 Ringing	[RFC 3261] 21.1.2	Y	Y	Y	Y	
181 Call Is Being Forwarded	[RFC 3261] 21.1.3	Y	Y	Y	Y	OpenScape Voice may return 181 response if call is forwarded by OpenScape Voice (without sending for example 302 response to calling UA). May be passed transparently if received from another network element.
182 Queued	[RFC 3261] 21.1.4	O	O	N	Y	OpenScape Voice acting as B2BUA never sends this response.
183 Session Progress	[RFC 3261] 21.1.5	Y	Y	Y	Y	
200 OK	[RFC 3261] 21.2.1	Y	Y	Y	Y	
202 Accepted	[RFC 3265] 7.3.1 [RFC 3515] 2.4.2	O O	O O	N Y	Y NA	OpenScape Voice currently only sends 202 code as a response to a REFER request for call transfer.
300 Multiple Choices	[RFC 3261] 21.3.1	O	O	NA	Y	OpenScape Voice acting as B2BUA never sends this response.
301 Moved Permanently	[RFC 3261] 21.3.2	O	O	NA	Y	OpenScape Voice acting as B2BUA never sends this response.
302 Moved Temporarily	[RFC 3261] 21.3.3	O	O	Y	Y	OpenScape Voice may send a 302 response to a SP to perform redirection, and in these cases a rtag URI parameter may be included in the Contact header. This rtag parameter should be returned in the request URI of the subsequent new SIP INVITE. Sending of 302 responses to a SP may be enabled or disabled via an endpoint provisioning option.
305 Use Proxy	[RFC 3261] 21.3.4	N	N	N	N	
380 Alternative Service	[RFC 3261] 21.3.5	N	N	N	N	

Table 6.2 SIP Response Codes (Sheet 1 of 3)

SIP Response Code	Reference	SP		OpenScape Voice		Comment
		Send	Recv	Send	Recv	
400 Bad Request	[RFC 3261] 21.4.1	Y	Y	Y	Y	
401 Unauthorized	[RFC 3261] 21.4.2	Y	Y	Y	Y	
402 Payment Required	[RFC 3261] 21.4.3	NA	NA	NA	NA	
403 Forbidden	[RFC 3261] 21.4.4	Y	Y	Y	Y	
404 Not Found	[RFC 3261] 21.4.5	Y	Y	Y	P	Will be treated as 400.
405 Method Not Allowed	[RFC 3261] 21.4.6	Y	Y	Y	Y	
406 Not Acceptable	[RFC 3261] 21.4.7	Y	Y	Y	Y	
407 Proxy Authentication Required	[RFC 3261] 21.4.8	Y	N	N	Y	
408 Request Timeout	[RFC 3261] 21.4.9	Y	Y	Y	Y	
410 Gone	[RFC 3261] 21.4.10	O	Y	N	P	Will be treated as 400.
412 Conditional Request Failed	[RFC 3903] 11.2.1	Y	Y	Y	Y	
413 Request Entity Too Large	[RFC 3261] 21.4.11	O	O	N	P	Will be treated as 400.
414 Request-URI Too Long	[RFC 3261] 21.4.12	O	O	N	P	Will be treated as 400.
415 Unsupported Media Type	[RFC 3261] 21.4.13	O	Y	Y	P	Will be treated as 400.
416 Unsupported URI Scheme	[RFC 3261] 21.4.14	O	O	N	P	Will be treated as 400.
420 Bad Extension	[RFC 3261] 21.4.15	Y	Y	Y	P	Will be treated as 400.
421 Extension Required	[RFC 3261] 21.4.16	O	O	N	P	Will be treated as 400.
422 Session Interval Too Small	[RFC 4028] 7.4, 9	Y	Y	Y	Y	
423 Interval Too Brief	[RFC 3261] 21.4.17	Y	Y	Y	Y	
480 Temporarily Unavailable	[RFC 3261] 21.4.18	Y	Y	Y	Y	
481 Call/Transaction Does Not Exist	[RFC 3261] 21.4.19	Y	Y	Y	Y	
482 Loop Detected	[RFC 3261] 21.4.20	Y	Y	Y	Y	
483 Too Many Hops	[RFC 3261] 21.4.21	Y	Y	Y	Y	
484 Address Incomplete	[RFC 3261] 21.4.22	O	O	N	P	Will be treated as 400.

Table 6.2 SIP Response Codes (Sheet 2 of 3)

SIP Response Code	Reference	SP		OpenScape Voice		Comment
		Send	Recv	Send	Recv	
485 Ambiguous	[RFC 3261] 21.4.23	O	O	N	P	Will be treated as 400.
486 Busy Here	[RFC 3261] 21.4.24	Y	Y	Y	Y	
487 Request Terminated	[RFC 3261] 21.4.25	Y	Y	Y	Y	
488 Not Acceptable Here	[RFC 3261] 21.4.26	O	Y	Y	P	May also be returned when called UA cannot support the offered IP version (IPv4/IPv6). Should be treated as a semi-permanent failure i.e. callback is not appropriate. When received, will be treated as 400.
491 Request Pending	[RFC 3261] 21.4.27	Y	Y	Y	Y	
493 Undecipherable	[RFC 3261] 21.4.28	O	O	N	P	Will be treated as 400.
500 Server Internal Error	[RFC 3261] 21.5.1	Y	Y	Y	Y	
501 Not Implemented	[RFC 3261] 21.5.2	O	O	N	P	Will be treated as 500.
502 Bad Gateway	[RFC 3261] 21.5.3	O	O	N	P	Will be treated as 500.
503 Service Unavailable	[RFC 3261] 21.5.4	Y	Y	Y	Y	
504 Server Time-out	[RFC 3261] 21.5.5	O	Y	Y	P	Will be treated as 500.
505 Version Not Supported	[RFC 3261] 21.5.6	O	O	N	P	Will be treated as 500.
513 Message Too Large	[RFC 3261] 21.5.7	O	O	N	P	Will be treated as 500.
600 Busy Everywhere	[RFC 3261] 21.6.1	O	O	N	Y	
603 Decline	[RFC 3261] 21.6.2	O	Y	Y	P	Will be treated as 600. OpenScape Voice may send 603 if Resource Management determines that requested bandwidth is not available/authorized.
604 Does Not Exist Anywhere	[RFC 3261] 21.6.3	O	O	N	P	Will be treated as 600.
606 Not Acceptable	[RFC 3261] 21.6.4	O	O	Y	P	When received from Service Provider will be treated as 600. OpenScape Voice may include a 606 case code in a Reason header field within a SIP BYE message to indicate that the call is being released due to bandwidth limitations imposed by the Call Admission Control: Reason: SIP ;cause=606 ;text= "Not Available".

Table 6.2 SIP Response Codes (Sheet 3 of 3)

For incoming calls, provided the OpenScape Voice and Service Provider are in the same Enterprise "Trust Domain" OpenScape Voice may deliver the releasing party identity within the *P-Asserted-Identity* header field.

If the OpenScape Voice Endpoint Profile's '*Privacy*' support is '*Privacy - Full*' or '*Privacy - Full-Send*', if the call is released by another party, the identity of the releasing party is included in the *P-Asserted-Identity* header filed for the *4xx/5xx/6xx* response.

6.6 SIP Event Packages

6.6.1 Message-Summary

Note: Support for a Service Provider acting as a MWI Supplier is not a fully supported capability of OpenScape Voice. Nevertheless, the capability is supported by the SIP interface and is described here.

The *message-summary* event package is defined in RFC3842 [26]. This event package is used for Message Waiting Indication (MWI) (see Section 5.6, “Message Waiting Indication”).

OpenScape Voice:

Sending requests and responses to Service Provider:

OpenScape Voice will not send a *message-summary* event to the Service Provider, because Message Waiting indications are only supported from the Service Provider to the OpenScape Voice system.

Note: The *Message Waiting Indication* feature support may reside at the Service Provider. The Service Provider sends *NOTIFY* requests with the *message-summary* event to the OpenScape Voice system client whenever a new message needs to be announced to the client or when the mailbox has been emptied.

Receiving requests and responses from Service Provider:

OpenScape Voice is able to process a received *NOTIFY* request with a *message-summary* event according to RFC3842 [26] if it acts as a MWI consumer. In this case it is able to process the *Messages-Waiting* line

from the SIP message body of a *NOTIFY* request containing a *message-summary* event (OpenScape Voice ignores *Voice-Message* line if present).

Note: Both MWI supplier and MWI consumer must have an agreement to send message-summary events without explicit subscription.

An example *NOTIFY* request is depicted below:

Event header field:	see Section 6.4.15, “Event”, *message-summary*
Subscription-State header field:	see Section 6.4.39, “Subscription-State”, valid values are either *active* or *terminated (pending* state not supported by OpenScape Voice)
Content-Type header field:	see Section 6.4.12, “Content-Type”, *application/simple-message-summary*
SIP Message Body:	*Messages-Waiting: yes* or *no* *Voice-Message: old_msg/new_msg*, where old_msg stands for the total number of messages and new_msg stands for the number of new messages. This line is ignored by OpenScape Voice. Details on the body type can be found in RFC3842 [26]. Note that some applications may send additional data in the body. All body data will be passed to the client.

Note: Some applications may send additional data in the *NOTIFY* bodies. All body data will be passed to the client.

Service Provider:

Sending requests and responses to OpenScape Voice:

A Service Provider, acting as a MWI supplier, may support sending a *message-summary* event in a *NOTIFY* request based on a mutual agreement with the OpenScape Voice server. The corresponding *NOTIFY* requests will be sent outside the context of a subscription.

Receiving requests and responses from OpenScape Voice:

OpenScape Voice will not send a *message-summary* event to the Service Provider, because Message Waiting indications are only supported from the Service Provider to the OpenScape Voice system. OpenScape Voice does not send SUBSCRIBE requests for MWI notification as the notification is based on a mutual agreement with the OpenScape Voice system.

6.6.2 CCBS/CCNR

Note: Use of SIP to provide the CCBS/CCNR features between OpenScape Voice and a Service Provider is not a fully supported capability of OpenScape Voice. Nevertheless, the capability is supported by the SIP interface and is described here.

The CCBS/CCNR event packages allow the SIP protocol to signal between switching entities CCBS and CCNR information that is normally carried in ISUP and in TCAP. With this feature, switching entities can request, cancel, suspend, and resume monitoring of a subscriber located on another switch.

The *ccbs and ccnr* event packages are defined in TISPAN_CCBS.

Event header field:	see Section 6.4.15, “Event”, Event: ccbs;event-parms Event-parms are the following: 1. queue=true/suspend/resume 2. caller= (only on initial SUBSCRIBE) 3. service-retention=service-release/service-retained 4. reason=T2 timeout/T3 timeout/T4 timeout/user deactivated/temporary failure Event: ccnr;event-parms Event-parms are the following: 1. queue=true/suspend/resume 2. caller= (only on initial SUBSCRIBE) 3. service-retention=service-release/service-retained 4. reason=T2 timeout/T3 timeout/T4 timeout/user deactivated/temporary failure
Subscription-State header field:	see Section 6.4.39, “Subscription-State”, valid values are either *active* or *terminated (pending* state not supported by OpenScape Voice)
Content-Type header field:	Not applicable – message body not used for this event package
SIP Message Body:	Not applicable – message body not used for this event package

6.7 SIP Bodies

6.7.1 SIP Body Type

An SSNE must pass through any SIP message body to the next hop.

6.7.2 Multipart-Mixed Body Type

An SSNE, acting as a B2BUA, should understand the multipart-mixed MIME data structure. It should be able to inspect a multipart-mixed MIME body and to retrieve the contained information from the multipart-mixed MIME body. Although OpenScape Voice supports the multipart-mixed MIME data structure, it is not currently used for the Service Provider interface.

6.7.3 Unknown SIP Bodies

An SSNE acting as a UAS must reject unknown SIP bodies with a *406 "Not Acceptable"* response if no *Content-Disposition* header field is specified, or if the *Content-Disposition* header field is specified with the value *handling=required*.

7 Configuration options for SIP Service Provider interoperability

The following OpenScape Voice configuration options have been found useful when attempting to comply with some SIP Service Provider signaling requirements that are outside the scope of any standards documents.

Name	Default	Description	Ref.
Rtp configuration parameters			
Srx/Main/ SRSSetDiversionHeader	RtpFalse	When enabled, OpenScape Voice treats Serial Ringing and Simultaneous Ringing as call redirections for purposes of the 'Originating tenant group required' and 'Send forwarding number rather than calling number for forwarded calls' options described below.	
Srx/Sip/ PhoneUserParameter	1	Values are: 0=never send, 1=send except for anonymous, 2=always send Applies to To, From, P-Asserted-Identity, P-Preferred-Identity, Diversion and Referred-By header fields	
Endpoint attributes			
Do not send INVITE without SDP	Disabled	When enabled, OpenScape Voice will not send reINVITE requests without SDP (a modified call flow is used to achieve this).	Sect. 4.3.15
Send redirecting number rather than calling number for redirected calls [See 1]	Disabled	When enabled, replaces the calling party number (in From and PAI/PPI) headers with the last redirecting of referring number.	Sect. 5.5.1
Do not send Diversion header	Disabled	When enabled, prevents OpenScape Voice from sending Diversion headers	
Send domain name in From and P-Preferred-Identity headers	Disabled	When enabled, the OpenScape Voice domain name will be sent in these headers when IP addresses would otherwise be sent.	Sect. 6.4.17

Privacy	Basic	For most Service Providers this parameter should be set to 'Full' to enable RFC3325 behavior i.e. sending and processing of P-Asserted-Identity header and Privacy header, while 'Basic' does not send or process the P-Asserted-Identity. Additional options are available; from the perspective of OpenScape Voice: • "Full Send" the information is sent but not processed upon reception. • "Full Receive" the information is processed upon reception but not sent..	Sect. 6.4.21
Send P-Preferred-Identity rather than P-Asserted-Identity	Disabled	When enabled, a P-Preferred-Identity header will be sent when a P-Asserted-Identity would otherwise be sent.	Sect. 6.4.22
Allow sending of insecure Referred-By header	Disabled	When enabled, allows a Referred-By header (received from transferring user) to be passed to the Service Provider.	Sect. 6.4.30
Send Uri in Telephone Subscriber Format	Disabled	When enabled, specific header field URI's containing numbers will be sent to the Service provider in Global number Format (GNF) i.e. E.164 format with a leading "+" character. The following header field URI's apply: • Request-URI • From • To • P-Asserted-Identity • P-Preferred-Identity • Diversion • Referred-By	Sect. 6.4.21
Send Authentication number in P-Asserted-Identity header	Disabled	When enabled, the last redirecting [See 2] (or transferring) number will be sent in the PAI header if the PAI would otherwise not contain an OpenScape Voice subscriber number. If the calling number is not an OpenScape Voice subscriber number or the redirecting number is not an OpenScape Voice subscriber number, a default Home DN identity may be sent.	Sect. 6.4.21

Send Authentication number in From header	Disabled	When enabled, the last redirecting [See 2] or transferring number will be sent in the *From* header. If the calling number is not an OpenScape Voice subscriber number or the redirecting number is not an OpenScape Voice subscriber number, a default Home DN identity may be sent.	Sect. 6.4.21
Send Authentication number in Diversion header	Disabled	When enabled, the last redirecting [See 2] or transferring number will be sent in the *Diversion* header. If the calling number is not an OpenScape Voice subscriber number or the redirecting number is not an OpenScape Voice subscriber number, a default Home DN identity may be sent. Attribute used in conjunction with “Do not send Diversion header”.	Sect. 6.4.21
Best Effort SRTP	Automatic	When set to Disabled, OSCV will remove any SRTP media stream from the SDP offer sent to the endpoint. This is necessary for Service Providers that cannot handle an SDP offer with an SRTP stream. If an SBC is used between OSCV and the Service Provider then mediation between SRTP and RTP can be provided by the SBC and this endpoint parameter does not have to be set to disabled.	
Automatic Collect Call Blocking Supported	Disabled	When set, OSCV will invoke Collect Call Blocking SIP signaling procedures as required for PSTN interworking in Brasil.	
Accept billing number	Disabled	When enabled, a charge number received in a X-Siemens-CDR header field of a SIP INVITE or REFER request (for blind call transfer) will be included as the "ANI/Billing number" (field13.) of the CDR for the call.In addition the number plan, rate area, and code/toll restriction services associated with this party will also be used to process the call.	
Transfer Handoff	Disabled	When enabled REFER requests from OSCV subscribers are passed to the endpoint i.e. OSCV 'proxies' the transfer request.	
Allow Sending of Insecure Referred-By Header	Disabled	When enabled, OpenScape Voice will sent a Referred-By header field for calls transferred to this endpoint.	

Send P-Preferred-Identity rather than P-Asserted-Identity	Disabled	When enabled, OpenScape Voice will send a P-Preferred-Identity header field whenever a P-Asserted-Identity header field would be sent.	
Supports SIP UPDATE Method for Display Purposes	Disabled	When enabled, OpenScape Voice will send a P-Asserted-Identity (or P-Preferred-Identity) header field for any changes in the identity of the OpenScape Voice calling or called user.	
Include Restricted Numbers in From header	Disabled	When enabled, the From header field URI will not be anonymized when the OpenScape Voice user's presentation is restricted. The attribute is dependent on the SIP Endpoint profile's 'Privacy' setting, which must be 'Full' (or 'Full-send').	
PRACK Enable	Disabled	When enabled,OpenScape Voice provides the mechanism for "reliable provisional response" handling on a half call basis (i.e. not end-to-end). **Exception**: When a 3PCC initial SIP INVITE is received not containing an SDP offer but including a Supported:100rel, the following applies: • OpenScape Voice shall respond with a delayed SDP offer in the 200 OK response. • When the egress SIP interface also has this attribute enabled, OpenScape Voice shall not include the 100rel indication in the Supported header field.	
Use SIP Endpoint Default Home DN as Authentication Number	Disabled	Used in conjunction with "Use Subscriber Home DN as Authentication Number". Both attributes may be reset (default) [See 3] or one set (mutually exclusive). If set, the SIP endpoint's "Default Home DN" is used as the authenticated number.	Sect. 5.1.1.1 Sect. 6.4.21
Use Subscriber Home DN as Authentication Number	Disabled	Used in conjunction with "Use SIP Endpoint Default Home DN as Authentication Number". Both attributes can be reset (default) [See 3] or one set (mutually exclusive). If set, the OpenScape Voice calling subscriber or feature subscriber's Home DN is used as the authenticated number.	Sect. 5.1.1.1 Sect. 6.4.21

CLI -> Application-level Management -> Feature Management Endpoint Profile -> QoS for SP Management			
DSCP Class DSCP Precedence	Expedited/ Default (binary 101000)	These parameters control the Differentiated Services Code Point values in the IP packet headers of SIP signaling messages (Signaling Type = SIP; QoS Type = Differentiated Services Code Point). Different Service providers may have different requirements. Verizon US requires Class 3/Medium (binary) 011 100. Note: The DSCP value for RTP packets is configured in the endpoints i.e. phones, Media Server, etc.	Sect. 4.3.12

1. This is the former "Send forwarding number rather than calling number for forwarded calls" attribute renamed since it applies to other scenarios and remains for backward compatibility. The attributes "Send authentication number in xxx header" should be used instead.
2. Redirecting features include the OpenScape Voice Serial Ringing, Simultaneous Ringing, or Subscriber rerouting feature like Call Forwarding.
3. If both “Use Subscriber Home DN as Authentication Number” and “Use SIP Endpoint Default Home DN as Authentication Number” are reset (default) the behavior for selecting the authentication number is:
   - For subscriber originated or feature subscriber calls the external Caller-ID is used
   - For trunk originated calls the SIP endpoint default home DN is used

8 Non-Standard SIP Trunking Capabilities for Italtel Service Provider

The following capabilities are requested when sending SIP requests to an Italtel service provider (or other service provider that has the same interop requirements) SIP trunk:

- Send P-Preferred-Identity (PPI) SIP Header field rather than P-Asserted-Identity (PAI) SIP header field.
- Send domain name (instead of IP address) in host part of SIP From Header header field.
- Send domain name of "anonymous.invalid" (instead of IP address) if the caller has Calling Line Identity Presentation Restricted (CLIR).
- When a call is forwarded send SIP From and PPI header fields with the identity of the transferring/forwarding party rather than the calling party.
- Do not send SIP reINVITE requests without SDP.

List of Abbreviations

The following list defines the abbreviations this manual uses.

Abbreviation	Definition
B2BUA	Back-to-Back User Agent
CCBS	Call Completion to Busy Subscriber
CCNR	Call Completion on No Reply
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Presentation Restriction
COLP	Connected Line Identification Presentation
COLR	Connected Line Identification Presentation Restriction
CRL	Certificate Revocation List
DID	Direct Inward Dialing
DN	Directory Number
DNS	Domain Name System
DNS	Domain Name Server
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DTMF	Dual-Tone Multifrequency
ENUM	Telephone Number Mapping
ETSI	European Telecommunication Standardization Institute
FQDN	Fully Qualified Domain Name
GWY	Gateway
IP	Internet Protocol
ISUP	ISDN User Part (SS7)
LIN	Location Identification Number
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control protocol
MTP	Message Transfer Part (SS7)
NAPTR	Naming Authority Pointer Records
NCS	Network Based Call Signaling Protocol
NE	Network Element

NNI	Network-Network Interface
OCSP	Online Certificate Status Protocol
PBX	Private Branch Exchange
PPPoE	Point to Point Protocol over Ethernet
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request For Comments
RTP	Real-time Transport Protocol
SBC	Session Border Controller
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SP	Service Provider
SSNE	SIP Signaling Network Element
TCAP	Transaction Capabilities Application Part (SS7)
TCP	Transmission Control Protocol
TISPAN	Telecommunications and Internet Converged Services and Protocols for Advanced Networking
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
URI	Uniform Resource Identifier
VCU	Video Conference Unit
VM MS	Voice Mail/Media Server
V-MG	Video Media Gateway
XML	Extensible Markup Language

Glossary

F

Fully Qualified Domain Name
Complete domain name from top level domain and all corresponding subordinate domain names, for example server.siemens.com.

G

Gateway
A protocol converter (that is between IP protocols and TDM protocols, or between one IP protocol and another IP protocol) that resides at the network edge and provides translation in both directions, for example SIP messages and RTP media streams are converted to other protocols like ISDN signaling over T1/E1 trunking facility.

I

Inbound Request/Response
SIP Request/Response from the Service Provider to the OpenScape Voice server.

IP PBX (PBX)
An IP PBX constitutes an Enterprise's collection of network elements that provides packetized voice call origination and termination services using SIP for signaling and RTP for media traffic. The definition of an IP PBX for the purposes of this specification includes any IP Phones under the IP PBX System's control (see "IP Phones" below).

IP Phones
IP Phones are devices that are capable of originating and terminating packetized voice calls using the Enterprise's IP PBX. For the purposes of this specification, IP Phones are considered part of the IP PBX System itself and are therefore subject to the same overall requirements.

L

Local Number
A number that is unique only within a certain context—for example, a geographic area, a certain part of the telephone network, an OpenScape Voice server, a particular local exchange carrier, or a particular country. Note: URIs with local phone numbers should only appear in environments where all local entities can successfully route the call. See RFC3966 [29] for details.
For example, the local number 1234 can only be used as dialed number/displayed number within a particular OpenScape Voice system and numbering plan without the possibility of alternate routing outside of that local area.

O

OpenScape Voice
A softswitch that may be deployed as an IP PBX. OpenScape Voice operates as a SIP B2BUA.

Outbound Request/Response
SIP Request/Response from the OpenScape Voice server to the Service Provider.

P

Private Identity
As per SIP Forum [33], the private identity represents the identity that the Enterprise wants to deliver to the **Service Provider** for a given call. Typically this would be a DID number if available.

Public Identity
As per SIP Forum [33], the public identity represents the identity that the Enterprise wants to deliver to the **PSTN** for a given call. Typically this could be the main business number.

S

SBC (Session Border Controller)
A network intermediary that resides between two networks, typically between the OpenScape Voice network and the Service Provider network. An SBC may provide functions such as the following:
- NAT traversal (inspect SIP messages and modify contained IP addresses and ports)
- security (TLS origination and termination, IPSec VPN tunnel origination and termination)
- network management (QoS, traffic monitoring, traffic shaping, and so on)

Service Provider
A provider of VoIP services to customers via a SIP interface.
Note: A Service Provider usually offers services like PSTN network access via gateways.
Note: A trusted Service Provider is when a Service Provider and an OpenScape Voice system have a mutual agreement, which assures that identity information is not conveyed beyond the Service Provider if this is requested by the calling or called party. This is usually configured during deployment of the OpenScape Voice system. Usually, a Service Provider is *trusted.*

SIP message
Either a SIP request or a SIP response.

SIP Trunk
An IP relationship between two SIP signaling network entities that provides for signaling a range of SIP user dialogs that may be originated, terminated or routed further in the network. These SIP user dialogs may be between network entities that support a multiplicity of users.
The interface between a client and the SIP Server with which the client registers, including when an entity such as an edge proxy or an SBC is situated between the client and the SIP Server, is outside the scope of this document.

SSNE (SIP Signaling Network Element)
A generic term for any network element that handles SIP messages. Within this document, this term is used when a statement refers both to OpenScape Voice and the Service Provider.

Index

T

U