
# Technical Description

Session Border Controller as a Service - SBCaaS

## Table of Contents



# 1 Technical description

This document describes the technical leaflet for *Service Provider X* which can be used as an example to set up the Netaxis SBCaaS solution for that *Service Provider X*. It provides a comprehensive overview of the technical requirements and configurations necessary for integrating with the SIP services of *Service Provider X*.

# 2 Structure

The document is structured with the following sections:

1. Overview
2. Basic Features
3. Parameters to communicate
4. SIP Specifications and Considerations
5. Example SIP Header Formats & Messages
    - SIP REGISTER
    - INVITE Outbound to PSTN
    - INVITE Inbound from PSTN

# 3 Overview

Customers can connect their own PBX/Voice infrastructure based on SIP registration or peering to the cloud service of *Service Provider X*. For registration and for placing PSTN calls, specific SIP header formats must be used. The header formats are described in the table below, and some message examples are provided for clarification.

# 4 Basic Features

- **External SIP Platform Registration**: External SIP platforms (servers and/or users) can register to the cloud SRE/SBC service of *Service Provider X*, enabling seamless integration and connectivity.
- **IP/Subnet Access Limitation**: Access can be restricted to specific IP addresses or subnets. Customers must provide their IP addresses or subnets during the onboarding process. All other IP addresses will be blocked, ensuring secure and controlled access.
- **CDR Call Rating**: *Service Provider X* handles Call Detail Record (CDR) rating based on the P-Asserted-Identity header information, removing the need for customers to perform their own CDR call rating. The SBCaaS solution can produce CDRs, in case customers or the Service Poviders them.
- **Call Admission Control (CAC)**: Call Admission Control is based on the number of concurrent calls assigned to a specific customer. The maximum number of concurrent calls is determined during the onboarding process. If a customer exceeds the allowed number of concurrent calls, the next call will be denied with a SIP 403 Forbidden response.
- **Customer Status Indication**: Customers are assigned a status of Production, Pre-Production, or Test. The CAC for test and pre-production statuses is set to a maximum of 2 concurrent calls, while the production status will have the configured limit for the customer.
- **Routing Based on tgrp/context**: Incoming and outgoing calls are routed based on the tgrp (trunk group) or context, ensuring proper call handling and routing.
- **Proxy Mode Handling**: All calls are handled in proxy mode, which allows *Service Provider X* to manage and control call flows efficiently.
- **Registration Requirement**: The customers' requirement for registration is specified in the customers' table (registration = True or False), indicating whether registration is necessary for the SIP trunk.
- **Authentication Data**: Authentication information, including usernames and passwords, is stored in a dedicated table for secure and efficient authentication management.

- **Call Screening**: For every incoming call from a customer, the calling number is verified first. P-Asserted-Identity, From, and Diversion headers are used to perform this call screening. If call screening fails, the call is terminated with a SIP 488 Not Acceptable Here response, enhancing security and call integrity.
- **Password Security**: Once configured, the customers' password is not displayed in the GUI.

# 5 Parameters to communicate

## 5.1 Parameters to be Communicated to the Customer

| Parameter | Value | Description |
|---|---|---|
| Domain | serviceproviderx.sre.netaxis.cloud | SIP domain to be used as described here. |
| Outbound Proxy | sip.serviceproviderx.sre.netaxis.cloud | FQDN of the SIP trunk on Netaxis cloud SBCs. |
| Username (*) | *SIP username* | Username for the authentication of SIP messages if registered SIP trunk is chosen |
| Password (*) | *SIP password* | Password for the authentication of SIP messages if registered SIP trunk is chosen |
| Signaling IP address | *IP address* | Public IP address of Netaxis cloud SBC currently in use for the signaling |
| Signaling IP port | 5060 (UDP/TCP), 5061 (TLS) | IP port used for signaling |
| Media IP address | *IP address* | IP address to be authorized on customers' firewall if any for media |
| Media IP ports range | 10000-19999 | IP port range used for the media |
| Registration expiry mode | 60 seconds | Registration parameter |
| Keep alive time-out | 30 seconds | Registration parameter |

(*) Parameter provided only for the SIP registration mode

### 5.2 Parameters that the Customer Must Communicate to *Service Provider X*

| Parameter | Description |
|---|---|
| Signaling IP address(es) | IP address(es) from which the SIP signaling is sent/received |
| Signaling port | IP port of the signaling |
| Transport protocol | UDP, TCP, or TLS |
| Registration | If the registration of the SIP trunk is necessary or not |
| Root/Intermediate cert | In case of TLS, the root/intermediate certificates of their SIP trunk |
| Media IP address(es) | IP address(es) from which the media is sent |
| Media ports | IP port range of the media |
| Phone numbers | Phone numbers of the PBX(es) |
| Number of channels | Number of concurrent calls to be allowed |

## 6 SIP Specifications and Considerations

| Parameter | Value | Description |
|---|---|---|
| Protocol | SIP/UDP/TCP/TLS | SIP over UDP/TCP/TLS |
| Related Standards | RFC2833, RFC3261, RFC3264, RFC3325, RFC3326, RFC4566 | Aim to be compliant with these standards, though deviations might occur for compatibility |
| Supported Methods | ACK, BYE, INVITE, OPTIONS, REGISTER | Only these SIP Methods can be used, all others might be ignored |
| Codecs | g711a | Only codec g711a-law allowed. Others might be available on certain destinations but are not officially supported. |
| DTMF | RFC2833 | Support only RFC 2833 for DTMF. SIP INFO or inband might work in certain cases but are not officially supported. |

| Parameter | Value | Description |
|---|---|---|
| T.38 | Not supported | Do not support T.38 passthrough. Although it might work on certain destinations, it is not officially supported. |
| Authentication | SIP DIGEST | SIP REGISTER with DIGEST authentication |
| Call Authorization | SIP DIGEST | SIP INVITE with DIGEST authorization |
| Number Format | E164+ | All SIP headers sent or received by *Service Provider X*, including Request URI, From, To, and PAI must use international E164+ format (example +3226260120) |
| Expiry Timer | Min SE | The value for the Session Expiry Timer is 1800 seconds |
| Caller ID | P-Asserted-Identity | Besides the From header, the caller ID should always be set in the P-Asserted-Identity header. Calls without P-Asserted-Identity will not be routed. |
| Anonymous Caller ID | Privacy | Calling out anonymously can be done using the Privacy header setting. The header “Privacy: id” will hide the caller id. The P-Asserted-Identity header should always be set to a valid number. |
| Call Deviation | Diversion | Supported |
| Provisional Responses | PRACK | Supported |
| Keepalive | OPTIONS | Might periodically send an OPTIONS packet to check if the trunk is alive. An OPTIONS message should always be replied with a 200 OK. We will also reply 200 OK to any received OPTIONS message. |