SIP Trunking Technical Specification

Document Date:	Friday, 2 October 2020
Document Version:	18

Introduction

This document describes the technical specifications for the SIP trunking service. This document is written for Network Engineers, System Administrators, Field Engineers, and Technical Consultants who have been tasked with setting up, managing, troubleshooting the SIP trunking Service.

Service Overview

sipsynergy's SIP Trunks provide VoIP connectivity for SIP capable PBX's, allowing inbound and outbound telephony through sipsynergy's network for termination with both national and international destinations.

sipsynergy's SIP Trunking service uses SIP (Session Initiation Protocol) as the signaling method and offers both Public and Private Access to the service depending on the specific customer needs.

The sipsynergy SIP Trunking Service includes the following:

- CLIP (Calling Line Identity Presentation)
- CLIR (Calling Line Identity Restriction)
- Fax
- DTMF support

The features listed above are supported in the sipsynergy network. However it should be noted that the features are not guaranteed to be supported on every CPE platform connected to the sipsynergy SIP Trunk Service because of vendor interoperability issues.

The sipsynergy SIP Trunk Service provides SIP signaling as a method for Communication Providers to interconnect with sipsynergy's VoIP network supporting calls to/from the PSTN as well as VoIP to VoIP calling between SIP accounts created within the sipsynergy SIP Trunk Service. The following types of calls are supported across this interface:

- Voice calls to/from PSTN or geographic destinations (01,02)
- Voice calls to/from non geographical, corporate or VoIP numbers (03, 05, 08)
- Voice calls to/from Premium numbers (09),UK, International)
- Voice calls to/from Mobile destinations (07)
- Voice calls to/from International destinations (00..)
- Operator, Emergency and non-Emergency calls (100, 101,111,112, 116xxx, 118, 123 1800x, 195, 999)

Service Features

Calling Line Presentation (CLIP)

Calling Line Identification Presentation (CLIP) is a service that transmits a caller's number to the called party's telephone equipment during the ringing signal.

If the CPE connected to the sipsynergy network presents a geographic number in the UK National format, the sipsynergy Network will pass these details as the A-Number CLI into the PSTN or Mobile network. This outbound presentation will be supported by default if the number presented is as follows:

- A number in E.164 format presented by the Customer Premises equipment (CPE) as the A-number.
- A sipsynergy provided Geographic Number that is allocated to the SIP trunk account or;
- A Geographic number that is ported from another Carrier to the sipsynergy Network that is allocated to the SIP trunk account

If the number presented does not meet the above criteria, the A-Number CLI presented will be witheld.

sipsynergy cannot guarantee consistent presentation of intended CLIs for calls made to mobile carriers as, successful presentation of the intended CLI is entirely dependent on the mobile carriers use of these numbers and specific call flow. Mobile missed calls and voicemail notifications can often use the default CLI, which is the first number in the sipsynergy allocated account range, rather than the intended CLI for presentation.

When CLIP is requested by the calling party on an inbound call towards the CPE, sipsynergy will ensure that all CLI information is passed to the sipsynergy SIP Trunk Service Endpoints; those headers being From, Contact and Privacy header (PAID)

> ⊘ Please do not use RPID. This header was defined in a failed RFC : http://tools.ietf.org/html/draft-ietf-sip-privacy-00 . Although this header is supported by many SIP devices, this was never accepted as a standard. You should not be using this header.

For example:

Headers contained within Invite towards SIP Trunking Endpoint

```
From: <sip:+44123456789@siptrunk.sipsynergy.net>;tag=3541226335-339769
Contact: <sip:+44123456789@siptrunk.sipsynergy.net>
P-Asserted-Identity: <sip:+44123456789@siptrunk.sipsynergy.net>
```

> ⚠ With CLIP no modifications are performed for SIP Trunking untrusted requirements.

Calling Line Restriction (CLIR)

When the calling (A-Party) has requested privacy (CLIR), sipsynergy will enforce privacy in accordance with RFC3325. Calling party information, including From Address, Contact and associated Privacy Header (PAID) are withheld from an endpoint.

For calls from the CPE to sipsynergy, the CPE must indicate that CLI is to be withheld by the following mechanism:

- RFC3261 Section 8.1.1.3 and 20.20 which describes the use of an "Anonymous" display field to the From: header to indicate that the client is requesting privacy.
- SIP Privacy which is described by RFC 3323 and RFC 3325

For calls from sipsynergy to the CPE, the From address is set to – "Anonymous"<sip: anonymous@anonymous.invalid> as per RFC 3323, the contact header is set to Anonymous and the Privacy header (P-Asserted-Identity RFC 3325) is removed from the outbound INVITE to the SIP Trunking endpoint to provide true CLI restriction.
If the Privacy header contains only "id," or only "id" and "critical" values, sipsynergy removes the Privacy header completely.
The Contact user part is changed to "anonymous."

Fax

The sipsynergy SIP Trunking Service will support Fax and Modem transmission subject to the following constraints:

- FAX and Modem transport in band using G.711 a-law codec is supported, but not recommended

- Renegotiation to T.38 is supported and recommended
- The use of G729 for in-band faxes is not supported

If the fax option for an endpoint is set to T.38 enabled then:

- The sipsynergy network will attempt to re-negotiate [re-INVITE] to T.38 for fax calls for ingress (Customer to sipsynergy) calls on detection of a fax tone.
- The sipsynergy network will accept a re-negotiation [re-INVITE] to T.38 for fax calls for egress (sipsynergy to Customer) calls.
- The re-negotiation must be done using the re-INVITE mechanism after answer.

Due to different vendor implementations sipsynergy cannot guarantee T.38 interoperability with all vendors and will not accept responsibility if T.38 interoperability cannot be achieved with a specific vendors implementation. If the fax T.38 renegotion option for an endpoint is not available then all fax calls will be handled as G.711 pass through providing the customer has a G.711 codec available in their media profile.

DTMF

The sipsynergy core network supports the generation of 'In-band' or 'RFC2833' DTMF transport based on end to end negotiation. RFC2833 is the preferred method for the transport of DTMF tones. Support of RFC 2833 is dependent on successful codec negotiation and requires the payload type 101 to be assigned.

Spend Limits

sipsynergy SIP trunks have a pre set spending limit applied to each trunk. The following table defines the spend limits applied by default, and the configurable maximums. If you want to increase the limit above the maximum, please raise a ticket with our service desk.

Limit	Amount
Daily Spend (Default)	15.00
Daily Spend (Max)	30.00
Monthly Spend (Default)	120.00
Monthly Sped (Max)	240.00

Service Capabilities

Calling Plans and Number formats

Two calling plans are allocated to each Endpoint: one for incoming calls from the customer to sipsynergy (ingress), and one for outgoing calls from sipsynergy to the customer (egress). It is a requirement of the SIP Trunking product that the calling party (A-number) be validated to confirm the format and ensure that the number is owned by sipsynergy, so that the emergency services have an accurate record of the calling customer.

Presentation CLI (A-Number)

A-numbers (SIP FROM, P-Asserted-ID) should be presented in E.164 format, i.e. +441611234567. The A-number is validated by the SBC and if it is not in the sipsynergy range it is overwritten and witheld. It is a requirement of the SIP Trunking service that the calling party (A- number) be validated to confirm the format and ensure that the number is owned by sipsynergy, so that the emergency services have an accurate record of the calling customer.

If the CPE connected to the sipsynergy network presents a geographic number, the sipsynergy Network will pass these details as the A-Number CLI into the PSTN or Mobile networks. This outbound presentation will be supported by default if the number presented is as follows:

- A-numbers are presented by the Customer Premises Equipment (CPE) in the SIP FROM and P- Asserted-ID fields as E.164 format
- It is a sipsynergy provided Geographic Number that is allocated to the Endpoint at order creation
- A sipsynergy provided Geographic Number that is allocated to the Endpoint at a later date via a Customer Change Request
- A Geographic number that is ported from another Carrier to the sipsynergy Network

If the presented number meets these criteria the A-Number CLI will be sent to the PSTN/next hop network. The delivery of the Presentation Number is dependant on the terminating network and is not under the control of sipsynergy. The A-number is checked against a database on the sipsynergy network of geographic numbers that are allocated to the SIP Trunking Endpoint. If the number presented does not meet the above criteria, the A-Number CLI that will be presented will be witheld, unless the call is to emergency

services in which case the number presented will be any number in a range assigned to the SIP trunk account to enable the emergency services to perform location based lookups. For ingress calls, A-numbers are sent to customers as received by sipsynergy from other network operators.

Network CLI (A-Number)

Every endpoint must have at least one CLI from the sipsynergy-allocated range i.e. a non-ported in number. This default number is known as the Network CLI and will be presented in the case of emergency calls and other call scenarios where the presented is invalid. Physical address information must be associated with a network CLI and it is the customer responsibility to ensure this address information remains current. sipsynergy supports both Network and Presentation CLIs. For calls from the customer to sipsynergy where the call terminates on the PSTN, the SIP FROM field is mapped to the presentation CLI and the SIP P-Asserted-ID is mapped to the network CLI.

To ensure the correct Network CLI is passed into the sipsynergy network and then forwarded to the PSTN, sipsynergy may insert the customer Network CLI Number in E.164 format into the PAID, replacing any value received from the customer CPE. For calls from the PSTN to the sipsynergy SIP Trunking endpoint, the SIP FROM field will contain the Presentation Number when available and the P-Asserted-ID field will contain the Network Number when available. If only the Network Number is available then this will be mapped to both the SIP FROM field and the P-Asserted-ID field.

B-Numbers

B-numbers should be sent to sipsynergy in E.164 format (+44 NSN). As a default configuration B-numbers will be presented to the customer as E.164.

Number Portability

Number portability for the SIP Trunking service is fully supported and tested. Number Porting changes are currently carried out manually, and it should be noted that BT will only port to a 'live' number; hence the sipsynergy SIP Trunking endpoints must be configured before the porting can take place.

Calls Per Second

For security reasons, sipsynergy set limits for the maximum calls per second (CPS). The limits are configured as a maximum of two calls per second per account.

Long Duration Calls

sipsynergy has a policy of disconnecting any call that exceeds eight hours in duration.

Codecs

Voice encoding can be g.711 A-law with a sample rate of 20 ms. sipsynergy do not support the use of video codecs and customers should make every effort to ensure that no video codecs are included in any SIP requests. sipsynergy police the media-stream bandwidth based on the negotiated codec. If a CPE exceeds the bandwidth for a specific codec, RTP packets will be discarded and this will result in poor voice quality. Silence Suppression and Comfort noise is disabled as standard. sipsynergy do not support the negotiation of codec Ptime. To preserve the quality and continuity of the service, sipsynergy enforce all the parameters in this section. Customers who do not adhere to these definitions are likely to experience issues with their calls, which may include a loss of service.

Inbound Calls

REGISTER Based

> (i)   You can only use REGISTER based inbound calling in conjunction with authentication based outbound calling.

In order for your SIP endpoint to receive inbound calls to your allocated DDI ranges, it can REGISTER with our SIP trunk service. Only one endpoint can be REGISTERed at any one time to receive inbound calls. Where more than one endpoint is REGISTERing, the last endpoint to REGISTER will receive the calls. This method of service delivery provides for greater service flexibility enabling you to choose where and when you wish to receive your inbound calls. When your endpoint originally attempts to register, you will receive a 401 Unauthorised response indicating you need to provide authentication credentials to register. You can avoid this step by sending the authorisation credentials in the original registration request if your endpoint supports it. If no endpoint is registered when we receive a call for an allocated number, we will return service unavailable to the calling party.

IP Based

> (i) You can only use IP based inbound calling in conjunction with IP based outbound calling.

You can choose to have your calls delivered to your endpoint by specifying your endpoint's IP address. Currently, sipsynergy only support IPv4 addresses, and all signalling will be UDP from our service to a destination port of 5060. You can specify one IPv4 endpoint per SIP trunk to receive calls, and you can change this registered address through gateway. This IP address will be used for outbound call authentication. Your media can terminate on alternate IP addresses, and these will need to be specified within the SIP SDP.

Protocol and Signalling

sipsynergy offer SIP signalling transport over UDP. In cases where PBXs use TCP signalling, SIP Proxy servers/IP gateways are required to convert to UDP on the customer's premises. sipsynergy SIP Trunk Service provides SIP signalling as a method for Communication Providers to interconnect with sipsynergy's VoIP network, supporting VoIP to VoIP calling as well as calls to/from the PSTN. The SIP Trunk Service supports the transport of SIP signalling messages using UDP. SIP messages sent using TCP, TLS, SCTP and IPSEC are not supported at present. SIP V2 is supported between the SBC and the customer CPE. The SIP standard is documented in the Internet Engineering Task Force (IETF) RFC 3261.

> (i) Please note that this service does not support H.323, SIP-I, SIP-D and SIP-T.

Format of the SIP INVITE Field

The SIP header requirements in the INVITE packets originated from the CPE should be set as follows:

- Request URI must contain the B-number followed by the assigned sipsynergy SIP gateway IP address: INVITE sip:+441234567890@siptrunk.sipsynergy.net;user=phone SIP/2.0
- The FROM header must contain your public facing IP address and originating CLI: FROM: <sip:+441234567890@"IP Address">; tag=3528194925-554920
- The TO header must contain the assigned sipsynergy domain and the B-number: To: <sip:+441234567890@siptrunk.sipsynergy.net;user=phone>
- SDP payload must be present, and must contain your public IP address.

Traffic on the following ports must be allowed through relevant routers and firewalls on the customer premises to allow access to the sipsynergy SIP Trunking Network:

- UDP Port 5060, 5061, 5080, 5081 egress/ingress
- UDP all ports between 16384 – 32767 egress/ingress
- For ingress calls the INVITE Request Line must contain a SIP URI.
- For egress calls from sipsynergy to the customer the INVITE Request Line will contain a SIP URI.

Outbound Calls

SIP Authentication Based

Every call attempt MUST provide athorisation credentials with EVERY INVITE. If an INVITE is received without authentication credentials, these will be requested by way of a SIP 407 Proxy Authentication Required response.

IP Authentication Based

You can specify an IPv4 address for inbound and outbound calls. This IP address will be used for outbound call authentication - your endpoint will not need to authenticate with a username and password, and you will not receive a SIP 407 Proxy Authentication Required response. Your media can terminate on alternate IP addresses, and these will need to be specified within the SIP SDP. You must use IP based inbound calling in conjunction with IP based authentication. You cannot mix IP based authentication and digest based authentication.